Hubilo

DATA PROCESSING ADDENDUM

Hubilo Technologies Inc. and its Affiliates

HUBILO DATA PROCESSING ADDENDUM

This Data Processing Addendum (hereinafter the "**DPA**" or "**Addendum**") with its annexures and appendix is part of the Master Subscription Agreement (the "**MSA**"), the Terms of Use and any other agreement wherein Hubilo Technologies Inc. and its affiliates (hereinafter called "**Hubilo**") have agreed to provide its Services (as defined below) to the organizer ("**Customer**") of an event on Hubilo Platform to reflect the parties agreement to Processing of the Customer Personal Data ("**Customer Personal Data**").

1. Commencement

This DPA shall come into effect on the same date as the MSA ("**Effective Date**"). This Addendum shall form an integral part of the MSA. The Customer and Hubilo shall be each referred to as "**Party**" or collectively as "**Parties**".

In the event of a conflict between the terms and conditions of this Addendum, or the Agreement, an Order Form, or any other documentation, the terms and conditions of this Addendum shall prevail with respect to the subject matter of Processing of Customer Personal Data.

Processing activities authorized by the Customer

The Platform provided by Hubilo is an online Software-as-a-Service solution that enables event organizers to create and manage online events through the various functionalities as made available by Hubilo, available and updated from time to time. This involves the Processing of Customer Personal Data by Hubilo about Data Subjects which includes: the personnel of organizers, sponsors, third parties and End Users / Attendees of such events as uploaded by the Customer into the Platform.

By using the Platform/ Services as a cloud-based environment, the Customer will act as Controller of all Personal Data shared and transferred to the Platform/ Services and hereby authorizes Hubilo (as Processor), its Affiliates, suppliers and sub-processors, to Process Customer Personal Data for the purpose as set out in this DPA and the MSA, and upon provision of any documented instructions to Hubilo from time to time.

In providing the Customer and facilitating the End User/s access to/ use of the Platform in accordance with the MSA, the Customer shall remain responsible for compliance with Applicable Data Protection Laws. The details of the processing, the rights and duties of the

Parties are further detailed below in this DPA and in the Standard Contractual Clauses attached and part of this DPA.

2. **Execution of DPA**

2.1 This Addendum (and Standard Contractual Clauses in Annexure I, if applicable) may have been pre-signed on behalf of Hubilo as the data importer.

2.2 To complete this Addendum, Customer must:

a. Complete the information in the signature box of this DPA and have theCustomer signatory sign on behalf of the Customer, Customer signatory represents to Hubilo that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

b. If the DPA is being signed virtually, by way of e-signatures, then you approve to execute the DPA through any of our e-signature platforms.

3. **Definitions**

All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of this Addendum, the following terms shall have the following meanings:

A. "**Affiliate**" means any legal entity directly or indirectly controlling, controlled by or under common control with a party to the MSA, where “control” means the ownership of a majority share of the stock, equity, or voting interests of such an entity.

B. "**Applicable Data Protection Laws**" means all data protection or privacy laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to the (i) the California Consumer Privacy Act (CCPA), (ii) the EU GDPR, (iii) any national data protection laws made under or pursuant to the GDPR (iv) the EU e-Privacy Directive (Directive 2002/58/EC), (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance, and (vi) UK GDPR or Data Protection Act 2018; in each case as may be amended, superseded or replaced.

C. "**Commercial Purposes**," "**Sell**," have the meanings assigned to them in section 1798.140 of the CCPA.

D. "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. The definition of Controller has meaning given to it under Article 2(7) of EU Data Protection Law.

E. "**Customer**" means the Organizer that has entered into the MSA with Hubilo to use/access Hubilo Platform to host virtual events, which term shall include its employees, independent contractors, consultants, Affiliates, successors and assigns using/ accessing the Platform/ Services.

F. "**Customer Personal Data**" means any Personal Data that the Customer shares with or permits Hubilo to access, store, host, modify, share, delete and further Process for the performance of the Services, which includes End Users/ Attendees of the Customer which is processed by Hubilo under this DPA.

G. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates to.

H. "**End Users**" or "**Attendees**" means the clients and all individuals who shall, from time to time, be attending or participating in the events organized by the Customer on the Platform and are part of Customer Personal Data under this DPA .

I. "**EU Data Protection Laws**" or "**GDPR**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, including any applicable national implementations thereof; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council 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" or "GDPR"), as amended, replaced or superseded, as well as any other applicable data protection laws and/or regulations in force in EU Member States.

J. "**Equivalent Protection Area**" means the area that comprises (a) countries within the European Union, including Iceland, Liechtenstein, and Norway, and (b) countries that the European Commission may from time to time recognize as ensuring an adequate level of protection as provided for in article 45 of the GDPR, which includes Switzerland and the United Kingdom.

K. "**ICO**" the Information Commissioner's Office, which is the UK's independent body set up to uphold information rights and promote good practice in handling personal data and guidance on data protection

L. "**Personnel**" means the employees, agents, consultants, and contractors of Customer/ Customer's Affiliates or Hubilo/ Hubilo Affiliate, as the case may be.

