Last Modified Date: January 11, 2020

Privacy Notice

Scope

PLEASE READ THIS PRIVACY NOTICE CAREFULLY.

This Privacy Notice ("**Privacy Notice**") details how the Smart Eye Technology ("**we" "us" "Smart Eye" or the "Company**") will collect, use, disclose and protect personal information ("**Personal Information**") obtained from users ("**End Users**") of our technology solution (the "**Solution**"). Further, it describes the rights that you have with respect to such information.

IMPORTANT: At this time, Smart Eye offers its Solution to End Users in the United States, Canada, South Africa, India, Israel, and Australia.

Description of Our Solution

Smart Eye's Solution is a security technology designed to protect devices and documents from unauthorized viewing and access by authenticating authorized End User's through biometric analysis. The Solution can be utilized through our mobile application or through a web application. Individual consumers can establish a Smart Eye account and use the Solution in a personal context to protect confidential information ("**Personal Use**"). The Solution is also available for deployment at an enterprise level by corporate entities to protect confidential information ("**Enterprise Use**").

When the Solution is deployed for Enterprise Use, Smart Eye collects End User Personal Information as a service provider to our commercial customers ("**Enterprise Customers**") and processes such Personal Information only as authorized by our contracts with those Enterprise Customers. Enterprise Customers may opt to deploy and store the Personal Information in their own technology infrastructure, in which case Smart Eye does not receive the Personal Information at all. In those cases, the Enterprise Customer's privacy policy will govern the processing of Personal Information.

What Is Personal Information

Personal Information is defined differently by different laws and is sometimes referred to as "personally identifiable information" or "personal data". Generally speaking, it is a category of information that can be used to identify a person or a household or that can be reasonably associated with a person or household. The specific data that qualify as Personal Information vary depending on the state and

country in which you reside. The following categories are examples of Personal Information in many (though not necessarily all) jurisdictions:

Sample Categories of Personal Information and Data Elements
Personal Identifier: Name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, and passport number
Biometric identifiers: Retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry
Commercial Information: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consumer histories or tendencies
Internet or other electronic network activity information: Browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement
Geolocation information: To disable the collection of precise location information from your mobile device through our mobile apps, you can access your mobile device settings and choose to limit that collection.

Smart Eye's Collection and Use of Personal Information

The Smart Eye Solution requires an End User to submit certain Personal Information when an account is established and when the Solution is used. When a Smart Eye account is established for Personal Use, Smart Eye determines the means by and purposes for which the Personal Information is processed.

Listed below are the sources from which the Company obtains Personal Information, the categories of Personal Information collected from each and the purposes for such collection.

Source of Personal Information	Category of Personal Information Collected	Purpose for Collection

The End User	Smart Eye collects the following **personal identifiers** from End Users when they register to use the Solution and during each transaction: **First and last name** **Phone number** **Email address** **IP address**	(a) To establish and maintain your account; (b) To fulfil your requests when using the Solution; (c) To respond to inquiries and requests you have; (d) To request feedback regarding your experience with the Solution; (e) To improve the operation of our Solution; (f) To detect, prevent, and investigate activities that may violate our policies, pose safety issues or be fraudulent or illegal, and; (g) For security purposes
The End User	**Biometric Identifiers**: **Facial geometry**: Facial geometry is captured to operate the Solution, the primary purpose of which is to protect confidential information an End User sends or receives. Facial geometry is one method by which the Solution authenticates the intended recipient(s). **Fingerprint**: When an End User accesses the Solution on a device that enables fingerprint capture, that fingerprint can be used by the Solution to protect confidential information transmitted. Fingerprints are not received or stored by Smart Eye. Rather, it remains localized to the End User's mobile device. **Voiceprint**: An End User has an option to record his/her/their voice to protect confidential information from unauthorized access.	(a) To establish and maintain your account; (b) To fulfil your requests when using the Solution; (c) To improve the operation of our Solution; (d) To detect, prevent, and investigate activities that may violate our policies, pose safety issues or be fraudulent or illegal, and; (e) For security purposes

