Bynder Data Processing Addendum

This Data Processing Addendum, including its Schedules, ("DPA") supplements and forms an integral part of the agreement as governed by the Bynder standard terms of service (v.14) available at www.bynder.com/en/legal ("Terms") or any other agreement between Customer and the applicable Bynder contracting entity ("Bynder") governing the use and access of the Product ("Agreement"). This DPA reflects the parties' agreement with regard to the Processing of Personal Data by Bynder on behalf of the Customer in connection with the Product. Unless otherwise defined in this DPA or the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 1 of this DPA.

1. Definitions.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.
"**Customer**" means the legal entity that is a party to the Agreement with Bynder.
"**Data Protection Legislation**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement.
"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.
"**EEA**" means the European Economic Area.
"**GDPR**" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
"**Personal Data**" means any information relating to an identified or identifiable natural person where such data is Processed by Bynder on behalf of Customer.
"**Processing**" (and all verb tenses) means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.
"**Sub-Processor**" means a Processor engaged by Bynder.
"**Standard Contractual Clauses**" means Schedule 4 attached to and forming part of this DPA pursuant to the European Commission Decision C(2010)593 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.
"**Supervisory Authority**" means an independent public authority which is established by an EU member state pursuant to the GDPR.

2. Processing of Personal Data.

2.1 Scope, Roles and Details of the Processing. This DPA, including any Schedules, applies when Personal Data is processed by Bynder pursuant to the Agreement. Regarding the Processing of Personal Data, Customer is the Controller, Bynder is the Processor and Bynder will engage Sub-Processors pursuant to the requirements set forth in Section 6 below. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 to this DPA.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Product, Process Personal Data in accordance with the requirements of Data Protection Legislation, including any applicable requirement to provide notice to Data Subjects of the use of Bynder as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Legislation. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Product will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3 Bynder Processing of Personal Data. Bynder shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); and (ii) Processing initiated by Users in their use of the Product.

3. Instructions.

3.1 Customer Affiliates. Customer represents that it is authorised to give data processing instructions to Bynder and to otherwise act on behalf of any Customer Affiliates under this DPA.

3.2 Documented Instructions. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement with Bynder for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately and in writing.

3.3 Exception. If Bynder is required by law to conduct additional processing, it shall inform Customer of that legal requirement before Processing, unless such notification is prohibited by law.

3.4 Instructions likely to violate Data Protection Legislation. If, in Bynder's opinion, Customer's instructions are either likely to violate Data Protection Legislation, Bynder is entitled to refuse to follow such instructions and shall inform Customer of the reasons for its refusal. In such cases, Customer shall provide alternative instructions in a timely manner and Bynder may cease all Processing of the impacted Personal Data (other than secure storage thereof) until it receives acceptable instructions.

4. Bynder Personnel.

4.1 Confidentiality Obligations. Bynder ensures that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, and have executed written confidentiality agreements.

4.2 Limited Access. Bynder ensures that Bynder's access to Personal Data is limited to those personnel performing services in accordance with the Agreement.

4.3 Data Protection Officer. Bynder has appointed a data protection officer ("DPO"). The appointed DPO may be reached at privacy@bynder.com.

5. Security of Processing.

5.1 Measures. Bynder has implemented and shall maintain appropriate technical and organisational measures to protect Personal Data against accidental, unauthorised, or unlawful destruction, loss, alteration, disclosure, and access ("Security Measures"), as described in Schedule 3 of this DPA, including as appropriate:

a. the pseudonymisation and encryption of Personal Data;
b. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems;
c. subject to the Service Level Agreement, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d. the regular testing, assessment, and evaluation of the effectiveness of the Security Measures.

5.2 Customer has made an independent determination as to whether these Security Measures meet the Customer's requirements.

5.3 Third Party Certifications. Bynder has obtained third party certifications as set forth in Schedule 3 of this DPA. Upon Customer's written request, but not more than once per year, and subject to the confidentiality obligations set forth in the Agreement, Bynder shall make available to Customer a copy of Bynder's then most recent third-party certification and audit report, as applicable.

6. Sub-Processors.

6.1 General Authorization. Customer agrees that Bynder may use Sub-Processors to fulfil its contractual obligations under this DPA or to provide certain services on its behalf.

6.2 Sub-Processor Obligations. Bynder will enter into a written agreement with the Sub-Processor and, to the extent that the Sub-Processor is performing the same Processing activities that are being provided by Bynder, Bynder will impose on Sub-Processors data protection obligations not less protective than those in this DPA.

