Seventh Sense™

EFFECTIVE OCTOBER 15, 2022

PRIVACY POLICY AND NOTICE

SEVENTH SENSE ARTIFICIAL INTELLIGENCE PRIVATE LIMITED

Seventh Sense Artificial Intelligence Private Limited
UEN 201902751E
30 Cecil Street #19-08
Singapore 049712
www.seventhsense.ai

PRIVACY POLICY AND NOTICE

1. INTRODUCTION

1.1 We are Seventh Sense Artificial Intelligence Private Limited, a company registered in Singapore having the Unique Entity Number of 201902751E with our registered office at 30 Cecil Street #19-08, Singapore 049712 ("we" or "us"). We operate the websites https://www.seventhsense.ai/ and https://developer.opencv.fr (the "Websites").

1.2 Our core face recognition service is a software-as-a-service technology, which customers subscribe to from our website. These technology services can be accessed by:

A. logging in through any of our Websites;

B. downloading our Agent7 mobile app (the "App"), and logging in to our services module;

C. using our software development kits ("SDKs") to access our API; or

D. using our HTTP REST API from a programming language of your choice.

1.3 By accessing and using our App, Websites, SDKs and the services provided therein (the "Services"), whether in connection with a paid subscription, free trial, promotion or otherwise, you must be of legal age and willing to be bound by the data practices described in this Privacy Policy and Notice. If you do not agree with any part of this Privacy Policy and Notice, then we cannot make the Services available to you and you must stop accessing and using them.

2. PURPOSE OF PRIVACY POLICY AND NOTICE

2.1 This Privacy Policy and Notice explains how we collect and use personal data provided by you and has been adopted in accordance with our obligations under applicable privacy and data protection law, including Regulation (EU) 2016/679 (the "GDPR"),the UK Data Protection Act 2018 ("Applicable Data Protection Law"), and the Singapore Personal Data Protection Act (the "PDPA").

2.2 This Privacy Policy and Notice does not intend to deal with data protection matters related to employment with us.

3. YOUR REGULATORY RESPONSIBILITIES

3.1 You are solely responsible for using our Services in a lawful manner consistent with such standards, procedures and restrictions under Applicable Data Protection Law.

3.2 Specifically, you acknowledge and agree that in the context of our Services and any data that you upload to them:

A. our role is limited to that of a data processor or data intermediary;

B. you are the data controller;

C. biometric facial data is a category of personal data that is subject to higher standards under Applicable Data Protection Law;

D. you will obtain any applicable consent from any data subjects, or have a legal basis for possessing personal data of data subjects to the extent required by Applicable Data Protection Law;

E. you will not upload or otherwise provide to us any information in connection with the Services, which is subject to Applicable Data Protection Law, and in respect of which any requisite explicit consent has not been properly obtained or a proper legal basis does not exist; and

F. you are solely responsible for:

(i) using our services in a lawful manner;

(ii) obtaining any consent required from relevant data subjects or possessing another valid legal basis other than consent; and

(iii) maintaining such policies, procedures and standards and adopting data transfer agreements as may required by Applicable Data Protection Law in order to use our services lawfully in any relevant jurisdiction.

3.3 Whenever you upload or submit any Personal Data using our Websites or App, you or the organization or entity that you warrant and represent to us that any third-party or data subject consent required has been properly obtained or another valid legal basis has been established and remains in effect. Should any such legal basis be revoked or deemed ineffective or unlawful, it is your responsibility to (i) remove any such Personal Data from our Websites and App and cease using such data in connection with our Services.

3.4 IF YOU ARE UNSURE OF YOUR DUTIES A DATA CONTROLLER WHILE USING OUR SERVICES, YOU SHOULD:

A. MAKE EVERY EFFORT TO INFORM YOURSELF OF YOUR RESPONSIBILITIES UNDER APPLICABLE DATA PROTECTION LAW; AND

B. OBTAIN AND ACT ON COMPETENT LEGAL OR OTHER PROFESSIONAL ADVICE TO ENSURE COMPLIANCE WITH APPLICABLE DATA PROTECTION LAW.