The End User's Device	**Internet or other electronic network activity information:** When an End User interacts with the Solution, Smart Eye collect electronic network activity information and device information. We also collect information regarding your use of the Solutions such as: ▪ Date Solution first opened ▪ Date Solution last opened ▪ Time spent per usage ▪ Cumulative time spent across all usage ▪ Frequency of usage ▪ Conversion from trial to paid ▪ Which biometrics are set up and when ▪ Frequency of changes to biometrics after set up ▪ Frequency of changing default security settings ▪ Solution features visited/ buttons clicked/actions taken and frequency of each **Unique device identification numbers** **Operating system and version** **Performance data**	(a) To establish and maintain your account; (b) To fulfil your requests when using the Solution; (c) To improve the operation of our Solution; (d) To detect, prevent, and investigate activities that may violate our policies, pose safety issues or be fraudulent or illegal, and; (e) For security purposes
From the Enterprise Customer	**Employment Information**	If you are using the Solution as an employee of an Enterprise Customer who accesses the Solution via Smart Eye's cloud infrastructure, Smart Eye will be aware of your status as an employee of the Enterprise Customer.

Collection of Biometric Identifiers

s, Smart Eye's Solution requires Biometric Identifiers. Specifically, Smart Eye collects scans of End User facial geometry. In addition, we enable use of fingerprints and voiceprints although that information is not transmitted to Smart's Eye's infrastructure. Smart Eye collects biometric identifiers only after receiving the informed consent of the End User from whom the information is obtained.

When an End User establishes an account, and prior to the collection of any biometric identifier, an End User is directed to electronically sign a notice stating that the End User: (1) acknowledges and consents to his/her/their biometric identifier being collected by Smart Eye; (2) acknowledges the purpose for which his/her/their biometric identifier is collected; and (3) reviews and acknowledges the notice regarding the length of time for which Smart Eye retains biometric identifiers. If the End User does not agree to the acknowledgement, the account setup process will terminate.

Biometric Information Policy

We will protect, store and transmit biometric identifiers in accordance with applicable laws and will use such information solely for the purposes outlined herein. Biometric identifiers are encrypted both in transit and at rest. We will not sell, lease, trade, or otherwise profit from the biometric identifiers we collect, but we receive payment for the use of our Solution, which utilizes such biometric information. In addition, we will not disclose or disseminate any biometric identifiers to anyone other than our third party service providers (e.g., cloud services provider) unless:

a. the End User first consents in writing to such disclosure or dissemination;

b. Disclosure is required by federal, state or local municipal laws; or

c. Disclosure is required pursuant to a valid order, warrant or subpoena issued by a court of competent jurisdiction.

When we collect biometric identifiers from End Users for Personal Use, such information is retained until the End User affirmatively deletes his/her/their Smart Eye profile. End Users have the ability to delete their biometric identifiers from Smart Eye's infrastructure via a "delete profile" function. Once that function is selected, all of that End User's biometric information is automatically and permanently destroyed.

If an End User uses our Solution as an employee or contractor of an Enterprise Customer, that End User must contact the organization with which their use is associated to determine how the biometric identifiers are managed.

For residents of Illinois, Texas and Washington: The Company does not collect biometric identifiers for commercial purposes. We collect biometric identifiers only for security purposes. The Company maintains a written policy that establishes the period of time for which the Company will retain biometric identifiers and the guidelines we use for storing, protecting, transmitting and permanently destroying biometric identifiers. Please review the Biometric Information Policy, which can be accessed **HERE**, for more information.

Smart Eye's Disclosure and Sale of Personal Information

Smart Eye does not "sell" Personal Information in the ordinary meaning of the word. Rather, Smart Eye licenses a Solution that is used for authentication and security purposes by End Users. That Solution requires the collection and use of Personal Information in order to function. When an End User initiates a transaction via the Solution, certain information will be electronically communicated to the recipient designated by the End User. The personal information shared will include the name and phone number of the End User who initiated the transaction. No other Personal Information is shared.

Smart Eye may disclose Personal Information as necessary or appropriate in connection with any of the purposes for which we use Personal Information.