M. "**Personal Data**" means any information relating to a Data Subject; an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic,

cultural or social identity of that natural person. This includes any special categories of Personal Data defined in Art. 9 of the GDPR, data relating to criminal convictions and offenses or related security measures defined in Art. 10 of the GDPR and national security numbers defined in Art. 87 of the GDPR and national supplementing law.

N. "**Processor**" or "**Data Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller and as instructed by the Controllers, usually for specific purposes and services accessible to the Controller The definition of Processor has meaning given to it under Article 2(8) of EU Data Protection Law.

O. "**Sub-processor"** or " means any person appointed by or on behalf of the Processor, or by or on behalf of an existing Sub-processor, to process Personal Data on behalf of the Controller, as defined in Art. 28(4) of EU Data Protection Laws.

P. "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 1 to this DPA pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third party countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "EU SCCs"), which do not ensure an adequate level of protection, and any further approved set of contractual clauses as approved by the competent authority from time to time.

Q. "**Security Incident**" means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, use, unauthorized disclosure of or access to Personal Data.

R. "**Services**" means the Hubilo Services as set forth in the Agreement or associated Hubilo order form.

S. "**Transfer**" means any Processing, which includes accessing, sharing, disclosing or otherwise making Personal Data available, whether by a Hubilo affiliate, its suppliers or the Customer, from another location than where the Processing initially occurs, which includes:

i) any transfer of Customer Personal Data from the Customer to Hubilo;

ii) an onward transfer of Customer Personal Data from Hubilo to a Hubilo Affiliate; or

iii) an onward transfer of Customer Personal Data from Hubilo and/ or a Hubilo Affiliate to another Sub-Processor,

iv) in each case, where such Transfer would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions

of Data Protection Laws) in the absence of appropriate safeguards and any lawful mechanisms for such Transfers, which includes the use of Standard Contractual Clauses.

T. "**UK**" means the United Kingdom.

U."**UK Data Protection Laws**" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 in the UK ("**UK GDPR**") and the Data Protection Act 2018.

4. Applicability of DPA

4.1 Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Hubilo deletes all Customer Personal Data as described in this DPA.

5. Processing of Personal Data: Roles and Responsibilities of the Parties to Process Customer Data

If EU Data Protection Law applies to the processing of Customer Personal Data:

5.1 The subject matter and details of the processing are described in the DPA.

5.2 Customer Personal Data is being processed by Hubilo as part of providing access and use of the Platform to the Customer and their End User/s, as further specified in the MSA.

5.3 Hubilo is a processor of Customer Personal Data under EU Data Protection Law.

5.4 Roles of parties: Customer is a controller or processor, as applicable, of that Customer Personal Data under EU Data Protection Law. Hubilo is the Processor of Customer Personal Data and processes the Customer Personal Data under the instructions of the customer, in accordance with Article 28(1) of EU Data Protection Laws.

5.5 Legitimacy of Processing. The Controller is responsible for ensuring a valid legal basis for processing the Customer Personal Data.

5.6 The details of processing Customer personal data are enumerated below in the DPA and the Appendix attached in this DPA.

5.7 Customer acknowledges and agrees that any Processing under this DPA may also be carried out by any Hubilo Affiliate, and Hubilo Affiliate shall assume the obligations of Hubilo, in its capacity of Processor, for any such Processing under this DPA.

5.8 Each party will comply with the obligations applicable to it under the Applicable Data Protection Laws with respect to the processing of that Customer Personal Data.

5.9 If laws other than EU Data Protection Law apply to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

6. Details of processing and Hubilo's duties as Processor of Customer Personal Data

6.1 Hubilo's obligations

Hubilo shall/ may:

i) only process Customer Personal Data for the purposes set forth in the MSA, DPA and only in accordance with the lawful, documented instructions of Customer (including with regard to transfers of Customer Personal Data to a third country), unless Hubilo is required to process Customer Personal Data by the Applicable Data Protection Laws to which Hubilo is subject to (in such a case, Hubilo shall inform the Customer of that legal requirement before processing, unless applicable law prohibits such information).

ii) only act on the Customer's instructions, which may be specific or of a general nature as set out in this DPA or as otherwise notified by the Customer to Hubilo from time to time and not for Hubilo's own purposes.

iii) refrain from processing Customer Personal Data and notify the same to the Customer immediately, if the instruction to process Customer Personal Data by the Customer infringes with the EU Data Protection Laws.