3.5 WE ARE A TECHNOLOGY SERVICES PROVIDER AND ARE UNABLE TO PROVIDE ANY LEGAL OR OTHER ADVICE TO ASSIST YOU WITH YOUR COMPLIANCE RESPONSIBILITIES AND EFFORTS.

4. PERSONAL DATA

4.1 For the purposes of this Privacy Policy and Notice, the term "Personal Data" means any information which identifies you or which allows you to be identified when combined with other information.

4.2 Personal Data does not include data where your identity has been removed ("Anonymised Data").

4.3 Personal Data could pertain to your registration information, information of developers linked to your account, or to personal data uploaded by you

to the service that you wish to search for through the user interface, app, or programmatically through our SDKs/APIs.

4.4 For purposes of Applicable Data Protection Law pertaining to your registration information alone, we act as a data controller, and you are the subject. By registering for our Services, you give consent to us to record your information and use it for communication with you regarding our Services.

4.5 For the purposes of Applicable Data Protection Law pertaining to information of developers linked to your account that YOU have added, or to the searchable personal data that YOU upload, we are a data processor or data intermediary processing uploaded information on YOUR behalf.

4.6 The Personal Data that may be shared with us in the course of you accessing our services could include some or all of:

A. biometric facial data;

B. contact information;

C. nationality;

D. date of birth; and

E. geographic location.

4.7 For example, in connection with using our services, you could use these personal data sets to cross-reference people against the data set of your employees or visitors to your premises.

4.8 The uploaded personal data will be securely stored on our servers and will be processed by us. You may access your personal data through (i) the App; (ii) your personal account through our Websites; or (iii) our SDKs or application programming interfaces ("APIs"). Your account with us is only accessible to you when logged in to your account using your email address and password, or through programmatic access using a developer key issued by us.

4.9 The table below shows the physical locations of our servers and the geographical regions that they cover. For example, if you are based in the United Kingdom, any personal data will be stored on our server in Ireland.

Region	Server Location
United Kingdom	Ireland
EU Member States	
United States and Canada	San Francisco, USA
All Other Regions	Singapore

5. SECURITY OF PERSONAL DATA

5.1 We are committed to security and privacy of personal data and to comply with applicable law in receiving, processing, storing, accessing and disposing of such data. To this end, we maintain standardised information security measures for your protection in accordance with, at least, market standards.

5.2 It is important that you read this Privacy Policy and Notice carefully together with our General Terms and Conditions, and any other information provided to you to understand our policies and practices regarding any Personal Data (as defined below) and how we will treat it.

5.3 Any Personal Data you enter into our App or Websites or programmatically through our SDKs or APIs is stored securely on our servers as set out in the table in Section 4.8 above. You are able to access your data either on your smartphone, from your secure account via our Website, through our SDKs or through a REST API using a programming language of your choice.

5.4 This Privacy Policy and Notice applies to the access and use of our Services, which are used to upload data, and to process Personal Data and information in order to provide our Services. It also applies to our SDKs.

5.5 We have put in place appropriate security measures to prevent your Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. This includes third-party certifications from independent bodies.

5.6 Your account username is your email address. Your email address and password, and all of the data you upload and enter into our SDK, Website and App is transmitted in encrypted form and is securely stored on Amazon Web Services servers as set out in the table in Section 4.8 above. We do not disclose your account details, or email addresses to anyone except when legally required to do so. However, it is your responsibility to keep your password secure.

5.7 You must ensure that you chose a secure password when you open an account to use our Services. It is your responsibility to follow the guidance provided when setting passwords follow the guidance provided.

5.8 We limit access to your Personal Data to those employees, agents, contractors and other third parties who have a business need to know. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

6. YOUR ROLE AS DATA CONTROLLER

6.1 NOTHING IN THIS PARAGRAPH 6 SHALL BE DEEMED TO DIMINSH YOUR RESPONSIBILITIES UNDER APPLICABLE DATA PROTECTION LAW OR PARAGRAPH 3 above.

6.2 When you use our Services, Personal Data, or personal information that can be used to identify your data subjects may come into our possession. The Services allow you to upload personal data of others as a result of you using our Services for the purposes of search -in order for the Services to fulfil their purpose. For clarity, in this context:

A. we act as a data processor or data intermediary for you as the user of the Services or the organization or entity that you represent; and

B. you act as data controller of the data that you upload using our Services.

6.3 You are the data controller for the data that you upload to our Services, while we are the data processor or data intermediary providing search services on the data that you control.