Purpose for Disclosure	To Whom and Further Detail
For our business or commercial purposes	We may use third-party service providers, agents, and independent contractors to help us maintain our Solution and assist us with other services (including, but not limited to, order processing and fulfillment, providing customer service, maintaining and analyzing data, and sending customer communications on our behalf).
For legal purposes	For instance, (i) to investigate, prevent or take action regarding actual or suspected illegal activities or fraud, situations involving potential threats to the physical safety of any person, or violations of our terms of use; (ii) to respond to or defend against subpoenas, court orders, or other legal process; (iii) to establish or exercise our legal rights; or (iv) to otherwise comply with applicable law.
As part of a corporate transaction	Smart Eye may acquire other businesses, and other businesses may acquire us. If that occurs, the information we collect would likely be one of the assets examined or transferred as part of the transaction. Smart Eye will not permit another business to examine the information we have collected without a confidentiality agreement. We will not transfer the information we have collected in this acquisition context unless the recipient agrees to provide privacy protections equal to or exceeding those established by this Privacy Notice.

As referenced above, Smart Eye uses a limited number of third-party service providers and partners to assist us in making the Solution available. Those third parties include:

Name	Description of Sub-processing Activities
Adobe	To enable the End User to open an Adobe account for document
Third Party Cloud Provider	Cloud hosting services

Pendo	User activity tracking and analytics

Smart Eye does not share Personal Information with third parties for marketing purposes.

Each third party with whom we share Personal Information is responsible for maintaining its own privacy notice and practices related to the use and protection of End User Personal Information. Smart Eye requires third party service providers with whom we share End User Personal Information to process Personal Information only as allowed in our contract with such third party service provider. We ensure that any third party service providers with whom we share Personal Information are subject to privacy and security obligations consistent with this Privacy Notice and applicable laws.

If You Are a Nevada Resident

Last Modified Date: January 11, 2020

In accordance with Nevada law, our Privacy Notice identifies for you the categories of "covered information" that we collect through our Solution and the categories of third parties with whom we may share such information.

Smart Eye does not sell "covered information" as that term is defined by Nevada law. In addition, Smart Eye does not enable third parties to collect "covered information" about End User's activities over time when using our Solution.

How Long We Retain and How We Protect Your Information

How long we retain personal information.

Smart Eye retains End User Personal Information until such time as the End User expressly requests deletion of his/her/their profile via the functionality provided in the Solution. When an End User "deletes" his/her/their profile, Smart Eye will delete such End User's Personal Information from our system. An End Users may also contact us and request that his/her/their Personal Information be deleted. Once deleted, an End User cannot re-activate the deleted account; a new account must be established in order to use the Solution.

How we protect personal information

Smart Eye's Solution is built with strong security features that continuously protect your Personal Information. We work hard to protect you and Smart Eye from unauthorized access, alteration, disclosure, or destruction of Personal Information we hold, including:

- We use encryption to keep your Personal Information private while in transit and at rest
- We offer a range of security features to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to Personal Information to Smart Eye employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

Access and Ability to Correct Your Information

If the Personal Information that we maintain about you is incorrect, you may correct it via the Settings, You may also contact us to request a correction via email or phone:

- Email:
- Phone:

This right does not apply to biometric information.

Children Under 17

The Solution is not intended for use by persons under 17. We do not knowingly collect Personal Information from children under 17. If you become aware that an End User under 17 years of age is accessing the Solution, please contact us via email or phone:

- Email:
- Phone:

We will take steps to remove Personal Information from the Company's servers and terminate the account should the Company determine that a child under 17 has provided Personal Information via the Solution.

Changes or Updates to this Privacy Notice

We reserve the right to revise or update this Privacy Notice at any time, and each update to the Privacy Notice will reflect the "Last Modified" Date. Your interaction with the Company through the methods discussed in this Privacy Notice constitutes your assent to the terms contained herein. You should periodically revisit the Privacy Notice to learn of any revisions or updates.

In the event we materially change the way in which we use Personal Information, the Company will provide you with at least 30 days' notice and provide you with the opportunity to indicate your express consent to our use of your personal information as described in the new Privacy Notice.

If you have specific questions about this Privacy Notice, please e-mail us at dexter@getsmarteye.com.