Vortex

Privacy notice for end users

Last updated: November 2, 2026
https://www.vortexvip.org/en/end-user-privacy

This page is a translation of the Spanish original. If they differ, the Spanish version prevails.

1. Who it applies to and who is responsible

This notice applies to the people who use the Vortex app (as it appears on Google Play) or the app of a service that runs on Vortex. The company or institution that gives you access to the service is «your provider».

Your provider is responsible for your data (the controller). Vortex provides it with the technology and processes your data as a processor: only on your provider's behalf and following its instructions. The data of the companies that hire Vortex is described in the Vortex privacy policy (https://www.vortexvip.org/en/privacy).

2. Which data is processed and why

The data is recorded by you when you create your account, or by your provider. It is:

- **Name, email and phone:** to create your account, send you your provider's emails and let your provider contact you.
- **Username and password:** to sign in to the apps. The password is stored hashed, so nobody can read it.
- **Profiles, including kids' profiles with a parental PIN:** to keep each household member's history and preferences apart and protect children's profiles.
- **Viewing history:** for continue watching, to remember the audio and subtitles of each title, and to calculate your provider's audience metrics.
- **Devices:** to sign in on the TV and manage your account's sessions.
- **Plan and payment dates recorded by your provider:** to know until when you have access and to send you renewal notices.
- **Interactions with the emails:** to make sure your provider's emails reach you.

3. Technical data from the app

The app integrates Firebase services (Google LLC), which Vortex uses to detect failures and improve the app: Firebase Crashlytics keeps crash reports with installation identifiers, device model, memory and app version, for 90 days; Firebase Remote Config uses the Firebase installation identifier to choose the app's settings; and Google Analytics for Firebase records usage events linked to an identifier of the app installation. This data is pseudonymous, not anonymous. These services operate under Google's privacy policy, available at policies.google.com/privacy.

4. Metrics and emails

With the viewing history, Vortex calculates audience metrics for your provider: what is watched, how much and on which type of device. Only your provider sees them. Vortex does not use them for its own purposes or sell them.

The automatic emails (welcome, renewal, catalog news) are sent at your provider's instruction and on its behalf. Vortex never uses your data to promote its own services and never sells it.

5. Kids' profiles

The account holder, who must be an adult, can create profiles for children and protect them with a parental PIN. The apps show no advertising. Data from kids' profiles is not used to build commercial profiles. Your provider is responsible for obtaining parental or guardian authorization where its law requires it.

6. Who it is shared with

Vortex uses these providers (sub-processors) to deliver the service:

- A server provider in the European Union: the platform's servers and database.
- Google (Firebase): crash reports, analytics and app settings.
- Resend: email delivery.
- Cloudflare (Turnstile): bot protection on forms.
- Vercel: hosts the website and the console.
- Google Play: app distribution.

Vortex hands over data only upon an order from a competent authority or when a law requires it. We check that the order is valid, hand over only what is requested and notify your provider beforehand, unless the law forbids it.

7. Where it is stored and how it is protected

The data is hosted on servers located in the European Union. The Vortex team administers it from Costa Rica, and some sub-processors (for example, Google, Resend, Cloudflare and Vercel) operate in the United States.

Communications between the app and our servers are encrypted (HTTPS) and passwords are stored hashed. If Vortex confirms a security incident affecting your data, it notifies your provider without delay and no later than 48 hours, so your provider can notify you and the authorities where the law requires it.

8. How long it is kept

Your data is kept while your account exists and your provider uses Vortex. If your provider leaves Vortex, the data is deleted after the period it has to ask for a copy (30 days). Technical records (logs) are kept for a short period, usually no more than 3 months.

9. Your rights

You can ask to access your data, correct it, delete it, receive a copy or object to certain processing, according to the law of your country. Write to your provider. If you write to us (soportevortextv@gmail.com), we send your request to your provider and let you know.

10. Delete your account

You can ask for your account and its data to be deleted as explained on the Delete your account (https://www.vortexvip.org/en/delete-account) page.

11. Data protection authorities

If you believe your rights were not respected, you can go to the data protection authority of your country: for example, PRODHAB (Costa Rica), the ANPD (Brazil), the AAIP (Argentina), the Superintendence of Industry and Commerce (Colombia), the National Authority for Personal Data Protection (Peru) or the Anti-Corruption and Good Governance Secretariat (Mexico).

12. Contact

Email: soportevortextv@gmail.com · WhatsApp: +506 8346 1166