Bynder's Artificial Intelligence Privacy Policy

This Artificial Intelligence Privacy Policy ("AI Policy") applies to Customers' use of Bynder products and/or services (the "Product") that incorporate artificial intelligence capabilities, as further set forth in a Customer's subscription agreement relating to the Product (the "Agreement"). This AI Policy is intended to provide Customers with additional information regarding Bynder's handling of Customers' Personal Information and guidelines for Customers' use of AI functionalities within the Product, including data handling and privacy considerations.

1. Definitions

1.1. "AI" means Artificial Intelligence. AI features may be purchased and used as part of Customer's subscription for the Product, as further detailed in the Agreement. AI features are intended for use in analysing data, making predictions, and automating tasks.

1.2. For purposes of this AI Policy, Bynder shall be a "Processor" and/or "Service Provider," as the terms are defined under applicable privacy law.

1.3. For purposes of this AI Policy, Customer shall be the "Controller," as the term is defined under applicable privacy law.

1.4. "Customer Data," 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 terms used but not defined herein, such as "Personal Data", "Sensitive Personal Data", "Data Subject" and "Data Subject Request" shall have the meaning given to them in accordance with the Agreement and/or the applicable privacy laws, including, but not limited to 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 (the "GDPR").".

2. Human Oversight of AI

By using AI features in the Product, Customer acknowledges and agrees that any action or decision that may impact an individual's privacy rights (for example, the application of tags and other metadata to an individual's photograph or recorded likeness) shall be subject to human oversight and intervention as needed. Under GDPR and other applicable privacy laws, individuals have the right to not be subjected to decisions solely based on automated processing (including "profiling") that may affect their privacy rights. Customer shall comply with applicable laws and regulations in its use of AI features.

3. Compliance with Laws: Customer Data Subjects' Rights

3.1. In accordance with GDPR and other applicable laws and regulations, Customer, as the Controller of Personal Data processed using Bynder's AI features, understands and acknowledges its requirement to fulfill Data Subjects' requests related to assets uploaded by Customer and its end users. This includes providing Data Subjects with (i) clear and comprehensive information regarding how Personal Data is processed; (ii) access to Personal Data held by Customer, with the right to request corrections for any inaccuracies; (iii) the option to receive Personal Data in a standard electronic format; (v) the right to object to the processing of Personal Data by Customer and to prevent exclusive reliance on automated decision-making or profiling; (vi) the ability to impose restrictions on the processing of data subjects' Personal Data or request its deletion by Customer; and (vii) the right to be informed about the sale or sharing of Personal Data as well as the opportunity to opt out.

3.2. Bynder, in accordance with GDPR and other applicable laws and regulations, will assist Customer in fulfilling Data Subjects' access requests, as outlined in Section 3.1 above. Bynder will offer necessary support and information to enable the Customer to meet its obligations and ensure compliance with applicable regulations. Upon Customer's written request, Bynder may additionally provide Customer with the option to complete a Data Protection Impact Assessment (DPIA) pertaining to any AI features that may be connected to a Data Subject's access request.

4. 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.

The following Section 5 shall apply only when Customer has purchased and implemented AI "facial recognition" features for the Bynder Product. These features are anticipated to be available in early 2024.

5. Biometric Data (Facial Recognition)

5.1. 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.

5.2. Customers are responsible for developing and complying with their own "Biometric Data retention policies," as may be required under applicable law and regulation.

5.3. Biometric Data may constitute "Sensitive Personal Data" under GDPR and other applicable privacy laws. Accordingly, Bynder shall use reasonable care to store, transmit and protect from unauthorised disclosure any Biometric Data it processes, and shall store, transmit, and protect from unauthorised disclosure all Biometric Data using the same standard of care with which Bynder stores, transmits, and protects its own personally identifiable information, taking all reasonable measures to comply with applicable laws and regulations.

5.4 Customer shall advise its users regarding the collection, use, storage and disclosure 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 the such Biometric Data within the Product.

5.5. Upon termination and/or expiration of the Agreement, Bynder shall comply with the data retention and deletion provisions set forth in the applicable Data Processing Addendum ("DPA"), including with respect to Biometric Data.

6. Changes to this AI Policy

This AI Policy will be subject to formal review annually, and updated 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 Customers by email or in-application notification. Customers with questions regarding this policy or the functionality of our AI features should contact their Customer Success Manager for prompt assistance and clarification.