Privacy Policy

Version: 1
Last updated: 20 October 2026
Effective from: 20 October 2026

1. About this policy and about us

This Privacy Policy explains how Tenor collects, uses, shares and protects your personal data when you use the Tenor app, our website tenorinpl.com, or contact our support channels.

"Tenor", "we", "us" and "our" means TENOR FZCO, a free zone company registered in the Dubai Multi Commodities Centre under registration number DMCC205425, of Unit BA2196, Level 1, Jewellery & Gemplex 3, DMCC, Dubai, United Arab Emirates. We are the controller of your personal data under Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the PDPL).

This policy applies to everyone who interacts with Tenor: visitors to our website, people who have registered but not yet completed verification, and verified customers. Identity verification is currently available to UAE residents only.

Tenor is for adults. You must be at least 18 years old to register. If we become aware that a user is under 18, we will close their account.

By registering for and using Tenor, you acknowledge this policy. Where the law requires your consent for specific processing, we ask for it separately.

2. Information we collect

We collect only the personal data we need for the purposes in this policy. Please tell us when your details change, such as your name, address, contact details, work, income or bank account, so that we can keep them accurate.

Information you give us

- Your phone number and email address, when you register.
- Identity details, when you verify your account: your name, date of birth, nationality and home address, your Emirates ID or passport, and a selfie or short video of your face that we match to your identity document.
- Your answers to our onboarding questions about your work, income, source of funds and any public role, and any documents we ask for to support them.
- Details of the bank account you register with us, and your authority for us to collect payments from it.

- Records of your communications with us, including chats, calls and emails with our support team.

Information we receive from others

- Identity verification results from our identity verification provider.
- Results of the screening checks the law requires us to carry out, against sanctions lists, lists of politically exposed persons and media reports, both when you join and while you remain a customer.
- Fraud prevention signals from specialist providers, such as indicators that a phone number, email address or device has been associated with fraud.

To verify your identity, we take a selfie or short video of your face and match it to your identity document. This also confirms that you are a real person. Your facial image and the biometric data created from it are sensitive personal data. We use them only to verify your identity and prevent fraud, and only staff who need them can access them. Screening checks may also return information about criminal matters, which we protect in the same way. We do not collect any other sensitive personal data, such as health information or data about race, religion or political opinions.

Information collected automatically

- Device and technical data: device type, operating system, app version, language settings and IP address, which we need for security and to deliver verification codes.
- Usage data: how you move through the app and website, and crash and diagnostic logs.

Payments

We keep the details of your registered bank account, because we use it to collect payments from you and to make payments to you. If you pay by card, your card details are collected and processed by our payment provider and are not stored on Tenor's systems. We receive confirmation of your payment, not your card details.

3. Legal bases

We process your personal data:

- To perform our contract with you, or to take steps you ask for before entering into it: operating your account, your purchases and your payments.
- To comply with our legal obligations: verifying your identity, including the face check described in section 2, carrying out anti money laundering and sanctions checks, keeping required records, keeping your data secure and reporting to the authorities.

- To establish, exercise or defend legal claims: such as recovering sums due under our terms or responding to a dispute.
- With your consent: marketing communications, and analytics that are not needed to provide our service. You can withdraw consent at any time in the app or by contacting us. Withdrawal does not affect processing that has already taken place.

4. Automated decisions

Some of our checks run automatically, such as parts of identity verification and screening. If we make a decision about you solely by automated means, and it has legal effects for you or affects you significantly, you can ask for a member of our team to review it. Contact us using the details in section 12.

5. How we use your information

We use your personal data to:

- Create and operate your account, and provide the app and website.
- Verify your identity, carry out screening checks and meet our know your customer, anti money laundering and sanctions obligations.
- Process your purchases, including orders, payments, cancellations and deliveries.
- Collect payments, send payment reminders and manage missed payments.
- Provide customer support and respond to you.
- Send service messages, such as verification codes, payment confirmations and changes to our terms. Service messages are not marketing and cannot be opted out of while you use Tenor.
- Improve our product, diagnose problems and keep the platform secure.
- Meet our legal and regulatory obligations and respond to lawful requests from authorities.
- Send you marketing, including offers tailored to how you use Tenor, and ask for your feedback through surveys, where you have agreed. See section 8.

We may also turn personal data into anonymised or grouped data that can no longer identify you. We use it for statistics, to improve our product and to report to our shareholders, investors and finance providers under our agreements with them.

We use your personal data only for the purposes in this policy. Before using it for a different purpose, we will tell you and, where the law requires, ask for your consent.

