Friym - FIDEVO GROUP SAS

Privacy Policy - v4.0 - effective since 2026-09-16

Privacy Policy

> **Version 4.0 — published on 8 September 2026, effective 16 September 2026.** It replaces version 3.0 of 21 July 2026. Previous versions remain available as PDFs at the bottom of this page.

Before you scroll through this document, please read this first

Writing a privacy policy that suits everyone is difficult. Most Friym users want a short, easy-to-understand text. We would like to say everything in a few lines, but our legal obligations require us to spell out certain points precisely.

With that in mind, we have written this document as simply as we could, so that you can understand and control the information we collect, how we use it, and the occasions on which it may be shared.

If you do not wish to read this document in full, remember at least this:

Closing your account does not erase everything See what actually happens	**We collect certain data about you** See what we collect and why	**Your data is hosted in the European Union** See where, and with whom
Your private messages are not end-to-end encrypted See why	**Your feed is ranked by an algorithm** See how	**We never use your data for external advertising** See how we use it

Executive Summary

- **1. Who we are** - Friym is operated by FIDEVO GROUP SAS, a Beninese company registered in Porto-Novo.
- **2. What changed in this version** - What is new or corrected compared to version 3.0, retention in particular.
- **3. Data we collect** - Your account, your profile, your content, your activity, and if you sell, your identity.
- **4. What we do not collect** - Your address book, your banking details, and no biometric data.
- **5. How we use your data** - To run the service, rank your feed, process your transactions and meet our legal obligations. Never for external advertising, never sold.
- **6. About messaging** - Your private messages are not end-to-end encrypted, which allows us to keep the platform safe and moderated.
- **7. Recommendation and personalisation** - Your main feed is ranked by an algorithm whose parameters are published.
- **8. Where your data is** - On our own servers in Paris, with backups in the Netherlands. Both inside the European Union.
- **9. Who we share data with** - Three providers, not one more. Never sold or rented to third parties.
- **10. How long we keep your data** - The detail, line by line, including what has no expiry.

---

1. Who we are

Friym is operated by **FIDEVO GROUP SAS**, a Beninese company registered under number RB/PNO/25 B 6467, Porto-Novo, Republic of Benin. FIDEVO GROUP SAS is the controller for the processing described in this document.

For any question about your data: **privacy@friym.com**.

---

2. What changed in this version

This version corrects and completes the previous one. The following points deserve your attention, whether or not you read the rest:

- **The wording "your data is erased within 30 days" has been removed, because it was inaccurate.** The 30 days that follow the closure of an account are a window during which you can undo it. After that, it is not the data that disappears: it is the ability to restore it. Section 11 explains exactly what happens to each category of content.
- **We publish the full inventory of our retention periods**, including the data that does not expire (section 10).
- **We state where your data is**: on our own servers in Paris, with backups in the Netherlands (section 8).
- **We name our only three processors** and the single transfer outside the European Union that remains (section 9).
- **We describe seller identity verification as it is actually performed**: by a member of our team, by hand, with no third-party provider and no biometric processing (section 14).
- **We document the account protections available to you**: two-step authentication, backup codes and backup e-mail, along with what we keep of them (section 12).
- **We document collections that were not described**: backup e-mail, error telemetry, location attached to a post, search history, local storage on your device.

---

3. Data we collect

3.1 Your account

- **On sign-up**: your e-mail address or your Google/Apple account, your username, your date of birth and your gender.
- **Backup e-mail**: you may declare a second address, which we confirm with a one-time code sent to it. It is used solely to restore access to your account.
- **Authentication factors**, if you enable any: the secret used to verify the codes from your authenticator app, and a non-reversible fingerprint of your backup codes. Neither of these can be used to sign in on your behalf. See section 12.2.
- **Sessions and devices**: the technical identifiers of your open sessions and the associated device, needed to keep you signed in and to let you revoke a session.

3.2 Your profile and your content

- **Your profile**: picture, bio, display name - all optional and editable.
- **Your content**: posts, comments, messages, products, media.
- **Audio content**: voice comments and sounds attached to a post. A voice recording is personal data and is treated as such.
- **The location attached to a post**: if you choose to associate a place with a post, the corresponding coordinates are stored with that post and used for nearby content discovery. This information follows the post: it has no expiry of its own.

