Privately SA: Privacy Policy

Version: Update on 11th of February 2025

About Us

We are a Swiss company with our headquarters at 109-110, Batiment D, EPFL Innovation Park, Lausanne, Switzerland. We also have a branch in London, UK. Swiss Registration Number:
CHE-286.854.770 and UK Company No: FC037096.

Background

Privately SA builds technology in the fields of age assurance and online safety. We are mainly a B2B business so for the most part we do not have any direct contractual 'end user' relationships except for special situations. We will therefore be processors of end user data on behalf of our clients. Our technology is built using on-device edge-AI that facilitates data minimization so as to maximise user privacy and data protection.

Definitions:

B2B: Business to Business – which means that our technology is built into mobile/web applications or hardware deployed by businesses. We do not directly have a contractual relationship or knowledge of the identity of the end users of our technology.
End User: The final user whose age is being estimated or who is being provided safeguarding.
On-device edge-AI: The machine learning based technology that we use (for age estimation and safeguarding) processes user's data on their own devices, thereby avoiding the need for us or for our partners to export user's personal data onto any form of cloud services.
Data processors: We would process user's data on behalf of our Clients and are therefore processors when integrated into our Client's workflows. Our Clients offer online safety or age estimation services, or use our age estimations services as part of onboarding or checkout processes.
Test Applications: We have a number of test applications which allows our Clients to test our technology using test 'data subjects'. For these applications we provide specific data collection guidelines for the data subject.

AgeAI app: We have built an application for automated and anonymous age estimation to be deployed primarily in a retail setting to assist retail staff with age checks.
Test Data Subject: An end user of our technology who agrees to test our technology and provide feedback on its performance. We might capture, process and retain the user's data for the specific purpose including for the purpose of training our classifiers and other R&D purposes.
Privately Showroom : A website that visiting users can use to test our machine learning technology.

User Data Privacy and Data Minimization by design

Our technology solutions are built to operate mostly on user devices and to avoid sending any of the user's personal data to any form of cloud service. For this we use specially adapted machine learning models that can be either deployed or downloaded on the user's device. This avoids the need to transmit and retain user data outside the user device in order to provide the service.

Training Machine Learning Models:

In our current implementations we do not train our machine learning models on the data of the end users of our technology. Our machine learning models are currently trained 'offline' from data sources that we have acquired but not on the user data itself. This might change in the future as we introduce new privacy-preserving technologies like Federated Learning. We will update our privacy policy accordingly.

Coverage of this Data Privacy Policy

This policy lays out the broad data collection and processing mechanisms across all of the public and private deployments of our technology, namely:

1. Our website privately.eu
2. Privately Showroom showroom.privately.swiss
3. Our AgeAI app for retail available at privately.eu/ageai

4. Our developer page developer.privately.eu/home
5. OWAS - Safety SDK: deployed in Client applications - for online safety
6. AgeAssure - Age SDK: deployed in Client applications - for age estimations
7. AgeAssure - Age: Web Browser Based Solution
8. Test application for online safety: Oyoty
9. Test application for age estimation: MMAE (Multimodal Age Estimation)
10. Test Sandbox: We may set up a Sandbox environment independently or within our Client environments to assist our age estimation use cases. In this test environment we would have Test Data Subjects who will give us explicit permission to separately process their Personally Identifiable Information PII (like biometrics) in order to improve or correct the predictions from our age estimation models.
11. We also collect data separately to train our classifiers. For this purpose we might use a mix of publicly available resources, licensed sources as well as data collected through our own sources. In this role we are 'Data Controllers'
12. We will additionally collect data for the users of our AgeAI app and those that might engage with the service website privately.eu. In this case too we will be data controllers.

What data does Privately Collect? How is it collected and what is it used for?