6.3 Sub-Processor List. Bynder currently uses the Sub-Processors listed in Schedule 2 to this DPA. A list of Sub-Processors is also available on Bynder's website at www.bynder.com/sub-processors/ ("Sub-Processors Page"). Bynder will update the Sub-Processors Page with any new Sub-Processor and notify Customer at least 7 calendar days before such Sub-Processors will begin to Process Personal Data.

6.4 Objection Right. Customer may object to the use of a new Sub-Processor on a reasonable and legitimate basis. In the event Customer objects to a new Sub-Processor, Customer shall provide written notice to privacy@bynder.com within the 7 calendar day notice period set out in Section [6.3] outlining Customer's specific concerns about the new Sub-Processor in order to give Bynder the opportunity to address such concerns. Bynder may, at its sole discretion, (i) not appoint the Sub-Processor and/or propose an alternate Sub-Processor; (ii) take the steps to address the Customer's specific concerns and obtain Customer's written consent to use the Sub-Processor; or (iii) make available to Customer the Bynder Product(s) without the particular aspect that would involve use of the objected-to Sub-processor. If Bynder is unable or determines in its reasonable judgement, that it is commercially unreasonable to do any of the options in Section 6.4 (i)-(iii), Customer may terminate the Agreement in accordance with section 19.3 of the Terms.

6.5 Liability. Bynder will remain responsible for the performance of a Sub-Processor to the same extent Bynder would be responsible if performing the services of each Sub-Processor directly under the terms of this DPA.

7. Rights of Data Subject.

Bynder will, to the extent legally permitted, notify Customer without undue delay if Bynder receives a request from a Data Subject to exercise the Data Subject's rights set forth in Data Protection Legislation, especially Chapter III of GDPR ("Data Subject Request"). Taking into account the nature of the Processing, Bynder will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to Data Subject Requests under Data Protection Legislation. To the extent Customer is unable to address a Data Subject Request, Bynder will upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request. To the extent legally permitted, Customer will be responsible for any costs arising from Bynder's provision of such assistance.

8. Assistance.

Taking into account the nature of Processing and the information available to Bynder, Bynder will provide reasonable assistance and cooperation to Customer in respect of its relevant obligations under Articles 32 to 36 GDPR. To the extent legally permitted, Customer will be responsible for any costs arising from Bynder's provision of such assistance.

9. Personal Data Breach Notification.

Bynder will notify Customer without undue delay, but always within 48 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Bynder or its Sub-Processors of which Bynder becomes aware ("Personal Data Breach"). Notification of Personal Data Breaches, if any, will be delivered by email at the email address specified for notices in the applicable Order Form, if no email address is specified, to one or more of Customer's Product administrators. Bynder's obligation to notify Customer of a Personal Data Breach is not an acknowledgement by Bynder of any fault or liability with regard to the Personal Data Breach. The obligations under this Section 9 do not apply to incidents that are caused by Customer or its Users.

10. Return and Deletion of Personal Data.

10.1 Upon Customer's request to privacy@bynder.com Bynder will return or delete Personal Data in accordance with the timeframes specified in the Agreement, unless European Union law or the laws of a EU member state requires that Bynder retains the Personal Data. Bynder may delete Personal Data six months after termination or expiration of the Agreement. Bynder shall dispose Personal Data in accordance with the latest method(s) of data sanitizing, as detailed in NIST 800-88 ("Guidelines for Media Sanitization").

10.2 Notwithstanding anything to the contrary in this DPA, Bynder may retain Personal Data if and for as long as required by law.

10.3 Personal Data stored in Bynder's auto-backup or archival systems will be deleted automatically after 180 days after back-up, or otherwise as soon as technically possible.

10.4 If Customer provides Personal Data on a hard drive or other forms of removable media, such removable media must be encrypted or password protected. In collaboration with Customer, Bynder shall either return the removable media to Customer, or securely destroy such removable media by using a certified third party. A certificate of destruction can be made available to Customer upon request.

11. Customer Audits.

11.1 Summary Report of Internal Audit. In addition to Section 5.3, Bynder will on a regular basis audit the security of the systems that it uses to Process Personal Data. Upon Customer's written requests, Bynder will make available to Customer a summary of the results of this audit ("Summary Report") to demonstrate compliance with the obligations under this DPA.