3.3 Your activity

- **Search history and related interactions**: your searches and the results you tap are kept to improve your later searches and to feed your recommendations. The app only displays a limited number of them; the retention itself is not time-limited.
- **Recommendation signals**: what you view, what you hide, what you ask to see less of. Section 7 explains how they are used.
- **Follows, blocks, social interactions**: required for the network to function.

3.4 Technical data

- **Connection data**: IP address at the time of connection, device type and model, operating system version, app version.
- **Error telemetry**: when an error occurs in the app, we receive its technical context. Such a report may be sent by a device that is not signed in to any account, deliberately, so that errors occurring before sign-in also reach us. We automatically redact authentication tokens, e-mail addresses and phone numbers written in international format. **This redaction has a known limit: a number written without a country code may not be redacted.** These records are kept for 30 days.
- **Push notification token**: a technical identifier issued by your device's operating system, required to send you a notification.

3.5 On your device

The app keeps locally, on your phone, a cache of your recent requests, your drafts and files being uploaded, as well as a queue of actions taken offline and messages not yet sent. This data stays on your device, is not transmitted to us until the action is carried out, and disappears when you uninstall the app.

3.6 If you open a shop

- **Identity verification**: a selfie holding your identity document, the front of the document and its back where one exists, the document type and number, your full name.
- **Payout details**: Mobile Money number, operator, country, account holder name.
- **Fingerprint of the identity document**: we compute a technical fingerprint of the document you provide in order to detect the same document being used across several accounts. This fingerprint serves an anti-fraud purpose only.

See section 14 for what we do with it.

3.7 If you use a partner code

If you enter a code from an Influx partner in the days following the creation of your account, we record the link between your account and that partner, the code used, and the time elapsed between account creation and entry. **This link is permanent and cannot be undone.** It is visible neither on your profile, nor to the partner, nor to any other user: only our internal team can see it. The programme's rules are set out in the Influx Partner Programme Terms.

---

4. What we do not collect

- **Your address book.** Friym does not sync your contacts and has no technical means of doing so.
- **Your banking details.** Friym stores no card number and no complete payment data. Payment is handled by our provider.
- **No biometric data.** The selfie requested during identity verification is looked at by a person on our team. We extract no facial template from it, and no automated comparison is made between your face and your identity document.

---

5. How we use your data

We use your data to:

- run your account, your profile and your content;
- **rank and personalise your feed and your suggestions** (see section 7);
- process your orders when you buy or sell, and pay sellers what they are owed;
- verify your identity when you open a shop, and prevent fraud;
- keep the service safe, handle reports and enforce our rules;
- send you service-related notifications;
- fix technical errors in the app;
- comply with our legal obligations, in particular tax and accounting ones.

We do not use your data for external advertising and we do not sell it.

---

6. About messaging

Unlike some messaging apps, messages exchanged on Friym are not end-to-end encrypted: they are therefore not unreadable to us. This choice allows us to better ensure the safety and moderation of the platform, for example to detect fraud or abuse, or to act on a report. Access to this data remains strictly limited internally and governed by the rules described in this document.

Private messages are kept for **one year**, then deleted.

When someone you are talking to closes their account, the conversation becomes read-only and their identity in it is replaced by a generic label. Your own messages remain readable to you.

---

7. Recommendation and personalisation

Your main feed is not chronological: it is ranked by an algorithm, based on your follows, your interests, what is popular on the platform and your past interactions.

The parameters of this ranking - the share of each source, the criteria that push a post up or down, the signals you can send to influence it - are published in a separate document: the Recommender System Transparency Notice.

Two points of honesty, as of the publication date of this document:

- the app **does not yet explain to you, post by post, why it is being shown to you**;
- the app **does not yet offer an alternative feed that is not based on your profile**.

Both features are identified and still to be built. We would rather write it down than let you guess.

---

8. Where your data is

	Location
Our production servers - app, media, payments, databases	**Paris, France**
Our backups	**Netherlands**

Both are located in the European Union.

We host our data ourselves. We use no third-party cloud storage service, no external content delivery network, and no third-party managed database. This includes the media you post and **the identity documents and selfies submitted for seller verification, which never leave our servers**.