1. On website privately.eu we currently use standard cookies to track user analytics to measure the performance of the website.
2. On our developer page - we invite developers to test our technology. We will collect their names, email addresses and organization details to verify and bill them. We will also retain analytics to understand how they will use our technology which will also form the basis of billing them.
3. OWAS Safety SDK deployed in client applications: We do not collect any user data since end user relationships are managed by Clients themselves within their closed environments.
4. On AgeAI webpage privately.eu/ageai: We will collect names and emails of people who sign up for the service and will additionally use cookies to track users through advertising.
5. AgeAI app: We do not collect any end user data (PII: Personally identifiable information) since the app anonymously detects age of users.We will however collect service metrics and analytics. This app is currently distributed through the Play Store (Google, Android).

6. FaceAssure SDKs deployed in client solutions: We do not collect any user data since end user relationships are managed by Clients themselves within their closed environments.
7. FaceAssure Web browser Solution: In this implementation we are subprocessors of data and will process user data on the browser of the user on behalf of our Client. We will only retain a session ID and an age range and no other Personal Identifiable Information about the end user.
8. On Oyoty test app: Privately keeps only usage analytics and email of the user.
9. MMAE (Multimodal Age Estimation) test app: We have only app analytics.
10. Test Sandbox : Here we might retain biometric data and other PII of the test data subject for an extended period of time depending on the contract signed with such test data subjects.
11. Data for Training Purposes: We do not use our customer's data for training. We train our machines separately on data specifically acquired for this purpose. We use data from a range of open, licensed sources or from manifestly public sources. Here we will collect both anonymous content to train our text model or photographs or videos of people and voices. We do not have any data information on any person that is not either licensed to us or is manifestly public. We may license such data or collect it from public sources.

Retention of Data

1. Through our website privately.eu we do not acquire any user data other than navigation analytics data.
2. Through the sign-ins on our developer page- we will collect their names, email addresses and organization details and usage analytics associated with developers.
3. Through OWAS Safety SDK deployed in client applications: We do not acquire any user data.
4. Through AgeAssure SDK deployed in client solutions :We do not acquire any user data.
5. AgeAssure Web browser Solution: We will retain a session ID and an age range and no other Personal Identifiable Information about the end user for the duration that is required by our Client.

6. On Oyoty test app: The email of the user is deleted when they delete their account.
7. On Test Sandbox: Here we might retain biometric data and other PII of the test data subject for an extended period of time depending on a specific contract signed with such test data subjects.
8. Training Data: This data can be retained by us infinitely.

Privately Website specific considerations

Tracking

We may use Facebook Pixels on this website to collect information about your browsing behaviour and interactions with our website.

Purpose of Collection:
The information collected through Facebook Pixel is used for the purpose of analysing website traffic, measuring the effectiveness of our advertising campaigns and user journeys.

Use of Cookies and Tracking Technologies:
Facebook Pixel uses cookies and similar tracking technologies to track and store information about your browsing activity on our website.

Information Sharing:
Facebook's Data Collection and Usage:
Please note that the information collected through Facebook Pixel is subject to Facebook's own data collection and usage practices. For more information about how Facebook handles your data, please refer to their privacy policy.

Your Choices of Opt-Out Platforms:
You can use industry-wide opt-out platforms, such as the Digital Advertising Alliance (DAA) opt-out tool (optout.aboutads.info) or the Network Advertising Initiative (NAI) opt-out page (optout.networkadvertising.org).These platforms provide opt-out mechanisms for personalized advertising, including Facebook Pixel.

Data Retention:
We retain the information collected through Facebook Pixel for a maximum of 6 months

AgeAI app

This section specifically details the use of personal information collected from users of AgeAI app.

Information We Collect:
We may collect certain information when you use our app, including device information, location data, usage statistics and user demographic statistics.

How We Use the Collected Information:
We use the collected information for the following purposes: improving the app, personalizing user experience, analysing usage patterns, and providing troubleshooting when needed.

Information Sharing and Disclosure:
We do not share personal information with third parties at all.

