



Realeyes Privacy Policy for XP Attention & Emotion and Verify

Last updated and effective 4th Jan 2024, version 2.0

1. Privacy Overview

Realeyes OÜ (Vahe 15, Tallinn 11615, Estonia, registry code: 11730664; “**Realeyes**”) and its affiliates (hereinafter jointly referred to as ‘**Realeyes**’, ‘**we**’, ‘**us**’ or ‘**our**’) offers technology infrastructure components that enable Realeyes’ clients to understand diverse human reactions and authorize the identity of individuals (‘**user**’, ‘**you**’ or ‘**your**’) via AI-enabled facial coding capabilities. These components range from camera-enabled facial measurement capabilities to face verification features and other miscellaneous services. Such service components are jointly called Experience Platform (XP), which is built on our patented facial feature tracking technology. XP Attention & Emotion, as well as Verify are face verification service components of Experience Platform (hereinafter referred to as ‘**Service**’).

- XP Attention & Emotion: This Service captures five measurements every second, gauging users' likelihood of manifesting attention and several emotion classifiers. Data, in real-time, is provisioned on the client-side for the host application's benefit. Concurrently, near-real-time data is relayed to the cloud or other specified endpoints utilizing a publisher/subscriber architecture.
- Verify: This Service calculates a user's distinct facial embedding. Such embedding can then be compared against a pre-existing user set for authentication purposes and to discern any duplications. Furthermore, Verify possesses the capability to identify bots, potential demographic discrepancies via age/gender assessments, and attempts at presentation or injection attacks wherein users strive to elude verification.

This Privacy Policy (‘**Policy**’) This Privacy Policy is intended to help you understand how we use the Personal Data (as defined in Section 2 below) we collect to provide our Service on behalf of our clients and build trust in our system.

This Policy describes how we collect and process your Personal Data while we provide our Service to our client. The provisions of our Terms of Service apply to this Policy as well.

You provide your Personal Data to us at the direction of our clients so that our client may verify your identity to prevent fraud. When we provide Services to our clients, we are generally acting on their behalf as their processor. Our Services provide check results to our clients who decide how to proceed with the user, this may be to proceed, to reject the user or to ask for further checks. For additional information about how your specific Personal Data is being collected and used, please review the privacy policy of our client who is using our Services with you.

Please read our Policy carefully to make sure that you understand our processing activities. When you engage with our Service that we provide, you are agreeing to this Policy. If you do

not agree with our Policy and our processing activities, please do not proceed with the verification carried out by our Services at this time.

Please note that Realeyes does not knowingly obtain Personal Data from any of our products, study data, or survey responses from individuals under the age of 18, unless (i) applicable local data protection legislation provides for a lower threshold age; or (ii) we obtain the required parental consent. Should we discover that any data has been collected from an individual under the age of 18, without meeting either conditions under points (i) or (ii) above, we will immediately delete it.

2. What does Personal Data mean?

Personal Data means anything that can be used to identify you, including scan of your facial geometry, that we collect as you interact with our Service.

3. Service

This part of the Policy explains the Personal Data processing activities associated with our Services.

In case of XP Attention & Emotion, when providing our Service, we'll analyse how people feel when they view on-screen media. We do this to help our clients improve their content and advertising. Your participation in our studies is voluntary and highly valued. The information that we share with our customers is anonymized and does not individually identify any test participants in the market research. Images from the camera are processed on the device without recording. Binary outputs are sent to servers and images are discarded.

In case of Verify, when providing our Services, we'll use the camera of your device to take a picture of your face. By extracting and comparing numerical biometric data from facial image data, Realeyes assesses whether it is likely that the same person appears on two separate photos or not in order help verify your face (hereinafter referred to as '**face verification**'). We will also look for signs of fraud, for example automatic participants (bots) which are identified by device metadata (e.g., a modern laptop or smartphone that suspiciously doesn't have a webcam, or using a synthetic webcam), demographic mismatches are identified when age and gender estimations provided by our Service are different from self-reported data, or webcam manipulation (e.g., injecting an image, covering the camera). Except as described in this Policy, when performing face verification based on biometric data we do not store the extracted biometric data once the check is complete.

Where a client has asked us to provide our Service, we maintain depending on the specific client request (i) a facial geometry map for each user account of our client's users or (ii) a facial geometry map for each survey access by a client user (per transaction) within retention periods set by our clients and subject to any maximum retention periods specified in applicable laws. When authenticating a user, we will compare an image of the user with the image we have stored. If the two images match, the authentication is confirmed.

Please note, Realeyes does not store video or images from your camera on your device or our systems, servers or cloud storage. Any images accessed from the camera will be discarded immediately after processing it on our encrypted and secured servers, such processing should not take longer than 1 second at most. However, personal data derived from images (including the map of your facial geometry) may be stored on our servers and systems.