---

9. Who we share data with

We do not sell or rent your data. We pass it to three providers, each for a specific function:

Provider	What it does for us	What it receives
PawaPay	Mobile Money collection and payout	Phone number, operator, country, amount, order reference
Expo Push Service	Delivery of push notifications	Your device's notification token, the title and body of the notification
Hostinger	Sending our e-mails (one-time codes, security alerts, verification notifications)	Your e-mail address and the content of the message

Only one of these flows leaves the European Union: Expo Push Service, operated from the United States. Since the body of a notification may contain an excerpt of a message or a profile name, we prefer to flag this explicitly rather than bury it in a list. You can disable push notifications from your device or app settings; no data is then sent to this provider.

We also use an internal technical alerting channel, which receives incident messages intended for our team and is not meant to receive personal data.

---

10. How long we keep your data

10.1 What expires automatically

Data	Duration
One-time code sent by e-mail	90 days
Session (refresh token)	30 days
Access token	15 minutes
Recent proof of identity for a sensitive operation	10 minutes
Sign-in procedure in progress	5 minutes, invalidated after 5 attempts
Unconfirmed activation of an authentication factor	15 minutes
Cancellation link sent by e-mail	7 days
In-app notification	30 days
Private message	**1 year**
Post draft	At its expiry date
Error telemetry	30 days
"Already seen" trace and negative feed signals	30 days

Data	Duration
Invitation to join a Page team	7 days
Window to enter a partner code	3 days after account creation
Restoration window for a closed profile or account	30 days
Deadline to appeal a sanction	7 days
Waiting period before resubmitting a rejected verification	1 day

10.2 What does not expire automatically

The following data has no technical expiry. We would rather say so plainly than announce a duration the service would not honour:

- your posts, comments, products and orders - including after your account is closed, under the terms of section 11;
- the location attached to a post;
- your search history and the related interactions;
- the reports you submit or that are made about you, along with sanctions and appeals, which stay attached to the account;
- a Page's activity log;
- financial data: transactions, payouts, balances;
- the link to an Influx partner;
- identity verification data, which follows the specific rule below.

10.3 Identity verification data

The identity documents, selfie, full name and document number submitted to open a shop are kept for **five years from the end of the commercial relationship** - that is, from the closure of your shop or the end of your selling activity. This starting point is more protective than the date on which you submitted your documents.

This retention serves two needs: the retention of identity records required by applicable regulation, and fraud prevention. Deletion at term is currently an operation we carry out ourselves, not an automatic mechanism.

The technical fingerprint of the identity document, described in section 3.6, may be kept beyond that period for the sole purpose of detecting fraudulent reuse of the same document. It cannot be used to reconstruct your document.

---

11. Closing your account: what "delete" actually means

This is the most important section of this document, and the one where it would have been easiest to let you believe otherwise.

11.1 The first 30 days

When you close a Page or your entire account, access is cut immediately. For **30 days**, the operation remains reversible: you can come back and find everything as it was.

11.2 After 30 days

After that period, your record is moved to an archive space separate from the live service. This move releases two things, and only two: your e-mail address becomes usable again to create an account, and the username of a closed Page becomes available to someone else.

This move is not an erasure. Each archived record then follows one of two outcomes:

- it is **de-identified** - what ties it to a person is removed, and what remains is no longer personal data;
- or it is **kept as is** where it remains necessary for a legal or security reason: accounting obligation, ongoing dispute, fraud investigation.

This sorting is currently carried out by our team and not by an automatic mechanism.

11.3 What happens to your content

Your posts and comments are **neither deleted nor hidden**. Their status changes:

	After your account is closed
The author shown	Becomes "Friym User" - your name and picture disappear
Distribution in the feed, trends, suggestions, explore, search	**Stopped**
Access via direct link and within comment threads	**Maintained**
Private conversations	Become read-only, your identity in them is replaced
Follows and followers	Marked, and restorable if you return within 30 days
A Page's username	Released after 30 days

The reason for this choice is simple: removing this content would punch holes in conversation threads written by other people, and in order histories, where a buyer needs to find what they bought.

11.4 What this means for your right to erasure

If you request the erasure of your data, the honest answer is this: we de-identify what can be de-identified, and we keep what the law or the safety of the platform requires us to keep, telling you which of those two answers applies to your request. Write to us at **privacy@friym.com**.

---

12. How we protect your data

We apply standard industry practice: encrypted connections, internal access limited to the people who need it, identity documents stored privately and never publicly accessible, and an encrypted, certificate-authenticated link with our payment provider.