iv) keep all Customer Personal Data Confidential, and ensure to only provide access to authorized employees, agents, suppliers, contractors, consultants and subcontractors who are authorized and have a need to access such complying with the same degree of confidentiality as under this DPA; Hubilo shall ensure that its relevant employees, agents and contractors receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Customer Personal Data

v) provide, at Customer's costs and expenses, reasonable cooperation and assistance to the Customer as set out this DPA;

vi) implement all appropriate technical, physical and organizational measures to ensure a level of security appropriate to the level of risk to Customer Personal Data as required by Applicable Data Protection Laws;

vii) complying with the terms of the MSA including, without limitation while providing access to: usage of the Platform/ Services, and for back-up and recovery, cyber security, operations, control, improvements and development of

the Services/ Platform, fraud and service misuse prevention and legal and administrative proceedings;

viii) unless permitted by the Customer, not: (a) sell Personal Data, nor (b) collect, retain, use, or disclose Customer Personal Data that it has access to for any purpose other than for the specific purpose of performing the Services specified in the MSA and this DPA. Unless otherwise permitted by the Customer, Hubilo shall not use any Customer Personal Data for its own commercial benefit. Except as otherwise instructed, the Customer hereby authorizes Hubilo to create de-identified or anonymized data for the purpose of improving the Services and the Platform and conduct analytics and reports on the use of the Platform/ Services;

ix) comply with other reasonable written instructions provided by the Customer in writing where such instructions are consistent with the terms of the MSA and comply with all Applicable Data Protection Laws.

x) process Customer data (business representative of the customer) for its own legitimate purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes:

a) sales pitching and management, billing, account, and Customer relationship management (marketing communication with procurement)and related Customer correspondence (mailings about for example necessary updates);

b) complying with and resolving legal obligations under Applicable Data Protection Laws, provide services to Data Subjects located in the EU or monitors their behaviors, appoint a Representative located in the EU to enable Data Subjects to exercise their rights and make such information available to Data Subjects in an appropriate manner, other tax requirements, agreements and disputes;

xi) anonymize and/ or use aggregate data for:

c) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of Hubilo Services;

d) internal reporting, financial reporting, budget planning, capacity planning and building, and forecast modeling (including product strategy);

e) receiving and using Feedback for Hubilo's overall service improvement; and

For more details on how Hubilo processes data has a controller, kindly refer to Hubilo Privacy Policy on Hubilo domain website.

6.2 When acting as an independent Controller, Hubilo will not process Customer Personal Data for any purposes other than the above list of legitimate purposes.

7. **Customer Obligations**

7.1 The Customer represents and warrants that it has undertaken to provide all necessary notices to End-Users and received all necessary permissions and consents, as required for Hubilo to Process the Customer Personal Data under this DPA and pursuant to the Applicable Data Protection Laws in their respective country and state (if applicable).

7.2 The Customer represents and warrants that it has complied with all information provision obligations under the Applicable Data Protection Laws.

7.3 To accomplish Customer's notice and consent obligations under Applicable Data Protection Laws, the Customer may refer End Users to Hubilo's Privacy Policy at https://hubilo.com/privacy-policy/ (https://hubilo.com/privacy-policy/). However, it is clear that Hubilo as a Data Processor does not bear the obligation for information provision and obtaining consent of End Users under the Applicable Data Protection Laws and only provides a notice as Processor for the Customer's convenience to explain the various processing activities, functionalities and measures and features available on the Platform. In no event, shall Hubilo's privacy policy be construed as legal advice nor replacing the Customer's privacy notice.

7.4 Responsibilities of Customer

The Customer:

i) instructs Hubilo (and authorises Hubilo to instruct each Sub-processor) to:

   a) Process Customer Personal Data in a manner that is in compliance with the Applicable Data Protection Laws; and

   b) in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the MSA;

ii) warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 5.1; and

iii) warrants and represents that it has complied with Applicable Data Protection Laws in respect of any obligations that it has under Applicable Data Protection Laws with respect to it being the Controller of Customer Personal Data. The Customer further represents and warrants that it has collected the Customer Personal Data in accordance with Applicable Data Protection Laws.

7.4.1 As Customer is the Controller of Personal Data of Data Subjects, it the responsibility of the Customer to ask for consent from End Users for new types of data processing, nor shall Hubilo

process Customer Personal Data for any "further" or "compatible" purposes (within the meaning of Articles 5(l)(b) and 6(4) GDPR) other than those specified in this DPA.

7.4.2 Customer's instructions to Hubilo for the Processing of Customer Personal Data shall comply with Applicable Data Protection Laws. Customer shall be responsible for the Customer Personal Data and the means by which Customer acquired Customer Personal Data.

7.4.3 The Customer agrees to defend, indemnify and hold harmless Hubilo from and against all claims, actions, third party claims, direct losses, damages and expenses incurred by Hubilo as a result of or in connection with the Customer's non-compliance with the Applicable Data Protection Laws.

8. Categories of Data Subjects

The Personal Data Processed by Hubilo, relates to the following categories of data subjects:

i) The Customer, its Affiliates and its End Users or Attendees, personnel, suppliers, agents, consultants, contractors, sub-contractors and suppliers and their personnel (which involves any authorized users of the Customer who shall operate the Account), and;

ii) End-Users authorized by the Customer to access the Platform.

