Au10tix – Biometric Data Policy

Policy Statement

The purpose of this policy is to explain the procedures for the collection, use, safeguarding, storage, retention, and destruction of Biometric Data used by Au10tix (the "Company"), as part of the Company's authentication and identity verification services, in accordance with applicable laws including, without limitation, the Illinois Biometric Information Privacy Act. As a part of these services, the Company uses its proprietary technology to analyze and compare facial images to verify the identity of a person and the authenticity of their identification card.

For the purpose of verifying your identity on behalf of the Company's business customer that referred you to the Company's services in connection with providing you with its own respective products and/or services (the "**Referring Business**"), the Company shall process your Biometric Data as a "data processor" (as defined under applicable law) acting on behalf of the Referring Business as the "data controller" (as defined under applicable law). In all other cases, the Company shall process your Biometric Data as the "data controller".

Each Referring Business is responsible for developing and complying with its own Biometric Data retention and destruction policies, as well as providing appropriate notice and obtaining consent from individuals, as may be required under applicable law.

Please note, once the Company finalizes the verification of your identity on behalf of the Referring Business, and subject to appropriate approval, the Company will retain your Biometric Data and process it as a "data controller" in accordance with this Biometric Data Policy and the Company's Service Privacy Notice.

Biometric Data Defined

"Biometric Data" includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, et seq, "biometric identifier" as defined under Texas. Bus. & Com. Code §503.001, "biometric identifier" as used in Washington. Rev. Code Ann. §19.375.020, "biometric information" as used in the California Consumer Privacy Act, 2018, "biometric information" as used in the New York Stop Hacks and Improve Electronic Data Security Act, "biometric data" as used in the Arkansas Code §4-110-103, and further includes any similar definitions under state or local law related to any biological characteristics of a person, or information based upon such a characteristic.

AU10TIX © 2025

“Biometric Identifier” means, as defined under BIPA, a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric Identifier has additional similar meanings under the laws stated above under the definition of Biometric Data.

“Biometric information” means, as defined under BIPA, any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. “Biometric information” has additional similar meanings under the laws stated above under the definition of Biometric Data.

Purpose for Collection of Biometric Data

The Company and its vendors may capture, receive, or otherwise obtain Biometric Data in the course of providing the Company’s products and services.

In order to deliver its services, the Company uses its proprietary technology to analyze and compare facial geometry images to verify the identity of a person and the authenticity of their identification card.

The Company and its vendors capture, receive, or otherwise obtain Biometric Data solely to provide, manage, maintain, improve and further develop the Company’s identity and authentication services (including machine learning and training of AI algorithms). Neither the Company nor its vendors sell, lease or trade any Biometric Data that it receives from, or generates on behalf of, Referring Businesses or receives from, or generates based on other data collected from, a Referring Business’s customer or another individual as a result of their use of the Company’s services.

Each Referring Business is responsible for its own compliance with applicable laws governing its collection, storage, use, and transmission of Biometric Data, including to obtain, in advance, a written authorization from each customer to collect, capture, receive, or otherwise obtain Biometric Data related to the customer, for the purposes described under this policy.

Disclosure

The Company will not disclose or disseminate any Biometric Data to anyone other than its authorized vendors who assist in providing the services, except in the following circumstances (where permitted by law):

the subject of the Biometric Data or the subject’s legally authorized representative consents to the disclosure or dissemination;

the disclosure or dissemination completes a financial transaction requested or authorized by the subject of the Biometric Data or the subject’s legally authorized representative;

AU10TIX © 2025

the disclosure or dissemination is required by State or federal law or municipal ordinance;

the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction; or

the disclosure is necessary for the Company's professional advisors (e.g., lawyers) to provide services to the Company or for the Company to complete a merger, acquisition, or other structural change.

All disclosures of Biometric Data to the Company's authorized vendors are in furtherance of the Company's services and are governed by contracts appropriate to the context of the services the authorized vendor is providing to the Company.

Retention Schedule

The Company and any authorized vendors will retain Biometric Data of a specific Referring Business's customer or other individual until the first of the following events occurs:

The initial purposes, as described under this policy, for collecting or obtaining the Biometric Data has been satisfied or storage of the Biometric Data is no longer necessary, adequate, or relevant to those purposes; or

Where the Company is acting as the "data controller", the time period prescribed by applicable law has lapsed or an individual has exercised a right to deletion; or

Where the Company is acting as the "data processor," the Company has received written notice from the Referring Business instructing the Company to delete such information, such as in the event the time period prescribed by applicable law has lapsed or the Referring Business's customer has exercised a right to deletion.

After such time, the Company and its authorized vendors will destroy the Biometric Data, unless retention is otherwise required by applicable law.

Data Storage

The Company will store, transmit, and protect Biometric Data using a reasonable standard of care within the Company's industry, and will contractually require its authorized vendors to do the same. The Company will perform such storage, transmission, and protection from disclosure in a manner that is substantially the same as or more protective than the manner in which the Company stores, transmits, and protects from disclosure other confidential and sensitive information within the Company's possession, including any sensitive personal information.

AU10TIX © 2025