12.1 How you sign in

Friym does not use passwords. You sign in with a one-time code sent to your e-mail address, or through your Google or Apple account. There is therefore no password of yours for us to store, or for anyone to steal from us. In return, **access to your mailbox is access to your Friym account**: protect it accordingly.

12.2 The protections you can turn on

- **Two-step authentication.** You can require, in addition to the code received by e-mail, a temporary code generated by an authenticator app of your choice. We keep the secret needed to verify those codes, never the codes themselves.
- **Backup codes.** A batch is issued to you on activation, **shown only once**. We keep no readable form of them: neither our team nor our support can restore them. Generating a new batch immediately invalidates the previous one.
- **Backup e-mail.** A second address, confirmed by a code, used solely to restore your access.

Any activation or revocation of a factor is notified to you by e-mail, with a link allowing you to cancel the operation for 7 days if you are not behind it.

> **A warning, because it genuinely concerns you.** These protections work because we cannot bypass them. Losing both your authenticator app and your backup codes may result in **permanently losing access to your account**: we will have no way to give it back to you.

12.3 The protections we apply without asking

- **Recent proof of identity.** Any operation affecting your means of access requires an authentication less than 10 minutes old, tied to the device you are using. A long-standing open session is not enough.
- **Stronger verification for two operations.** Changing your payout details and transferring a Page to someone else require validation of a strong factor. These are the two operations through which a compromised account would do the most damage.
- **Attempt limits.** A sign-in procedure expires after 5 minutes and is permanently invalidated after 5 failed attempts.

No online service is 100% invulnerable. Should an incident affect your data, we undertake to inform you within a reasonable time.

You can report a security vulnerability to **security@friym.com**.

---

13. Your rights

You have rights of access, rectification, objection, restriction and portability over your data, as well as a right to erasure under the conditions and limits set out in section 11.4.

These rights are exercised by writing to **privacy@friym.com**. You can also close your account yourself from the app settings. We respond within 30 days.

Where applicable regulation gives you that right, you may also lodge a complaint with the competent data protection authority in your country of residence.

---

14. Selling on Friym (identity verification)

Only Page profiles can open a shop, and only after identity verification. Until it is approved, you can showcase your products but not collect payment for a sale.

How this verification is done: your documents are reviewed by a member of our team, who decides to accept or reject them. We use no identity verification provider and no facial recognition technology. The only automated check is a comparison of the name you declare with the one associated with your Mobile Money account, performed by our payment provider.

Where your documents are stored: on our own servers, in Paris, in a space that is not publicly accessible.

For how long: see section 10.3.

The full commercial rules - commission, payout, delivery, refunds, disputes - are set out in our Terms of Sale.

---

15. Reports and moderation

When you report content, we record your report, its reason and **your identity as the reporter**. This information is never disclosed to the person reported, but it is kept: it allows us to handle abusive reporting and to reconstruct a contested decision.

When you are the subject of a report or a sanction, the corresponding history is attached to your account, not only to the profile concerned. It has no expiry.

How moderation works - thresholds, measures and appeals - is described in article 12 of the Terms of Service.

---

16. Requests from authorities

Friym may be required to disclose some of your data to a competent judicial or administrative authority, as part of an admissible legal procedure, made in writing and precisely reasoned. We never respond to a merely informal request.

Where there is an imminent danger to a person's life, an emergency request may be handled within 24 to 48 hours, provided it comes from a competent authority and is duly justified.

Unless legally prohibited, we endeavour to inform the user concerned that such a request has been received and handled about them.

Any such request must be addressed to **legal@friym.com**.

---

17. Minors

Access to Friym is restricted to people aged at least 13. Between 13 and 17, a legal guardian's authorisation is required.

Our commitments regarding the protection of minors, and how to report content or behaviour that puts them at risk, are set out in our Child Safety Standards.

18. Changes to this policy

We may amend this policy to reflect changes in the service or in our legal obligations. Any material change will be notified through the app with reasonable notice before it takes effect.

Every published version remains available as a PDF, with its effective date, at the bottom of this page.

19. Contact us

Personal data Email: privacy@friym.com

Security Email: security@friym.com

Legal enquiries Email: legal@friym.com

Content reports Email: report@friym.com

Appealing a sanction Email: appeals@friym.com

Child safety Email: childsafety@friym.com

Address FIDEVO GROUP SAS, Porto-Novo, Republic of Benin