8.1 Type of Customer Personal Data:

The Personal Data, Processed by Hubilo under this DPA includes the following categories of Personal Data:

ii) Customer Personal Data Processed for Events:

this includes event attendees, sponsors, speakers, and other third parties' Personal Data managing and supporting the online events, including:

- **contact and login details**, such as name, last name, e-mail address, phone number;
- **communication data**, such as personal data that may be used to
- **media data**: this may include pictures of attendees on their account profile, videos and voice recordings as uploaded on the platform to advertise the event in a banner, and any other media that is relevant to event management and organization that may contain other media containing Personal Data.
- **account data**, such as job profile, Customer name, type of Customer, social media account ID, LinkedIn or Facebook profile details, and any other Personal Data that the Customer may require its End-Users to include when connecting to the Platform.

- any other data that the Customer expressly instruts Hubilo to process.

8.2 Special Categories of Personal Data

Hubilo generally does not Process any Special Categories of Customer Personal Data for the performance of the Services unless the Customer exclusively instructs Hubilo to do so. If the Customer requires the Processing of any Special Categories of Data, the Customer shall ensure that such Processing is lawful and complies with all Applicable Data Protection Laws, which may include special protections of such data.

9. **Rights of Data Subjects**

9.1 Hubilo, depending on the nature of processing, must provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to any Data Subject rights under Applicable Data Protection Law (including its rights of access, to rectification, to erasure, to restriction, to objection, and data portability, as applicable).

9.2 If Hubilo's Privacy Team receives a request from a data subject that relates to Customer Personal Data, Hubilo will: (a) advise the data subject to submit their request to Customer; (b) notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customers will be responsible for responding to any such request, and where necessary, Hubilo will provide complete assistance in responding to the Data Subject requests. Hubilo reserves the right to reimbursement from Customer for the reasonable cost of any time, expenditures or fees incurred in connection with such assistance provided to Customer.

10. Cooperation and assistance

10.1 Hubilo will provide the Customer with commercially reasonable cooperation and assistance in relation to handling the inquiries from End Users regarding their Personal Data to the extent legally required and to the extent Customer is unable to Process such End User request through the features available on the Platform, if the Customer has requested, in writing, Hubilo's assistance. The Customer is liable to reimburse Hubilo for any costs and expenses related to the provision of such assistance.

10.2 This includes responding to inquiries from authorities and data subjects and, where applicable, to provide reasonable support to the Customer in case of data breaches and notifications to authorities and/or data subjects, with data protection impact assessments or to consult authorities.

10.3 It is clarified that Hubilo or any of its Sub-processors shall not respond to that request except as required by Applicable Data Protection Laws to which Hubilo or any of its Sub-processors is subject, as applicable, in which case Hubilo shall to the extent permitted by Applicable Data Protection Laws inform Customer of that legal requirement before Hubilo or any of its Sub-processors responds to the request.

11. Authority Of Customer to issue instructions assistance

11.1 The Customer shall issue instructions to Hubilo in writing/ via e-mail. Hubilo will duly cooperate with and make commercially reasonable efforts to assist the Customer in complying with Customer's obligations pursuant to the Applicable Data Protection Laws, considering the nature of processing, technical and organisational feasibility, and the information available to Hubilo. The Customer shall reimburse costs and expenses for any cooperation and assistance services provided to the Customer in that regard.

12. Hubilo Personnel

12.1 **Limitation of Access:** Hubilo shall take reasonable steps to ensure the reliability of any employee, agent or contractor of Hubilo who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/ access the relevant Customer Personal Data, as strictly necessary for the purposes of the MSA, and to comply with Applicable Data Protection Laws in the context of that individual's duties to Hubilo, as applicable, ensuring that all such individuals are subject to required confidentiality obligations.

12.2 **Confidentiality** Hubilo shall ensure that all such Personnel are informed of the confidential nature of the Customer Personal Data and are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

12.3 Hubilo shall also impose required contractual obligations upon its Personnel who are engaged in the Processing of Customer Personal Data regarding obligations under Applicable Data Protection Laws and thus bind the Personnel to the same obligations that Hubilo has with respect to the Processing of Customer Personal Data.

13. Approved Sub-processing

13.1 Customer acknowledges, agrees and authorizes, that Hubilo may engage Sub Processors for certain Processing activities as required from time to time on Customer's behalf in accordance with this section 13 and subject to any restrictions in the MSA.

13.2 Customers approve the Authorized Sub-processors listed at https://www.hubilo.com/sub-processors.

13.3 Hubilo may continue to use those Sub-processors already engaged by Hubilo as at the date of this DPA, subject to Hubilo in each case as soon as practicable meeting the obligations set out in section 14.

13.4 Hubilo shall notify the Customer of the appointment of any new Sub-processors, including full details of the Processing to be undertaken by the Sub-processors within 30 (thirty) days of such appointment. If, within 10 (ten) days of receipt of that notice, Customer notifies Hubilo in writing of any objections (on reasonable grounds) to the proposed appointment, Hubilo shall

work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processors.