If you do not grant permission for us to access your front facing camera on your device, we will not be able to verify your face.

3.1. Personal Data Categories

For the Service to operate, we request your technical permission to use the camera of your device. Our application then collects the following separate data-points Personal Data related to face verification:

- i. Provided our client has obtained the necessary legal grounds for processing activities carried out by our Service, then we will process the following Personal Data about you:
 - o Unique ID number assigned to your session by our client when you are redirected to our Verify platform ("**Transaction ID**");
 - o Images of your face (that is discarded immediately after it is processed);
 - o Your biometric data, including facial scan data, embedding and numerical biometric data, age and sex estimations extracted from such images;
 - o Image metadata
 - o Telemetry events related to the camera of your device:
 - camera available / unavailable;
 - other camera information.
 - o Whether a face is detected and, if so, the position and orientation of the face relative to the screen.

3.2. Information Use and Legal basis of processing

We use your Personal Data for the following purposes based on the below specified legal basis:

- To provide the Services to our clients. Please note that the legal basis of any processing activity carried out for such service performance purposes is determined by our client. For information on the legal basis of our processing, please refer to the privacy policy of our client who is using our Services.
- To protect our legal rights, including file claims or protect us against claims, in which case the legal basis for processing is our legitimate interest to protect our rights;
- To perform our obligations arising from applicable legal acts.

In addition, if in relation with particular activity relating to our Service we want to use your Personal Data for specific purposes materially different from those specified here, we will request your consent.

If the legal basis for processing is your consent, you have the right to withdraw the consent at any time. Please note that the withdrawal of your consent does not affect the lawfulness of the processing carried out under the consent prior to the withdrawal and therefore does not apply retrospectively.

Broadly speaking legitimate interest as a legal basis means that we process your Personal Data based on our genuine and legitimate reason and on condition that we are not harming any of your rights and freedoms during such use. In our assessment, we have taken into

account considerations of the risks present in our processing, your likely response to those risks and the benefits you are likely to receive from such processing. You have the right to file an objection at any time against such processing. If you object, we will refrain from further processing of your Personal Data, except if we prove that the Personal Data is being processed due to a compelling lawful reason which overrides your interests, rights and freedoms, or if we process your personal data for the purpose of preparing and filing legal claims or protecting against claims filed against us.

4. Who do we share your Personal Data with?

Realeyes may share your Personal Data in limited ways for the following reasons in order to provide our Services:

- We work with trusted partners to perform the following tasks on our behalf and we may need to disclose Personal Data to them so that they can perform these tasks. These tasks include website hosting, content management services, technology and communications platform providers, and data annotation platform providers. However, these companies are bound by confidentiality obligations and do not have any independent right to use Personal Data beyond what is necessary to assist us in order to provide our services.
- We may share your Personal Data, where appropriate, with any member of our group of companies and with any of our affiliates for the purposes of supporting our business. Any disclosure will be in accordance with data protection regulations and you consent to share your Personal Data with our group companies and affiliates.
- We may share your Personal Data when we believe that doing so is necessary to protect, enforce, or defend the legal rights, privacy, safety, or property of Realeyes, our employees or agents or users, or to comply with applicable law or legal process, including responding to requests from public and government authorities.
- You agree that, if there is a change in the ownership of Realeyes or any of our assets, such as in connection with a merger, acquisition, reorganization, dissolution or liquidation, or if we take steps in anticipation of such a transaction, we may transfer and disclose Personal Data we have collected to the new or prospective company, subject always to the data protection regulations.
- We may share anonymized, aggregated or de-identified data without restriction.

In addition to the sharing described in this Privacy Policy, we may share information about you with third parties whenever you consent to or direct such sharing.

5. Automated Decision Making

Automated decision-making takes place when an electronic system uses Personal Data to make a decision relevant to you without human intervention.

When we verify a face on behalf of a client, we provide a verification status (unique, duplicated, webcam tampering, bot) to that client as an output. The various verification statuses are generated from our different machine learning models that are used to verify a face.

We will not make any decision that would significantly affect an individual based solely on processing by automated means, however our clients may use such automated decision-making based on the outputs that we provide them depending on how a given client uses our Service.

We only provide recommendations to our clients who will then decide how to proceed with the given user, this may be to proceed, to reject the user or to ask for further checks. If we're able to verify the face of a user, we notify the client that the face verification was successful.

If we're unable to verify the face of a user, we return results including but not limited to the following: 'Duplicate', 'Webcam manipulation' or 'Bot'. Exact face verification results may vary based on client specific requirements. Clients will decide how to proceed based on the information we provide and their processes. They may reject the user, proceed anyway or conduct additional checks before continuing with the given process.