6.4 For our mutual security, during your trial of our Services, we provide you with very limited access to our Services with a restricted number of allowed registrations and a limited number of API calls per day. We reserve the right to deny you the right to enter a subscription contract should we determine, in our sole discretion, any suspicious or fraudulent activity in your trial account. Security and fraud and abuse prevention form the legitimate basis for us processing the information provided by you during the trial phase.

6.5 When you subscribe to our Services, providing you with the search functionality constitutes a contractual obligation to you or the paid user subscribing to our Services.

6.6 As a data controller of the data that you upload to our Websites or App or in using our SDK, you are bound by the GDPR to abide by prevailing privacy regulations pertaining to your data subjects. The data you upload must be collected for a valid lawful basis, which may be one or more of the following:

A. *Consent*: the individual has given clear consent for you to process their personal data for a specific purpose;

B. *Contract*: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;

C. *Legal obligation*: the processing is necessary for you to comply with the law (not including contractual obligations);

D. *Vital interests*: the processing is necessary to protect someone's life;

E. *Public task*: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law; and

F. *Legitimate interests*: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

7. DATA COLLECTION METHODOLOGIES

7.1 We collect and use Personal Data using our proprietary technologies:

A. face verification;

B. face anti-spoofing; and

C. face search.

7.2 Face verification is a task whereby a user uploads two sets of images to determine if they are the same person. An example is verifying an image of a person that is obtained from a webcam against an image of that person's face from his or her photo identification image.

7.3 Face anti-spoofing involves a user uploading a single image, after which our systems determine if the image is of a real person, obtained from a real camera, or whether it is a photo of a paper or screen showing the face of a person.

7.4 Face search means a task whereby a user uploads or enrols images of persons that they will later need to search and check against a database. Examples uses could include matching an unknown person against previously registered persons, for example, in a visitor management, perimeter security or law enforcement context.

8. HOW WE COLLECT AND USE PERSONAL DATA

8.1 When you use our Services, we may also collect Personal Data automatically from you or from third-party partners or services. This data collection and use is designed to provide you with a better experience when using our Services.

8.2 The Personal Data we collect includes:

A. *Basic identifiers and contact information*: We collect information from you when you provide it to us directly such as via an email or online form, through the support feature embedded in our Websites and App, or through another form of inquiry. This information may include your name, email, and phone number as well as other information;

B. *Device Information*: When you download and use our App and otherwise access our Services, we automatically collect information on the type of device you use, operating system, resolution, application version, mobile device identifiers (such as your device identification and advertising points), language, time zone and internet protocol address;

C. *Usage information*: We collect information automatically about your activity through our Websites and App such as the date and time you use the Services; and

D. *Location information*: We may collect, information such as geolocation (latitude and longitude) using information including GPS, Bluetooth or Wi-Fi connections, or internet protocol addresses.

8.3 We may receive information about you from our third-party service providers (principally Google Analytics), which collect this information through our Websites in accordance with their own privacy policies.

9. YOUR CONSENT FOR US PROCESSING SPECIAL CATEGORY DATA

9.1 The information you provide when using our App, SDK and Website may include special category data (as defined the GDPR framework) such as biometric facial data. Special categories of Personal Data for the purposes of the Applicable Data Protection Law attract additional security and we require consent to our processing of that data, unless or until it is anonymised.

9.2 By agreeing to our General Terms and Conditions, you give us consent to process any special category data that you make available to us in connection with the Services.

10. AGGREGATED ANONYMISED DATA

10.1 The information we collect from you may be combined with information provided by others, but only in an anonymised format, to produce aggregated anonymised data sets for research purposes. We refer to this combined data as "Aggregated Data". Aggregated Data is not considered to be Personal Data as it does not reveal the identity of any data subject.

10.2 Aggregated Data may be used for the operation of our App and the Services we provide to you, and to provide general statistics regarding use of our Services. We may also use such anonymised Aggregated Data and provide it to third parties for research purposes.

