Biometric Technology LLC Privacy Shield, GDPR, Website, App and Email Privacy Policies

Last Updated - July 29th, 2022

This privacy statement relates to Biometric's methods and intentions regarding how we collect, use and how you may manage any personal information you provide to us when we, in general, collect personal information, during visits to biometric.vision.

Data we may collect without your consent:

- Usage activity about how you interact with us, including content you viewed and interacted with.
- We may automatically gather information about your computer such as:
    - Your IP address
    - Browser type
    - Referring/exit pages
    - Operating system

Personally identifiable information we will collect if you provide it to us:

- Name
- Email Address
- Phone Number
- Company Name
- Information on a Photo ID
- Face Images

Information disclosure policy

We will never share your information with third parties unless you explicitly allow us to do so, and only as described in this privacy statement.

When we may disclose your information

- When required by law, such as to comply with a subpoena or similar legal request.

- When we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud or to respond to a government request.
- To another third party with your explicit, prior consent.

Site and app activity tracking

We may use cookies, pixels, beacons, scripts and other similar technologies (collectively, “cookies”) to recognize your browser, operating system or device, learn more about interests and intentions, provide you with features and services, or for additional purposes, including:

- Recognizing repeat visitors.
- Keeping track of specified preferences such as language and country of origin.
- Conducting research and diagnostics to improve our offerings.
- Preventing fraudulent activity.
- Improving security.
- Delivering relevant content.
- Reporting, measurement and analysis of our site’s performance.

If you block or reject our cookies, you might not be able to receive certain content or take advantage of certain site functionality.

Approved third parties may also set cookies when you interact with our offerings. Third parties include search engines, providers of measurement and analytics services, social media networks, and advertising companies.

You can manage browser cookies through your browser or device settings.

EU GDPR Compliance

How we collect, use and store your data

We gather the following things:

- Your IP (Internet Protocol) address, which is a set of numbers that identifies the location of a piece of hardware connected to a network, including the internet. An IP address allows a device to communicate with other devices over an IP-based network like the internet. By itself, it cannot provide the identity of the user. It is

important to us because it indicates where in the world our software is being used, which helps us better prepare the product for distribution and daily use.

- Email address provided: In the event we have questions about how you intend to use our service or what issues you might have had with it, we will use your email address only to contact you directly with questions and to send you only our own product updates if you desire.

The data may be used for the following purposes:

- To determine which products or services are most relevant to you
- To respond to service or product information requests
- To better focus marketing efforts
- To help conduct market research

Your access and options to manage your data

You have control over your information. You may do the following at your discretion:

- Request your data be erased (“The right to be forgotten”)
- Request a copy of what data is captured
- Withdraw your consent at any time
- Lodge a complaint with the authoritative body in your region

At the same time, we provide the following information about us:

- Our identity and contact information:
    - Biometric Technology, LLC.
      605 GEDDES STREET
      WILMINGTON, New Castle, DE 19805
      info@biometric.vision
- The following purposes of and legal basis for processing your data:
    - We have given explicit consent to the processing of your personal data for the specific purpose of authenticating you as the correct user, and that you are present and alive when you enroll or log in.
    - Processing your data is necessary to protect your vital interests. Our process makes it certain that no other person gains access to your confidential information.

        - Processing your data is a necessary part of the service the company we provide user authentication services for.
- The location in which we process the data:
    - The data we collect is processed in the United States.
- Who the recipients of the data are:
    - We do not send the data we collect and process to any other organization or individual.
- The period for which the data is stored:
    - We store your collected data for a time period that meets our business and development needs, and only for the purposes of a) our own ability to perform our service, and b) as reference for continued product integrity and improvement.

U.S. D.O.C. Privacy Shield Policy

Biometric Technology, LLC. ("Biometric") complies with the EU-U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the collection, use and retention of Personal Data transferred from the European Union and the United Kingdom as further described in the Scope section below. This Privacy Shield Policy outlines our commitment to the Privacy Shield Principles ("Principles") and our practices for implementing the Principles. If there is any conflict between the terms in this Privacy Shield Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

Scope

Biometric complies with the Principles with respect to the Personal Data the company receives from its Customers or their Users in the European Union and the United Kingdom in connection with the use of (i) applications downloaded to a User's mobile/web device ("Mobile/Web Applications"); and (ii) Biometric's hosted software applications (the "Service") and related support services ("Support Services") that we provide to Customers. In this Privacy Shield Policy, the Service and Support Services are collectively referred to as the "Service."

Definitions

For the purposes of this Privacy Policy:

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

“Customer” means any entity that purchases the Service.

“Customer Data” means the electronic data uploaded into the Service by or for a Customer or its Users.

“Device” means a mobile or web device.

“Personal Data” means any information, including Sensitive Data, that is (i) about an identified or identifiable individual and (ii) received by Biometric in the U.S. from the European Union or the United Kingdom in connection with the Service.

“Processor” means any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of a Controller

“Sensitive Data” means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

“User” means an individual authorized by Customer to access and use the Service.

Types of Personal Data Collected

Biometric hosts and processes Customer Data, including any Personal Data contained therein, at the direction of and pursuant to the instructions of Biometric’s Customers. Biometric also collects several types of information from our Customers, including:

- Information and correspondence our Customers and Users submit to us in connection to our Service.
- Information we receive from our business partners in connection with our Customers’ and Users’ use of the Service or in connection with services provided by our business partners on their behalf, including configuration of the Service.
- Information related to Users’ use of the Mobile/Web Applications, including geographic location data and information regarding Users’ Devices and OS identification, login credentials, language and time zone.