13.5 With respect to each Sub-Processor, Hubilo shall:

i) Hubilo shall ensure that Authorized Sub-processors have executed confidentiality agreements that prevent them from unauthorized Processing of Customer Personal Data both during and after their engagement by Hubilo.

ii) ensure that the arrangement between on the one hand (a) Hubilo, and on the other hand the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

iii) if that arrangement involves a Transfer, Hubilo shall ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Hubilo and on the other hand the Sub-processor, or before the Sub-processor first Processes Customer Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the Customer; and

iv) provide to Customer for review such copies of Hubilo's agreements, as applicable, with Sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Customer may request from time to time.

v) Hubilo shall communicate the request made by the data subject regarding any data subject rights regarding their personal data in accordance with the Applicable Data Protection Law to each of its Sub-Processor to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort.

14. Hubilo’s Security Responsibilities

14.1 Taking into account the current state of the art, best industry standards the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Hubilo shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and equivalent provisions under the Applicable Data Protection Regulations, including, but not limited to, the “Security Measures” set out in Annex II to the Standard Contractual Clauses . Customer acknowledges that the Security Measures are subject to technical progress and development and that Hubilo may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

14.2 Hubilo will maintain administrative, physical and technical safeguards to ensure a level of security including the anonymization, pseudonymization and encryption of Customer Personal Data and protection of the security, confidentiality, and integrity of Customer Personal Data. Hubilo shall monitor compliance with these safeguards and will not in any case, decrease the overall security during the Terms of the MSA.

14.2 Hubilo shall provide for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

14.3 In assessing the appropriate level of security, Hubilo shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

14.4 Hubilo shall provide to the Customer at reasonable intervals (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum), the most recent version of Hubilo's information security policy, as Customer may request from time to time.

15. Customer's Security Responsibilities

15.1 Without prejudice to Hubilo's obligations under this Section (security), the Customer:

i) shall remain solely responsible for its use of the Services, including: (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (c) backing up the Customer Personal Data; and

ii) acknowledges that Hubilo has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Hubilo and each Hubilo Affiliate's and its Sub-processors' systems (for example, offline or online premises storage).

15.2 For the provision of Services, Hubilo warrants that they comply with the data protection measures required by the Applicable Data Protection Laws.

16. Supervisory Power of Customer and Audits

16.1 Upon Customer's written request, at reasonable intervals, Hubilo shall make available to Customer which is not a competitor of Hubilo, information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer, at the Customer's cost, in relation to the Processing of the Customer Personal Data by Hubilo and their Sub-processors, provided that such audit right is available to the Customer once yearly.

16.2 Information and audit rights of the Customer only arise under clause 16.1 to the extent that the MSA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

16.3 Customer or an auditor mandated by the Customer undertaking an audit shall give Hubilo a notice of 30 (thirty) days prior to any audit or inspection which is to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing any damage, injury or disruption to Hubilo' s premises, software, equipment, Personnel and or business while its personnel are on those premises in the course of such an audit or inspection.

16.4 Nothing in contrary to the above, if the Customer believes, acting reasonably and in good faith, that an on-site or remote audit is necessary to verify compliance with privacy and security obligations of Hubilo, the Customer may request that it or a third party conducts an audit, which shall be subject to the conditions set out below:

i) an audit plan must be agreed by the Parties and, if applicable, the third-party auditor, eight (8) weeks in advance of the proposed audit date.

ii) the audit plan will describe the scope, duration, third party auditor and start date of the audit and shall be limited as to ensure Hubilo's confidentiality and security obligations towards its employees and counterparties.

iii) unless prohibited by legislation binding on the Parties, the Customer must provide Hubilo with a copy of the audit report free of charge.

16.5 Customer shall ensure that any such auditor as engaged by the Customer shall perform the audit in compliance with this DPA, and Applicable Data Protection Laws.

16.6 Hubilo, and its Sub-processors need not give access to its premises for the purposes of such an audit or inspection:

i) to any individual unless he or she produces reasonable evidence of identity and authority; or

ii) outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Customer undertaking an audit has given notice to Hubilo that this is the case before attendance outside those hours begins.

17. Personal Data Breach Management and Notification

Breach prevention and management

17.1 Hubilo will continue to maintain security incident management policies and procedures to the extent required by law and shall promptly notify Customer of any Personal Data Breach which Hubilo or any Sub-processor becomes aware of.

17.2 Hubilo shall provide the Customer with sufficient information regarding the Personal Data Breach enabling the Customer to meet any obligations to report such Personal Data Breach to any authorities or inform the End-Users of such Personal Data Breach.

Remediation

17.3 Hubilo will make reasonable efforts to identify and, to the extent such Personal Data Breach is caused by a violation of the requirements of this DPA by Hubilo, remedy the cause of such Personal Data Breach. Hubilo will provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Laws to notify a regulatory authority or any Data Subjects of a Personal Data Breach.

17.4 Hubilo shall provide notification of a Personal Data Breach in the following manner:

i) Hubilo shall, to the extent permitted by Applicable Data Protection Laws, notify Customer without undue delay, after Hubilo's confirmation or reasonable suspicion of a Personal Data Breach impacting Customer Personal Data of which Hubilo is a Processor;

ii) Hubilo will notify the occurrence of the Personal Data Breach to the email address of the Customer's Account owner.