These machine learning models are under constant development, the growth and complexity of machine-learning can make it challenging to understand how an automated decision-making process works. However, as a data subject that may be subject to automated decision making by our clients, you should be provided with sufficient information on the logic involved behind the automated decisions. Please see a simplified, but comprehensive summary of the logic behind our face verification algorithms:

Our machine learning model is used to authenticate unique users and identify duplicate users. The machine learning model produces a probability, with a particular level of confidence, that two faces are the same. The supplementary probabilistic decision tree subsequently provides our clients with a classification based on the fraud risk for a given user along with other detailed information about the telemetry events that explain the service results.

6. How long do you keep Personal Data for?

Where possible, we pseudonymize, de-identify and/or aggregate data, to protect users' privacy and minimize security risks.

We perform our Services on behalf of our clients as a data processor for various reasons. Such reasons are solely identified by our clients, and we rely on them to tell us when they no longer need us to store the information on their behalf, subject to maximum retention periods imposed by applicable laws, defined by our clients or by Realeyes.

If you, as a user, would like to make a specific request to have your information deleted, please make that request directly to our client that redirected you to the platform of our Service. For more information about how to do this, please see below under Section 8 below.

Where we have a legitimate interest, we may also store information for longer than described above. If you exercise your right to delete your Personal Data in such cases, we will do so as expeditiously as possible following your verification, unless otherwise stated here, but in each case within 30 days of receipt of your request at latest.

7. International Transfer of Personal Data

We may transfer your Personal Data to countries outside of the European Economic Area EEA (such as the US). We do this for our data management and business purposes, in particular, for outsourced data processing by organisations on our behalf and in accordance with the stated aim of the data processing. We take appropriate steps to ensure your information is adequately protected in accordance with applicable data privacy legislation.

8. Rights of Data Subjects

For processing of your Personal Data for service performance purposes, Realeyes is the data processor on behalf of its client. If you are an individual whose face has been verified through Verify, please contact the appropriate client to exercise any rights that you may have under applicable law. If you have further concerns or questions regarding the processing of your Personal Data, please email verify@realeyesit.com. Please note, Realeyes may need to notify the relevant client for most requests so the client (and not Realeyes) may fulfill the request. This is necessary where Realeyes is acting on the client's behalf.

In relation to other processing activities that are carried out by Realeyes as a data controller (for example as detailed under Section **Error! Reference source not found.** above), you are entitled to exercise the following rights with regards to your Personal Data to the extent prescribed in applicable law:

Right of Access

The GDPR gives you the right to access information that we hold about you. If you want to access that information, please send your request to verify@realeyesit.com. Any request for access of your information shall be a subject to providing the acceptable proof of identification. If all complies, you will be provided with the copy of your Personal Data. If a person's request for information or measures is clearly unjustified or excessive, a reasonable fee may be asked, or the action taken may be refused.

Right of Rectification

You can have your Personal Data rectified at any time, in case it is inaccurate or incomplete. You should notify us to correct or update your Personal Data. You can notify us at any time at verify@realeyesit.com

Right of Erasure

You can request to delete your Personal Data at any time by contacting us at verify@realeyesit.com

Right to Restrict Processing

In certain circumstances, you have a right to restrict or block us from processing your Personal Data.

Right to Withdraw your Consent

If the processing is done based on your consent, you have the right to withdraw your consent to processing of your Personal Data at any time by contacting us at info@realeyesit.com

Right to object

At any given time, you have a right to object to the processing of your Personal Data. Please follow the instructions for erasure.

Complaints

The Policy is governed by legislation of Republic of Estonia. Any disputes in connection with this Policy shall be settled through negotiations. If the Parties fail to resolve the dispute

through negotiation, the disputes shall be settled by Harju Maakohus (Harju County Court), pursuant to the procedure provided by the law of the Republic of Estonia.

If you have any concerns with the way we process or handle your Personal Data, we would encourage you to contact us directly to resolve your concerns. However, you have the right to lodge a complaint with the Estonian Data Protection Inspectorate (you may find their contact details [here](#)).

You may exercise any of these rights at any time by emailing us at dpo@realeyesit.com.

9. Contacting us

Please contact us if you have any comments or questions about information that we hold or about our Privacy Policy.

Send an email to verify@realeyesit.com under the subject heading "Software Privacy Policy"

Write to us at Realeyes, 201 Borough High St, London SE1 1JA, UK

10. Changes to our Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of changes by posting an announcement on our website or during the use of the Service we provide. You are bound by any changes to our Privacy Policy when you engage with our Service after you are notified of these changes (by an announcement on our website or in the Service or during other services). We recommend you check back periodically.