Bynder's Artificial Intelligence Policy

This Artificial Intelligence Policy ("AI Policy") applies to Customer's use of Bynder products and/or services (the "Product") that incorporate artificial intelligence capabilities ("AI Features"). This AI Policy is intended to provide Customers with additional information regarding Bynder's handling of Customers' data and provides guidelines for Customers' use of AI functionalities within the Product, including data handling and privacy considerations.

1. Definitions

1.1. "AI" means Artificial Intelligence.

1.2. "AI Features" means features powered by AI bringing the capability to analyse data, make predictions, automate tasks or generate content, and that may be purchased and used as part of Customer's subscription for the Product, at Customer's sole discretion.

1.2. "Applicable Law" means, as the case may be, the EU AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2017/2109), the GDPR, (the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC), state and/or federal laws that govern or regulate the use of AI Features within the United States of America, or any other legislation or regulation applicable to the use by the Customer of AI functionalities within the Product.

1.3 In the context of personal data processing, Bynder shall be the "Processor" and/or "Service Provider," and Customer shall be the "Controller," as the term is defined under applicable privacy law.

1.4. "Customer Data" or "Customer Content" means electronic data, text, documents, pictures, videos, or other materials uploaded to, generated and/or stored within the Product by Customer and Users.

1.5. Any capitalized terms used but not defined herein shall have the meaning assigned to them in the relevant Applicable Law.

2. Responsible AI Requirements.

2.1. AI Features proposed by Bynder are designed, developed, and deployed in a way that allows for effective human oversight, preserving human autonomy and ensuring that human beings remain in control of decision-making processes.

2.2. Bynder will keep Customer informed of the upstream AI systems and/or AI models used for providing the proposed AI Features.

2.3. AI Features proposed by Bynder are designed to streamline content operations, accelerate time-to-market, and enhance brand consistency. They also improve efficiency, reduce costs, and enable easier and more accurate content discovery. Bynder shall communicate to Customer, at Customer's first request, the specific intended use of each AI Feature. Customer will use the AI Features for such intended use. None of the AI Features are intended for use qualifying as prohibited activity or high-risk use under Applicable Law. In particular, Customer will not

2.3.1. submit inputs that could reasonably be interpreted as abusive, defamatory, deceptive, false, misleading into Bynder's artificial intelligence features ("AI Features") or provide instructions intended

to produce such outputs;

2.3.2. generate through the AI Features content that could cause reputational, legal, or economic harm to others, including but not limited to impersonation, deepfakes, disinformation, or biased, discriminatory, or otherwise harmful outputs;

2.3.3. use AI Features in any application involving autonomous decision-making, life-critical systems, or the operation of dangerous machinery without appropriate fail-safes and human-in-the-loop safeguards;

2.3.4. attempt to reverse engineer, extract, or otherwise access the underlying models, datasets, training techniques, or other proprietary AI components used in the Product, or intentionally circumvent safety filters and functionality or encourages model to act in a manner that violates this Policy or applicable law ;

2.3.5. develop, train, or fine-tune competing AI models or labels or annotate data for training of third-party AI system;

2.3.6. fail to disclose where content has been materially generated or modified by AI Features, particularly where such content may reasonably be interpreted as human-authored;

2.3.7. involve, promote or use in a manner that is intended to support activities that are prohibited or considered high risk under Applicable Law, including biometric categorization according to sensitive or protected attributes or characteristics or for emotion recognition.

2.3.8. submit personal, sensitive, or protected information (including special categories of personal data under GDPR or similar regimes) into the AI Features unless expressly permitted and subject to proper safeguards.

3. Biometric Data

As used in this AI Policy, "Biometric Data," means any Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow for or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

3.1 Facial Recognition and Auto tagging

At Bynder, our AI facial recognition feature, served through AWS Rekognition, is designed to enhance user experiences within the Product. AI facial recognition feature accurately detects and locates faces in various media files and provides users with a convenient tagging system, enabling the seamless search of assets within the Product. To ensure data security and privacy, facial vectors used are meaningless on their own and cannot be reverse engineered, as they are stored in encrypted form.

3.2 AI facial recognition feature serves several key purposes within the Product: (i) minimising manual work by adding name tags to uploaded images (automatic tagging), (ii) optimising the findability of assets, (iii) detecting faces, (iv) characterising faces, (v) celebrity recognition, and (vi) facilitating data protection compliance and aiding users in quickly finding content related to Data Subject requests.

3.3 Bynder shall ensure that Biometric Data processed within the Product as part of the AI Features are processed in compliance with the Data Processing Addendum in force between the Customer and Bynder. In particular, Bynder will use reasonable care to store, transmit and protect from unauthorised disclosure any Biometric Data in its control, and shall store, transmit, and protect from unauthorised disclosure all Biometric Data in its control using the same standard of care in which Bynder stores, transmits, and protects its own personally identifiable information but in no case less than a reasonable standard of care in compliance with Applicable Law.

3.4 It is Customer's responsibility to deploy the AI features, and AI facial recognition features in particular in a secure, responsible and confidential manner, in accordance with Applicable Law . Customer shall advise its users regarding

the processing of users' Biometric Data, as provided herein, and shall ensure that it has the appropriate approvals in place prior to collecting, storing, and/or using such Biometric Data within the Product.

4. Service Improvement

4.1. Bynder is committed to carry out periodic checks on the accuracy of its recommendations towards the Customer on the use of the suggested AI Features.

4.2. Bynder ensures traceability, including in relation to datasets and processes during the AI system life cycle, to enable analysis of the AI system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.

4.3. Bynder will apply a systematic risk management approach to each phase of the AI Features life cycle on a continuous basis to address risks related to these AI Features, including privacy, digital security, safety and bias, in accordance with Applicable Law.

5. Security Requirements

Bynder shall maintain and frequently review policies for information security which include administrative, physical and technical safeguards required to ensure the confidentiality, integrity, availability and continuity of the Product, in accordance with the security requirements set forth in the SOW.

6. Changes to this AI Policy

Please become acquainted with this AI Policy. This AI Policy is formally reviewed annually and is updated as often as necessary. Updates will be posted publicly on the Website. If we make material changes to the purposes and policies set out here, we will update this page and inform Customer by email or in-application notification. Furthermore, should you encounter any concerns regarding the functionality of our AI features, please do not hesitate to contact our dedicated support team following the procedure described in the SLA.