17.5 As part of above notification, Hubilo shall provide:

i) A description of the nature of the Personal Data Breach including the volume and type of Customer Personal Data affected and the categories and approximate number of individuals concerned;

ii) The likely consequences of the Personal Data Breach; and

iii) A description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

18. Data Protection Impact Assessments and Prior Consultations

18.1 Hubilo shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with any supervisory authority or other competent data privacy authorities, which the Customer reasonably considers to be required as under article 35 or 36 of the GDPR or equivalent provisions of the Applicable Data Protection Laws , in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to Hubilo, Hubilo Affiliate, or any Sub-processor.

19. Deletion Retention and Return of Customer Personal Data

Data Deletion and Return

19.1 Hubilo shall retain the Customer Personal Data for a period of 3 (three) years from the date of termination of the MSA solely for repurposing and/or reusing the Customer Personal Data for any future events hosted by the Customer on the Platform in accordance with the terms of the MSA. Hubilo shall not use this data for any purpose apart from retaining it for the Customer. Post completion of the above mentioned 3 (three) years period, Hubilo shall automatically delete all data provided by the Customer and procure the deletion of all copies of Customer Personal Data from its Sub-processors.

19.2 The Customer can request Hubilo at any point in time to delete and/ or return all data by way of a written request or instruction, which shall be processed by Hubilo within 15 days from the receipt of such request. It shall be Customer's exclusive responsibility to secure all necessary data/ information from the Customer's Account prior to such deletion, including the Personal Data of End Users.

Data Retention

19.3 Copies or duplicates of the data shall never be created, except when Customer agrees that Hubilo may retain copies of Customer Personal Data as necessary in connection with its routine backup and archiving procedures. The data retention of Customer Personal Data shall remain anonymous in such a manner that the data no longer constitutes personal data.

19.4 Hubilo and its Sub-processors may retain Customer Personal Data to the extent required by Applicable Data Protection Laws and other applicable laws and always provided that Hubilo and its Sub-processors shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Data Protection Laws requiring its storage and for no other purpose.

Disclosure To Competent Authorities

19.5 Hubilo may disclose Customer Personal Data, (a) if required by a summon/ subpoena or other judicial or administrative order, or if otherwise required by the Applicable Data Protection Laws and other applicable laws if any.

Compliance and contact

19.6 Hubilo's team is responsible to make sure that all Hubilo Personnel, Affiliates, and Sub-processors adhere to this DPA. You can reach out to Hubilo for compliance related queries at mydata@hubilo.com (mydata@hubilo.com).

20. Cross-border data transfers

20.1 The parties acknowledge and agree that in the event that Customer transfers Customer Personal Data to Hubilo makes routine transfers of Customer Personal Data in the normal course of business to itself or its Affiliates and/ Sub-processors, and these transfers include may Customer Personal Data wherein Applicable Data Protection Laws apply to, such transfers, to any countries which do not ensure an adequate level of data protection, be undertaken by Processor through one of the following mechanisms:

i) Where a Data Transfer occurs for which the Customer are acting as Controller and provide Customer Personal Data of EU/ EEA and Swiss Data Subjects to Hubilo as a processor under this DPA, then any Data Transfers that occur of such data shall be governed by the Standard Contractual Clauses set forth in Annexure I to this Addendum. (EU Standard Contractual Clauses (Module 2: Controller to Processors), any change on the sub-processor list will be informed to the Customer by Hubilo here.

ii) Appendix Annex I to the SCC will be completed with the information that Customer will be the data exporter and Hubilo shall be the data importer of Customer Personal data.

iii) Appendix Annex II contains the security measures adopted by Hubilo to keep Customer Personal Data safe and secure.

iv) For international data transfer as per UK GDPR, where a Transfer occurs for which the Customer is acting as a Controller and provide Customer Personal Data of UK Data Subjects to Hubilo acting as a Processor under this DPA, then any Transfers which occur of such data shall be governed by the EEA controller to processor SCCs incorporating the amendments set out in clause 3.a. and the UK Addendum set forth in this DPA.

20.2 Where Customer permits the transfer of the Customer Personal Data outside the Equivalent Protection Area (European Union, Iceland, Lichtenstein, Norway, or the United Kingdom (the "EEA")), the Transfer should be based on the Standard Contractual Clauses or via any other lawful transfer mechanism. The Customer's approval is given at the effective date in accordance with the instructions and processing activities as set out in this DPA.

20.3 To the extent that any chosen lawful mechanism provided above is no longer valid, the Customer shall implement any appropriate alternative transfer mechanism to comply with Applicable Data Protection Laws.

20.4 Subject to section 20.1, the Customer (as "data exporter") and Hubilo and their Sub-processors, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Transfer from the Customer to Hubilo or their Sub-processors.

20.5 The Standard Contractual Clauses shall come into effect under section 20.1 on the later of:

(i) the data exporter becoming a party to them;
(ii) the data importer becoming a party to them; or
(iii) commencement of the relevant Transfer.