In addition, Biometric may collect general information about its Customers, including a Customer’s company name and address, credit card information, and the Customer representative’s contact information (“General Information”) for billing and contracting purposes.

Purposes of Collection and Use

Biometric may use Personal Data submitted by our Customers and Users as necessary to provide the Service and Mobile/Web Applications, including updating, enhancing, securing and maintaining the Service and Mobile/Web Applications and to carry out Biometric's contractual obligations to its Customers. Biometric also obtains General Information in connection with providing the Service and maintaining Biometric's relationships with its Customers.

The Biometric iOS App uses Face Data in order to create a Digital 'EZ ID' that is emailed to the User upon successful usage of the App. Biometric does not share this Face Data with 3rd Parties. The Face Data is stored on private and secure AWS servers, and will be deleted upon request.

Third-Party Disclosures

We may disclose Personal Data that our Customers and Users provide to our Service and Mobile/Web Applications:

- To business partners and service providers we use to support our Service
- In the event Biometric sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation), in which case Personal Data held by us about our Customers will be among the assets transferred to the buyer or acquirer
- If required to do so by law or legal process
- In response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements

Access

Individuals in the European Union and the United Kingdom generally have the right to access their Personal Data. As an agent processing Personal Data on behalf of its Customers, Biometric does not own or control the Personal Data that it processes on behalf of its Customers or their Users and does not have a direct relationship with the Users whose Personal Data may be processed in connection with providing the Service. Since each Customer is in control of what information, including any Personal Data, it collects from its Users, how that information is used and disclosed, and how that information can be changed, Users of the Service should contact the applicable Customer administrator with any inquiries about how to access or correct Personal Data contained in Customer Data. To the extent a User makes an access or correction request to Biometric, we will refer the request to the appropriate Biometric Customer and will support such Customer as needed in responding to any request.

To access or correct any General Information Customer has provided, the Customer should contact their Biometric account representative directly or by using the contact information indicated below.

Choice

In accordance with the Principles, Biometric will offer Customers and Users choice to the extent it (i) discloses their Personal Data to third party Controllers, or (ii) uses their Personal Data for a purpose that is materially different from the purposes for which the Personal Data was originally collected or subsequently authorized by the Customer or User. To the extent required by the Principles, Biometric also will obtain opt-in consent if it engages in certain uses or disclosures of Sensitive Data. Unless Biometric offers Customers and Users an appropriate choice, Biometric uses Personal Data only for purposes that are materially the same as those indicated in this Policy.

Biometric may disclose Personal Data of Customers and Users without offering an opportunity to opt out, and may be required to disclose the Personal Data, (i) to third-party Processors that Biometric has retained to perform services on its behalf and pursuant to its instructions, (ii) if it is required to do so by law or legal process, or (iii) in response to lawful requests from public authorities, including to meet national security, public interest or law enforcement requirements. Biometric also reserves the right to transfer Personal Data in the event of an audit or if the company sells or transfers all or a portion of its business or assets (including in the event of a merger, acquisition, joint venture, reorganization, dissolution or liquidation).

Liability for Onward Transfers

Biometric complies with the Privacy Shield's Principle regarding accountability for onward transfers. Biometric remains liable under the Principles if its onward transfer recipients process Personal Data in a manner inconsistent with the Principles, unless Biometric proves that it was not responsible for the event causing the damage.

Dispute Resolution

If Biometric maintains your Personal Data in one of the Services within the scope of our Privacy Shield certification, you may direct any inquiries or complaints concerning our Privacy Shield compliance to info@biometric.vision or by regular mail as indicated below. Biometric shall respond within 45 days. If your complaint cannot be resolved through Biometric's internal processes, Biometric will cooperate with The International Centre for Dispute Resolution-American Arbitration Association (ICDR-AAA), which administers the arbitrations under Annex I. ICDR-AAA's website is at http://go.adr.org/privacyshieldfund.html. The mediator may propose any appropriate remedy, such as deletion of the relevant Personal Data, publicity for findings of non-compliance, payment of compensation for losses incurred as a result of non-compliance, or cessation of processing of Personal Data of the Customer or User who brought the complaint. The mediator, or the Customer or User, also may refer the matter to the U.S. Federal Trade Commission, which has Privacy Shield investigatory and enforcement powers over Biometric. Under certain circumstances, Customers and Users may be able to invoke binding arbitration to address complaints about Biometric's compliance with the Principles.

How to Contact Biometric

To ask questions or comment about this Privacy Shield Policy and our privacy practices or if you need to update, change or remove your information, contact us at: info@biometric.vision or by regular mail addressed to:

Biometric Technology, LLC.
605 GEDDES STREET
WILMINGTON, New Castle, DE 19805
info@biometric.vision

Security

We will retain and use information as required to comply with our legal obligations, resolve disputes and enforce our agreements. If you have any specific security questions, or for additional information, please contact us at info@biometric.vision.

Privacy statement updates

Our privacy policy may be updated at any time to reflect changes in our practices or the laws governing them. Please review this page periodically for the latest updates.