11.2 Customer Audit. If Customer substantiates that the Summary Report cannot satisfactorily demonstrate Bynder's compliance and that it has a justifiable suspicion that Bynder is in breach of this DPA, Customer may conduct an audit on Bynder's premises, not more than once per year, and subject to the confidentiality obligations set forth in the Agreement and following conditions:

a. Customer must provide at least 30 days' prior written notice to privacy@bynder.com. Such notice must indicate the reasons for the audit request, and will be effective upon Bynder's confirmation of receipt;

b. Audits will be conducted within a mutually agreed scope, duration, and timing; performed by Customer, or a third party that is pre-approved by Bynder, such approval not to be unreasonably withheld; and conducted within Bynder's normal business hours and with best efforts taken to avoid disruption of Bynder's business operations;

11.3 Cost. The cost of an audit on Bynder's premises will be borne by Customer, unless a Material Breach (as defined in the Agreement) of this DPA is found, in which case Bynder will bear the costs.

11.4 Nothing in this Section 11 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

12. Transfers of Personal Data to Third Countries.

12.1 Regions. Customer may specify the location where Customer Data, including Personal Data, will be Processed in the Agreement ("Region"). Except as necessary to provide the Product and services initiated by Customer, or as necessary to comply with the law, Bynder will not transfer Personal Data from Customer's selected Region. A transfer to a third country shall take place only if the conditions of Chapter V. GDPR are complied with.

12.2 Application of Standard Contractual Clauses. Bynder will enter into Standard Contractual Clauses with each affiliate and/or Sub-Processor where the Processing of Personal Data is transferred outside the EEA, either directly or via onward transfer, to any third country not recognized by the European Commission as providing an adequate level of protection for Personal Data. Customer hereby authorises Bynder to enter into Standard Contractual Clauses (also) on its behalf and commissions Bynder to enforce them against the relevant Sub-Processor on the Customer's behalf where appropriate. The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA.

12.3 Order of precedence. If the Standard Contractual Clauses apply, nothing in this Section 12 varies or modifies the Standard Contractual Clauses.

13. Limitation of liability.

Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

14. Entire Agreement, Hierarchy.

Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will take precedence to the extent of such conflict.

15. Term and termination.

This DPA shall enter into force at the same time as the Agreement and shall automatically terminate upon any termination or expiration of the Agreement.

16. List of Schedules.

Schedule 1: Details of the Processing of Personal Data
Schedule 2: List of Sub-Processors and Bynder Entities
Schedule 3: Security Measures
Schedule 4: Standard Contractual Clauses

Schedule 1: Details of the Processing of Personal Data

Nature and Purpose of Processing
Bynder will Process Personal Data as necessary to provide the Product pursuant to the Agreement and as further instructed by Customer in its use of the Product.

Duration of Processing
Subject to Section 10 of this DPA, Bynder will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects
Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole Personal Data required for the use of the Product relates to the following categories of Data Subjects:

- Employees of Customer
- Customer's Users

Types of Personal Data
Customer may store Personal Data in the Product, the extent of which is determined and controlled by Customer in its sole discretion. The sole categories of Personal Data required for the use of the Product are:

- First and last name
- Email address

Special categories of data
Customer may not store special categories of data in the Product(s). The Product is not intended for Customer to store sensitive categories of data, which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal data relating to criminal convictions and offences.

Schedule 2: Sub-Processors and Bynder Entities

Infrastructure provider
Bynder engages the following Sub-Processor(s) to host and store Customer Data.

Entity name	Sub-Processor activity	Entity country
Amazon Web Services EMEA SARL	Cloud Service Provider	Luxembourg
Google Ireland, Inc.	Cloud Service Provider (for Video Brand Studio only)	Ireland

Other Sub-Processors
Bynder works with certain third parties, as listed below, to provide specific functionalities within the Product(s). In order to provide the relevant functionality these Sub-Processors access Customer Data. Their use is limited to the indicated activities:

Entity name	Sub-Processor activity	Entity country
Pricon BV	Pricon is a call centre that assists Bynder with the provision of phone support outside office hours.	Netherlands
Zendesk Inc.	Zendesk provides a cloud-based system for tracking and solving customer support tickets.	United States
Drift.com Inc.	Drift allows direct communication with the Customer within the Product(s).	United States

Bynder also engages the following Sub-Processors to support the Video Brand Studio module:

Entity name	Sub-Processor activity	Entity country
Google Ireland, Inc.	Google also provides a performance and diagnostics tool to monitor and measure the health of Google resources and applications.	Ireland
FileStack, Inc.	FileStack supports the upload of Customer Data in the Video Brand Studio module.	United States

Bynder entities
The following entities are part of the corporate structure of Bynder. Depending on the geographic location of the Customer, Bynder may also engage one or more of the following entities as Sub-Processors.

