Hedra Biometric Data Privacy Policy

Hedra, Inc. ("**Hedra**", "**we**", "**us**" or "**our**") provides a platform to its users, which includes desktop, web, and mobile applications, as well as tools driven by artificial intelligence (the "**Hedra Platform**"). Through or in connection with the Hedra Platform, Hedra may process, derive or otherwise possess biometric data, as defined below. This Biometric Data Privacy Policy applies to Hedra's processing of such biometric data from or regarding our users.

Hedra may also offer services, including the Hedra Platform or parts of the Hedra Platform, to its business customers. This Biometric Data Privacy Policy does not apply to biometric data we process on behalf of our business customers (e.g., where our business customers provide or make available to Hedra biometric data concerning their own customers or end users). We use biometric data we receive from our business customers solely on the instructions of our business customers, as governed by our agreements with those business customers. If you have concerns regarding biometric data we process on behalf of one of our business customers, please direct your concerns to that customer.

1. Biometric Data Defined

As used in this Biometric Data Privacy Policy, biometric data includes both "biometric identifiers" and, where applicable, "biometric information," as such term(s) are defined under the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. ("**BIPA**"), the Texas Capture or Use of Biometric Identifiers Act, Tex. Bus. & Com. Code Ann. § 503.001 ("**CUBI**"), or the Washington H.B. 1493, RCW 19.375 ("**WA HB 1493**"), where applicable based on the user's state of residency (the "**Applicable Biometric Data Privacy Law**").

For example, under BIPA, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, but does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers under BIPA also do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. "Biometric information" under BIPA means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual, but does not include information derived from items or procedures excluded under BIPA's definition of biometric identifiers.

2. Purpose for Collection of Biometric Data

Hedra may derive, generate, collect, store and use biometric data, which may include certain scans of facial geometry, in order to provide certain features of the Hedra Platform to our users. For example, Hedra may generate facial templates in connection with the scanning of user-provided photos, videos or other images and may derive certain information from user-provided audio or voice recordings in order to create avatars and may use biometric data in order to provide certain other video, image and audio editing and animation tools and features through

the Hedra Platform. Hedra will only use this biometric data for purposes of providing the applicable features of the Hedra Platform to the user and for legal compliance purposes.

Before collecting, deriving or generating any biometric data from or regarding a user, we will obtain the user's express written consent where and as required by Applicable Biometric Data Privacy Law.

3. Disclosure of Biometric Data

Hedra may disclose biometric data to its third-party vendors only as necessary to facilitate the provision of the Hedra Platform to the applicable user.

Hedra does not share biometric data with any other third parties unless:

- The user or the user's legally authorized representative consents to the disclosure;
- The disclosure is required by applicable law or regulation or otherwise permitted by Applicable Biometric Data Privacy Law;
- The disclosure is required to complete a financial transaction requested or authorized by the user; or
- The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

4. Retention and Storage of Biometric Data

Hedra and its vendors generally retain biometric data for only as long as necessary to satisfy the purposes for collection and processing identified above. Notwithstanding the foregoing, except to the extent required by applicable law, in no event will Hedra retain a user's biometric data beyond the date that is three years following the user's last interaction with Hedra.