10.3 However, if you or we combine or connect Aggregated Data with any of your Personal Data that enables you to be directly or indirectly identified, we will treat such data as Personal Data to be used in accordance with this Privacy Policy and Notice.

11. USE OF COOKIES AND GOOGLE ANALYTICS

11.1 We may use cookies and similar technologies to enhance your experience when you use our Services. Our cookies cannot be used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you, and can only be read by a web server in the domain that issued the cookie to you.

11.2 Our Websites use cookies and similar technologies to distinguish you from other users. This helps us to provide you with a good experience when you browse our Websites and allows us to improve our Websites. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of the Websites may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookie Policy **here**.

11.3 We use Google Analytics and reCaptcha. The information generated by the Google Analytics cookie (including your internet protocol address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of our Services compiling reports on activity and providing other services relating to activity and internet usage.

11.4 Google may also transfer this information to third parties where required to do so by law, or where third parties process the information on Google's behalf. You should consult their respective privacy policies for details.

11.5 We always allow you to consent to the cookies we can use. However, certain cookies are essential to the normal functioning of the Services, and without consenting to them, you cannot use the individual components of thereof such as our Websites and App and their respective features. The rest are at your discretion and you can consent to their use, if you so choose. Consent can also be withdrawn at any time.

12. PROVIDING PERSONAL DATA TO THIRD PARTIES

When you pay for our Services, you are providing your Personal Data to third-party providers appointed by us in the payment process. Any charges for using our Services are administered by the App store used to download our App, and Stripe used to purchase

subscriptions to our Services. We recommend that you refer to the privacy policies of the relevant app store and Stripe to make sure you understand how your Personal Data, including your financial Personal Data, may be used when you purchase apps and software.

13. PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

13.1 We hold and process your personal information and Personal Data to operate our Services. The legal bases we rely upon to use your Personal Data may include the contract we have with you, your consent and our legitimate interests, or where we need to comply with a legal or regulatory obligation. Please contact us if you require further details concerning the specific legal ground(s) we are relying on to process your Personal Data.

13.2 We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

13.3 We offer here non-exhaustive examples of the ways in which we use your Personal Data and the legal bases we may rely upon to do so:

A. to provide and maintain our Services, including to register you as a new user, perform essential business operations, and our legal basis for processing is performance of a contract with you which you entered into with us when you subscribe to our Services and accepted our General Terms and Conditions available **here**.

B. to administer our Services (including troubleshooting, data analysis, testing, support, fraud, reporting and hosting of data), our legal basis for processing is legitimate interests for running our business and provision of administration and services. If processing of any sensitive personal data is required that will be on the basis of your consent from when you signed up.

C. to inform you of other products or services that we and/or our business partners provide. We may also contact you via surveys to conduct research about your opinion of our Services.

13.4 We may share your Personal Data for certain purposes with our business service providers or affiliates in accordance with Applicable Data Protection Law, as set out below.

13.5 We may share your Personal Data with our third-party business service providers who perform functions on our behalf. These may include:

A. IT service providers and system administrators;

B. Data hosts and providers of programming or technical support;

C. Professional advisers including lawyers, bankers, auditors;

D. Payment services; and

E. Third-party analytics partners to analyse website traffic and understand customer needs and trends or our third-party marketing service providers to help us to communicate with.

13.6 *For corporate transactions*: We may transfer your Personal Data if we are involved, whether in whole or in part, in a merger, sale, acquisition, divestiture, restructuring, reorganisation, dissolution, bankruptcy or other change of ownership or control.

13.7 *When required by law*: We may also share Personal Data if we are also under a duty to disclose or share your Personal Data in order to comply with any legal obligation, or to protect the rights, property, or safety of our business, our customers or others.

13.8 *To enforce legal rights*: We may also share Personal Data:

A. if disclosure would mitigate our liability in an actual or threatened lawsuit;

B. as necessary to protect our legal rights and legal rights of our users, business partners or other interested parties;

C. to enforce our agreements with you; and

D. to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing.

14. CROSS-BORDER DATA TRANSFERS

14.1 Sharing of Personal Data sometimes involves cross-border data transfers, including transfers outside of the EEA in accordance with the law. We only transfer Personal Data to entities in third countries that have provided appropriate safeguards to ensure that their level of data protection is in agreement with this Privacy Policy and Notice and applicable law.