20.6 Section 20.1 shall not apply to a Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Transfer to take place without breach of Applicable Data Protection Laws.

20.7 Before Hubilo provides its services to the Customer in accordance with the present Agreement, if the Customer concludes, based on its current or intended use of the Services, that the alternative transfer mechanism and/or Standard Contractual Clauses, as applicable, do not provide appropriate safeguards for Customer Personal Data, then Customer may immediately terminate the applicable Agreement and for convenience choose to do so by notifying Hubilo.

21. General Terms

21.1 If the Customer Personal Data with Hubilo is jeopardized due to attachment or confiscation, insolvency proceedings or due to other events or measures of third parties, Hubilo shall immediately notify (i) the Customer thereof, and (ii) all institutions or persons competent or concerned that the Customer as the Controller as defined in the Applicable Data Protection Laws holds the exclusive sovereignty over and exclusive title to the data.

21.2 Each Party shall keep a record of their processing activities. They agree to co- operate with the Data Protection Authority/ Supervisory Authority when required to do so.

21.3 Hubilo may designate a representative as laid down in Art 27 Paragraph 1 GDPR in the European Union, as applicable.

22. Governing law and jurisdiction

Without prejudice to the Standard Contractual Clauses:

22.1 The parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the MSA with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

22.2 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the MSA.

23. Order of precedence

23.1 Nothing in this Addendum reduces Hubilo's obligations under the MSA in relation to the protection of Personal Data or permits Hubilo to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the MSA. In the event of any conflict or inconsistency between the provisions of this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

23.2 In the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the MSA and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

24. Severance

24.1 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Hubilo

ANNEXURE I

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

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

Clause 3

Third-party beneficiaries

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

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

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

(iii) Clause 9(a), (c), (d) and (e)

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

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.

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.

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.

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.

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).

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.

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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

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 of Regulation (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.

Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) 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 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

(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 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.

(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[4];

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

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

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

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

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

Clause 15

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

15.1. Notification

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

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

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

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

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

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

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

15.2. Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the laws of Ireland. Any dispute arising out of the Standard Clauses shall be brought before the exclusive courts of Ireland.

Clause 18

Choice of forum and jurisdiction

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

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

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

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

APPENDIX

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

Applicable to European Data Transfers

A. LIST OF PARTIES

Data exporter(s)-

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): **Controller**

Data importer(s)-

Name: **Hubilo Technologies Inc. and its Affiliates**

Address:

- **Hubilo Technologies Inc., 505 Montgomery Street, 10th floor, San Francisco, CA 94111**
- **Hubilo Softech Private Limited, Block - A-2301, Privilon, Bh. Iscon Temple, Ambli-Bopal Road, SG Highway, Ahmedabad, India – 380054**

Contact person's name, position and contact details: **Srishti Tripathy, Data Protection Officer, privacy@hubilo.com, srishti@hubilo.com**

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): **Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred-

Customer Personal Data

Categories of personal data transferred-

Customer's Personal Data:

Customer Business Representative - Name, Contact Information (email, phone, etc.), Business Card Details (company, position, etc.)

End Users/ Attendee Personal data- Name , email address, organization name, Attendee interactions during the event

Speaker Personal Data: Name , Email address, Organization name and Designation

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.

NOT APPLICABLE

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

As necessary for the performance of this Agreement transfer happens on a continuous basis.

Nature of the processing

As identified in this Agreement and/ or the Service Agreement by and between the data exporter and data importer.

Purpose(s) of the data transfer and further processing

As identified in this Agreement and/ or the Service Agreement by and between the data exporter and data importer.

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

3 years post termination of contract with the customer

For transfers to (sub-) processors, also specify

subject matter- ***As identified in this Agreement and/ or the Service Agreement by and between the data exporter and data importer.***

nature- ***As identified in this Agreement and/ or the Service Agreement by and between the data exporter and data importer.***

duration of the processing-***As identified in this Agreement and/ or the Service Agreement by and between the data exporter and data importer.***

C. COMPETENT SUPERVISORY AUTHORITY

…

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA[S1]

1. Information Security Program

Hubilo is ISO 27001, ISO 27701, ISO 27018, and ISO 27017 , SOC 2 Type 2 certified organization and has implemented and maintains appropriate technical and organizational measures designed to protect Customer Personal Information as required by Applicable Data Protection Law(s) across the globe. Further, Hubilo agrees to regularly test, assess, and evaluate the effectiveness of its Information Security and Privacy Program to ensure the security and privacy of the data Processing.

2. Encryption

- All data flow in data pipelines is encrypted using a secure channel like TLS1.2+/SSL 3.0/ HTTPS. Data at rest is encrypted using AES 256 standard (one of the strongest block ciphers available).
- Data whether at rest or in motion is completely encrypted by using industry standard AES-256 encryption algorithm at rest and in transit uses SHA-256 with RSA encryption. All the static files stored on AWS S3 are using AES-256 encryption.
- Hubilo has a password masking technique for the data lifecycle to ensure a secure key management process. All user passwords are encrypted using Bcrypt.

