Content Workflow Standalone Data Processing Addendum

This Content Workflow Standalone Data Processing Agreement, including its Schedules, ("DPA") supplements and forms an integral part of the Content Workflow Standard Terms of Service available at https://www.bynder.com/en/legal/content-workflow-standalone-terms-of-service/ ("Terms") between Customer and Bynder Ltd. ("Bynder") governing the use and access of the "Content Workflow Standalone" subscription service ("Product"). 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 Terms, 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 Terms with Bynder.

"Data Protection Legislation" means all laws and regulations applicable to the Processing of Personal Data under the Terms.

"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 (a) where the GDPR applies, the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 202, or (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022.

"Supervisory Authority" means an independent public authority established or recognized under Data Protection Laws.

"UK GDPR" means the Data Protection Act 2018, as well as 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 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

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 Terms. 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 Terms; 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 Terms are Customer's complete and final documented instructions at the time of signature of the Terms 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 Terms.

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 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 applicable service levels, 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 Terms, 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. Bynder will update the Sub-Processors 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 Terms in accordance with 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 Terms, 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 Terms, 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 Terms. 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 90 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 Terms 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 Terms) 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 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. The Standard Contractual Clauses will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA..

12.2 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.

13.1 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 Terms, 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 Terms and all DPAs together.

14. Entire Agreement, Hierarchy.

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

Bynder reserves the right to amend this DPA from time to time and will post a message on its homepage along with the new version of the DPA if that happens.

15. Term and termination.

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

16. List of Schedules.

Schedule 1: Details of the Processing of Personal Data
Schedule 2: Sub-Processors and Bynder Entities
Schedule 3: Security Measures

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 Terms 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 Terms, 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

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:

- Amazon Web Services Inc., Cloud Service Provider, United States
- Appcues Inc, In-app training, United States
- Intercom R&D, Customer support and in-app notifications, Ireland

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.

- Bynder BV, Parent Company, Netherlands
- Bynder LLC, Subsidiary, United States
- Bynder Ltd, Subsidiary, United Kingdom
- Bynder Software FZ-LLC, Subsidiary, Dubai
- Bynder Software SL, Subsidiary, Spain
- Bynder Pty LTD., Subsidiary, Australia

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.

Third Party Certifications

Bynder currently holds and maintains the following certifications:

- ISO 27001:2013
- ISO 27018:2019
- ISO 22301:2019