6. Who we share it with

We share personal data only where needed, with protections in place:

- Our identity verification and screening providers, which receive the details needed to verify your identity and carry out screening checks.
- Our payment provider, to process your payments.
- Our supply, storage and delivery partners, which receive the details needed to supply, store, transfer and deliver your purchase, including your identity details where they must carry out their own checks.
- Cloud hosting and IT providers that run our infrastructure on our instructions.
- Providers that send our messages to you by SMS, email, WhatsApp and app notification, and that help us run customer support.
- Analytics and app performance providers that help us understand how the app and website are used and fix problems.
- Companies in our corporate group, where needed to operate Tenor.
- Professional advisers, such as lawyers, accountants and auditors, bound by confidentiality.
- Government and regulatory authorities, including those responsible for anti money laundering and our licensing authority, and courts and law enforcement, where the law requires us to disclose.
- Anyone we need to share it with to establish, exercise or defend our legal rights, such as recovering sums due under our terms.
- A prospective buyer or investor in a sale, restructuring or financing of our business, under appropriate safeguards.

Providers acting on our instructions may use your data only to deliver their service to us and must protect it. Our app and website may contain links to third party sites, which may have their own privacy policies.

7. Where your information is stored

We and our service providers may store and process your personal data in the United Arab Emirates and in other countries. We transfer personal data outside the UAE only where the PDPL allows it. We may transfer it to a country whose laws, or whose agreement with the UAE, protect personal data to an adequate standard. Otherwise, we transfer it only in the cases the PDPL permits, such as under a contract that requires the recipient to protect your data to the standard of the PDPL, where the transfer is needed to perform our contract with you, or with your express consent. You can ask us for details of the safeguards we use.

8. Marketing and cookies

Marketing. With your consent, we may send you offers and product updates by push notification, SMS, email and WhatsApp. We may tailor them to how you use Tenor, and we may ask for your feedback through surveys. You can opt out at any time in the app's settings or through the message itself. Opting out does not affect service messages.

Cookies. Our website uses necessary cookies to function and analytics cookies to understand how it is used. You can withdraw your consent to analytics cookies at any time, and you can manage cookies through your browser settings.

9. How we protect it

We protect your personal data with appropriate technical and organizational measures, with access limited to those who need it. No transmission over the internet is completely secure, so please also protect your device and verification codes. If a personal data breach occurs that puts you at risk, we will notify the UAE Data Office and affected users as required by law.

10. How long we keep it

We keep your personal data while your account is active, and afterwards for as long as the law requires us to keep records of that kind. We keep identity and verification records for up to 10 years after our relationship with you ends, and transaction records for up to 10 years after the transaction is completed. We keep records for longer where the law requires it, or where they are needed for an investigation, a dispute or a legal claim. When data is no longer needed, we delete or anonymise it. If you opt out of marketing, we keep a record of that so we can respect it.

11. Your rights

You have the following rights under the PDPL:

- Information: ask what personal data we process about you, why, who we share it with and how long we keep it.
- Correction: ask us to fix inaccurate or incomplete data.
- Deletion: ask us to delete your data in certain circumstances.
- Restriction and objection: limit or object to certain processing, including marketing.
- Portability: receive certain data in a machine readable format or have it sent to another provider.

- Automated decisions: ask for a person to review a decision made solely by automated means, as described in section 4.
- Withdraw consent: at any time, where processing is based on consent.
- Complain: to the UAE Data Office if you believe we have mishandled your data.

To exercise any of these rights, contact us using the details in section 12. We may ask you to verify your identity first. We aim to respond within 30 days. We do not charge a fee unless a request is clearly unfounded or excessive, in which case we may refuse it or charge a fee. We may also refuse or limit a request where the law allows or requires us to.

12. Contact

For any question about this policy or your personal data:

- Email: admin@tenorinpl.com
- Our data protection lead oversees compliance with this policy and can be reached at the email above.

13. Changes to this policy

When we update this policy, we will post the new version here with an updated "last updated" date. For material changes, we will notify you in the app or by SMS or email before the changes take effect.

14. Definitions

In this policy:

- Anonymise: to change personal data so that it can no longer be linked to you and you can no longer be identified.
- Automated means: a program or system that operates automatically, with no human involvement or only limited human involvement.
- Biometric data: personal data produced by technical processing of a person's physical or behavioral characteristics, such as a facial image, that allows or confirms that person's identification.
- Consent: your specific, informed and unambiguous agreement to the processing of your personal data, given by a statement or a clear action.
- Controller: the organization that holds personal data and decides how and why it is processed.
- PDPL: Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

- Personal data: any information relating to an identified person, or to a person who can be identified directly or indirectly, such as a name, identification number, picture or location. It includes sensitive personal data and biometric data.
- Personal data breach: unauthorized or unlawful access to personal data, or its disclosure, loss or alteration.
- Politically exposed person: a person who holds, or has held, a senior public role in the UAE, abroad or in an international organization.
- Processing: any operation carried out on personal data, such as collecting, storing, using, sharing or deleting it.
- Screening checks: checks of your details against sanctions lists, lists of politically exposed persons and media reports.
- Sensitive personal data: personal data that reveals a person's family, racial origin, political or philosophical opinions, religious beliefs, criminal record, biometric data or health.
- UAE Data Office: the federal authority, established by Federal Decree-Law No. 44 of 2021, that oversees the PDPL.