Data Retention:
We retain personal information for as long as necessary to fulfil the purposes outlined in this Privacy Policy, unless a longer retention period is required or permitted by law.

Security:
We take reasonable measures to protect the security of personal information within our app. However, please note that no method of transmission or storage is completely secure.

Third-Party Links and Services:
Our app may contain links to third-party websites or services that are not operated by us. We are not responsible for the privacy practices of these third parties.

Lawful bases of the use of information

As per the requirement of Article 6 of the UK GDPR, we have conducted assessments to determine our lawful basis for Processing: We believe that ‘Legitimate Interest’ best describes the lawful basis for processing user data.

Lawful basis	Examples
Legitimate Interest 1- Performance of website	We retain neither performance analytics nor any other visitor information currently. However we might soon retain certain visitor related analytics using cookies in the future.
Legitimate Interest 2- To provide age estimation services to our client using User Face And Voice Pattern Analysis	On behalf of our Clients who provide online safety solutions, our technology will process data generated by end users including text, and images/photos. In order to provide age estimation our technology will analyse patterns of faces through photos and voice through examining microphone inputs (sometimes patterns of writing) to establish which age bracket the user might fall in. This data is processed within user devices and we have no access to any of the underlying data. The output of these processes - namely a threat assessment or an age estimation - is then transmitted to our Client environments to enable their use cases.

Legitimate interest 3 - to provide online safety services in the form of an app to our clients	Some personal data may be required to run parts of our business. **Data for setting up a user relationship**: In some of our test services or some uses we run for our clients,identifying data like an email address of an end-user might be needed to use some of our services. **Training** : For the moment we do not train our machine learning models using any of the user data that we process for our clients. However that might change in the near future once we implement privacy preserving learning technologies. **Analytics:** We aggregate the metrics information we get from users to understand how our website and app are performing, to identify bugs and improve our services.
Legitimate interest 4- Information to subprocessors	In order to perform our services, we might share the required user session information with our subprocessors like Exoscale, AWS, Mixpanel and Google for them to provide subservices like analytics, notifications, etc.

Special Category Data: As per guidelines of Article 9 of the UK GDPR - we deal with the following special category data :facial and voice data which in normal cases would come under 'Biometric' category. However we do not use this data for identification but for pattern matching so strictly speaking *we believe we do not deal with facial and voice data biometrically as no identification or profiling is involved. The processing is matching face and voice patterns with known patterns to determine an age range.*

Basis of Processing Special Category Data: For most of our use cases such processing is done with 'Explicit Content' of the data subject.

However in some client use cases such processing might be done in a 'silent' mode. The basis for 'silent processing ' can be found in ***'Reasons of substantial public interest (with a basis in law)'***. The public interest in our case is defined in Paragraph 8 of Schedule 1 of the DPA 2018: 'Safeguarding of children and individuals at risk'.

Information sharing

Privately does not retain any user’s personal data beyond that specified in this document nor do we share any of this user’s data with third parties.

Rights of the data subject (End User)

As data subject, by asking your requests to support@privately.eu, you can exercise your rights as listed here, when it applies to our products that you are using:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure or right to be forgotten
- Right to restrict processing
- Right to data portability
- Right to object
- Right not to be subject to automated decisions
- Where automated decision making is in place, right to ask for human intervention

Contact:

If you have any questions you can reach us at support@privately.eu

Addendum

Double blind implementation

Privately’s FaceAssure privacy by design implementations rely on Edge AI, as such the age estimation takes place on the user’s device and np biometric data is transferred.

Privately’s FaceAssure browser deployments and SDKs allow a “double blind” implementation for services integrating FaceAssure through any of our partners. In such an implementation, Privately will not know where the age estimation requests originate from.

While a party integrating Privately’s FaceAssure would know the service requesting an age verification, this information is not relayed to Privately. Conversely, Privately would have some information about the age verification target, but no information is relayed to the partner except for the age verification result. This provides a very high degree of privacy for end users going through an age verification process.