3. Application Security

- The Hubilo development team is trained on OWASP Secure Coding Practices and uses industry best practices for building secure applications.
- The Hubilo security team conducts Whitebox testing on each code release and they also do Blackbox testing on third-party software to mitigate risk. Apart from this Hubilo also performs code scanning using Sonarqube in QA environment. Hubilo Security team uses Burp Suite Professional software to test for all vulnerabilities from time to time as per Hubilo policies and procedures.

- Hubilo code is stored in a code repository system hosted by our cloud data centre provider. Hubilo adopts a strict, least access privileges principle for access to the code. Commits to production code are strictly reviewed, and approval is restricted to just CTO/Sr. VP of Engineering / Lead-DevOps, (after passing Unit Testing and QA in Test and Staging).
- The data stored on production servers is accessible only to the CTO/Sr. VP of Engineering/ Lead-DevOps of the org. No other workforce member of Hubilo has access to customer data unless access permission is granted by the CTO/Sr. VP of Engineering to resolve any technical issue or for debugging.
- The Hubilo production environment is logically segregated from the staging and development environment with concepts of virtual private cloud and subnets. There is an hourly backup of the database data at secured cloud storage of cloud service provider (AWS).
- Connection to the Hubilo web-app via HTTPS by using the latest version of Transport Layer Socket (TLS) like TLS 1.2+ and above.

4. Application Access

- Role-based access and least access privileges principle provision while creating an account to ensure an appropriate level of access to the Hubilo account
- Hubilo supports Single Sign-On (SSO) through SAML 2.0 for all attendees
- Provision to enable email alerts whenever specific activities take place in a customer's account.
- Provision to sign out all other logged-in sessions
- Provision to disable/delete users
- Auto-logout of a user if the Password is changed in any other session or if the user is disabled/deleted
- Session Management: Every time a Hubilo user signs in to the Hubilo account, the system assigns a new session identifier for the user. The session identifier is a 64-byte random generated value to protect the account against brute force attacks
- Encryption of users passwords using bcrypt

5. Infrastructure and Network Security

- Since the Hubilo platform is hosted on AWS, numerous security controls are implemented using AWS Managed Services like AWS GuardDuty, AWS Shield, AWS Inspector, and AWS WAF, along with AWS CloudWatch and AWS CloudTrail. These managed services help Hubilo to have robust Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) in both Production and Non-Production

environment. Notifications from these tools are sent to the Hubilo Security Team so that they can take appropriate action. Hubilo has also implemented Application Performance Management (APM) Tool which provides us real time notification of any changes/ amendments to the production and non-production environment.

- We have implemented the CrowdStrike Falcon Intelligent End-point Detection and Response (EDR) on our public facing critical systems both in production and non-production environments and regularly monitors them.
- Hubilo regularly updates network architecture schema and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.
- Access to Hubilo servers requires the use of a VPN with Multi-factor authentication and extensive access monitoring.

6. Operational Security

- Hubilo runs an annual training program for its employees to treat data protection and security as the highest priorities. Hubilo is committed to implement tighter security standards across policies, procedures, technology, and people on an ongoing basis.
- Hubilo runs Vulnerability Assessment Penetration Testing (VAPT) on a quarterly basis through a third-party service provider, Grant Thornton LLP, who is globally empaneled with Computer Emergency Response and operate
- Applications and servers are regularly patched to provide ongoing protection from exploits with the help of a robust Change Management process in place.
- Hubilo has a disaster recovery strategy in place, which is tested on a yearly basis. Under any DR condition, our customer's websites will not get affected and will work fine. Though the data collection might get stopped until Hubilo services are restored.
- All of Hubilo's customer data is hosted in a secure cloud data centre service provider (AWS) and also logically segregated by the Hubilo application.

ANNEX III TO THE STANDARD CONTRACTUAL CLAUSES

LIST OF SUB-PROCESSORS

List of Hubilo Sub-processors:

- https://www.hubilo.com/sub-processors

---

[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 C(2021) 3972 final.

[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.

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

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

UK INTERNATIONAL DATA TRANSFER ADDENDUM

To the extent that Hubilo is a recipient of Personal Data governed by UK GDPR in a country that is not recognized as providing an adequate level of protection for Personal Data as described in the UK GDPR, the Parties agree to abide by the EU SCCs together with the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force March 21, 2022): https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

The UK Addendum is incorporated into the Addendum by reference. Capitalized terms used but not defined in this addendum will have the meaning provided in the Addendum and the DPA.

The UK Addendum is deemed completed as follows:

(a) Hubilo is acting as the Importer and Customer is acting as the Exporter. The same will be populated in the UK Addendum (attached above) in Table 1 of the Addendum.

(b) The Parties agree the UK Addendum is appended to the EU SCCs and will be detailed in Table 2 of the UK Addendum.

(c) The parties agree to populate table 3 in accordance with the EU SCC.

(d) The Parties elect that neither party may end the UK Addendum with respect to Section 19 of the UK Addendum.