Entity name	Entity type	Entity country
Bynder B.V.	Parent company	Netherlands
Bynder LLC	Subsidiary	United States
Bynder Ltd.	Subsidiary	United Kingdom
Bynder Software FZ-LLC	Subsidiary	Dubai
Bynder Software SL	Subsidiary	Spain

Content Deliver Networks ("CDN")
Bynder may use CDN to assist with the delivery of the Product(s). CDNs do not have access to Customer Data itself, but are systems commonly used to provide fast delivery of content based on the geographic location of the individual accessing the content and the origin of the content provider:

CDN Provider	CDN Location
Amazon Web Services EMEA SARL	Global

Schedule 3: Security Measures

Bynder will implement and maintain the following Security Measure to adequately protect Customer's Personal Data. Customer understands and agrees that these Security Measures are subject to technical progress and development and Bynder is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in this Schedule 3 is maintained:

1. Technical measures

1.1. Access control. Bynder shall prevent unauthorized access to data processing systems. Personnel shall only have access to Customer data when it's necessary for them to perform their job. Customer data shall not be read, copied, modified or deleted without authorization.
1.2. Entry control. Bynder shall prevent that data processing systems can be accessed by unauthorized parties.
1.3. Logging control. Bynder shall ensure that all events in the data processing systems can subsequently be checked.
1.4. Transmission control. Bynder shall ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transmission.
1.5. Data at rest. Bynder shall ensure the appropriate encryption of data at rest.
1.6. Separation control. Bynder shall ensure that data collected for various purposes are processed separately.
1.7. Reliability control. Bynder shall ensure that all functions of the data processing system are available and occurring malfunctions are notified.
1.8. Integrity control. Bynder shall ensure that stored Personal Data cannot get damaged by malfunctions of the system or that damaged data can be replaced by the original and correct data.
1.9. Availability control. Bynder shall ensure that Personal Data is protected against unintentional destruction or loss and therefore available for the Customer.

2. Organisational measures

2.1 Admission Control. Bynder shall prevent unauthorized persons from gaining access to Bynder premises.
2.2 Security and awareness training. Bynder shall maintain a security awareness program that includes the appropriate training of personnel on Bynder's security policies.
2.3 Personnel screening. Criminal background checks shall be performed for all employees before hiring. Additionally, Bynder will ensure that all employees have executed written confidentiality agreements.
2.4 Information security management process. Bynder shall maintain an ISO 27001:2013 certified information security management system.
2.5 Business continuity management process. Bynder shall maintain a business continuity management system that defines the processes and procedures in the event of a disaster, including the testing and reviewing of the disaster recovery plans.
2.6 Regular evaluation of Security Measures. Bynder shall ensure a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure a level of security appropriate to the risk of processing.

3. Third Party Certifications

Bynder currently holds and maintains the following certifications:

- ISO 27001:2013
- ISO 27018:2014
- ISO 22301:2012

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity defined as **Customer** in the DPA

(the data **exporter**)

And

Name of the data importing organisation: **Bynder LLC**

Address: 321 Summer Street, Boston MA 02210, USA

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

1 Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor

which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

3 This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is the legal entity specified in as Customer in this DPA.

Data importer
The data importer is Bynder LLC.

Data subjects
As provided in Schedule 1 in the DPA.

Categories of data
As provided in Schedule 1 in the DPA.

Special categories of data (if appropriate)
As provided in Schedule 1 in the DPA.

Processing operations
The objective of Processing of Personal Data by data importer is the performance of this DPA as necessary to provide the Product pursuant to the Agreement, and as further instructed by Customer in its use of the Product.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will implement and maintain the technical and organizational measures to adequately protect the data exporter's Personal Data as further described in Schedule 3 of this DPA. Data exporter understands and agrees that these technical and organizational measures are subject to technical progress and development and Bynder is therefore expressly allowed to implement adequate alternative measures as long as the general security level described in Schedule 3 of this DPA is maintained.