14.2 Currently this does not include the United States of America, as rules and procedures under the EU-US Privacy Shield have not been deemed by the European Commission to provide sufficient safeguards for Personal Data.

15. DATA RETENTION

15.1 We will retain your Personal Data only for as long as is necessary for meeting our contractual obligations and the purposes set out in this Privacy Policy. Typically, this is as long as you or the organisation or entity you represent use our services with regard to you and your Personal Data.

15.2 We will also retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable law), resolve disputes, and enforce our legal agreements and policies.

15.3 Your Personal Data will be processed as soon as you upload it to us. The uploaded data will be retained for the period of your subscription to the Services and for one month after termination of such.

15.4 Should you opt out of using our Services you will be able to re-join and access your Personal Data within one month.

15.5 Should you terminate your account with us, all the data pertaining to your account will immediately be deleted.

15.6 Your Personal Data will be reviewed regularly and at least once every year for relevance. Any Personal Data deemed no-longer relevant is deleted.

15.7 If we have taken steps to anonymise your personal data (so that it can no longer be associated with you) we may use this indefinitely for

analytical, research and statistical purposes and to help us to improve our Services.

16. YOUR RIGHTS

16.1 *Your right to withdraw consent at any time*: Whenever we rely on your consent to process your Personal Data, you have the right to withdraw your consent at any time. If you wish to withdraw your consent, please contact Seventh Sense AI using the contact details provided at the end of this privacy policy. This will not affect the lawfulness of any processing carried out before you withdraw, nor ongoing contractual or other obligations requiring us to process data for example due to a court ordered law enforcement request.

16.2 *Your right to access the Personal Data we hold about you*:

A. You have the right to make a request to access your Personal Data collected through our Websites and App (known as a "Data Subject Access Request" or "DSAR").

B. You may submit a DSAR request here: https://prighter.com/cc/seventhsense

C. We aim to respond electronically to all DSARs within 30 days. In circumstances where it may take us longer to respond (for example if your request is particularly complex or if you have made a series of requests), we will notify you. We generally do not charge a fee for responding to a DSAR. However, we may charge a reasonable fee if your DSAR is manifestly unfounded or excessive.

16.3 *Right of rectification*: You have the right to ask us to rectify Personal Data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

16.4 *Right to erasure*: You have the right to ask us to erase your Personal Data in certain circumstances.

16.5 *Right to restriction of processing*: You have the right to ask us to restrict the processing of your Personal Data in certain circumstances.

16.6 *Right to object to processing*: You have the right to object to the processing of your Personal Data in certain circumstances.

16.7 *Right to data portability*: You have the right to ask that we transfer your Personal Data to another organisation, or to you, in certain circumstances.

17. OPT-OUT AND UNSUBSCRIBE

We respect your privacy and give you an opportunity to opt-out of receiving announcements of certain information. You may opt-out of receiving any or all communications from us by contacting us or selecting the "Unsubscribe" option on such email announcements.

18. CHANGES TO THIS PRIVACY POLICY

We may occasionally update this Privacy Policy and Notice to reflect company and customer feedback and any changes in applicable law. We encourage you to periodically review this Privacy Policy and Notice to remain informed of how we are processing your information.

19. CONTACT INFORMATION

19.1 We welcome your questions or comments regarding this Privacy Policy. If you believe that we have not adhered to this Privacy Policy and Notice, please contact us at dpo@seventhsense.ai or:

Seventh Sense Artificial Intelligence Private Limited
30 Cecil Street #19-08
Singapore 049712

19.2 Questions, comments and requests regarding this privacy policy are welcome and should be addressed to the Data Protection Officer at our address given above.

19.3 We ask that you try to resolve any issues with us first, although you have a right to lodge a complaint with the Information Commissioner's Office ("ICO") at any time about our processing of your personal information.

19.4 The ICO is the UK regulator for data protection and upholds information rights under English law. The ICO's contact information is as follows:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
United Kingdom

Telephone: 0303 123 1113
Fax: 01625 524510