Vortex

Vortex privacy policy

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

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

1. Introduction and scope

At Vortex we respect the privacy and the protection of the personal data of our clients. This Privacy policy describes what data we collect from the Clients of the Vortex platform (and, in certain cases, data of their end users for the proper use of the Vortex platform), why we collect it, how we use, store and eventually disclose it, and the rights and choices Clients have regarding their data.

This policy applies to the information Vortex obtains through the use of its service and the associated applications (including the Vortex mobile app, available on the Google Play Store under the identifier org.vortextv.playall). Since Vortex offers its services internationally, we strive to comply with the privacy principles common to the applicable jurisdictions, including the data protection laws of Latin America, Europe (GDPR) and other regions, as applicable.

By using the Vortex platform or providing us with personal data, the Client accepts the practices described in this Policy. If the Client does not agree with this policy, it must refrain from using the Service or providing personal information. We may update this Policy from time to time to reflect changes in our practices or legal requirements, which will be notified to the Client through the usual channels; continued use of the Service after such changes constitutes acceptance of the updated Policy.

(Note: in this Policy, references to the «Client» mean the natural or legal person that hires and uses Vortex. Vortex acts mainly as a provider to the Client and has no direct relationship with the end users the Client manages on its streaming platform. Any end-user data processed by Vortex is processed solely on behalf of the Client, as detailed below.)

The data of the people who use our Clients' apps (end users) is described in the Privacy notice for end users (https://www.vortexvip.org/en/end-user-privacy): there, the Client is the controller and Vortex acts as processor.

2. Personal data collected

- **Data provided by the Client:** when registering and using Vortex, the Client may give us certain personal data needed to provide the service, such as: the name or legal name of the company, the name of the contact person, email, phone number, billing information (for example, tax ID, tax address) and platform configuration information (for example, names of admin users, logos, brands to integrate, secret keys and access tokens, etc.). This data is requested for the sole purpose of creating the Client's account, identifying it correctly, managing the contractual relationship and providing the Service (including service communications, technical support and billing).
- **Demo requests and business contacts:** when a company asks for a demo on the website or writes to us, we keep the data it sends (name, email, organization, country, type of organization, expected size and message) to answer it and prepare the demo. The form uses Cloudflare Turnstile to tell people from bots.

- **Support:** the messages the Client sends us by email or WhatsApp, to handle its request.
- **Website visitors:** the www.vortexvip.org website does not use cookies. We use Vercel's cookieless analytics, which counts visits in aggregate (for example, pages viewed, country and type of device) without identifying people.
- **Data collected automatically:** while the platform is used, our systems may automatically collect certain technical data needed for the operation and security of the service. This includes, for example: IP addresses, timestamps of logins and relevant actions, system event records (logs of operations performed in the backend), information about the device used to access the app (model, operating system, app version) and performance or diagnostic metrics in case of errors. This data is collected to monitor the proper functioning of the platform, detect failures, provide support and ensure the security of the Client's account (for example, detecting unauthorized access).
- **Data collected by services built into the app:** the Vortex app integrates Firebase services (Google LLC): 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.
- **Data of the Client's end users:** Vortex processes it as a processor, on the Client's behalf, and it is described in the Privacy notice for end users (https://www.vortexvip.org/en/end-user-privacy). It is the Client's responsibility to have the consent or appropriate legal basis from its end users. If an end user contacts Vortex to exercise rights over their data, Vortex will forward the request to the Client, as the controller of that data.
- **Sensitive data:** Vortex does not require or ask the Client for sensitive personal information to provide the service. Sensitive data means data about racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, personal financial information (beyond what billing needs) or other data that the applicable law considers a special category. The Client must refrain from entering sensitive data of third parties or of its end users into the platform, since Vortex is not designed to store or protect information of that nature under special standards beyond the general security measures described in this policy. If sensitive data is entered into the system inadvertently, the Client assumes full responsibility for it.

3. Purpose and use of the data

The personal data collected will be used strictly for the legitimate and necessary purposes of operating Vortex. In particular:

- **Providing the Service:** we use the Client's registration information (name, contact, etc.) to create and manage its account, authenticate logins, provide the contracted features (backend, Android app) and, in general, fulfil our contractual obligations. For example, the Client's email may be used as the login user and to send important notices about the service (updates, maintenance notices, security alerts, etc.). The end-user data the Client loads into the platform will be used to enable the corresponding features (for example, allowing those users to sign in to the streaming app, applying the content settings defined by the Client, recording content consumption, etc.). With the viewing history, Vortex calculates audience metrics for the Client (what is watched, how much and on which type of device), which only the Client sees in its console. Vortex does not use them for its own purposes or sell them.

- **Customer care and technical support:** the contact information provided may be used to give support and resolve questions or issues reported by the Client. If the Client opens a support ticket, Vortex may access certain data of its instance (for example, review logs or specific settings) for the sole purpose of diagnosing and solving the reported problem. These operations are carried out under strict confidentiality.
- **Billing and administration:** identification and tax data are used to issue invoices, process payments, keep internal accounts and comply with tax obligations. For example, the tax ID or address is included in electronic invoices as the regulations require, when needed. We may also use the contact information to send payment reminders, transaction confirmations or subscription expiry notices, when applicable.
- **Platform improvements:** Vortex may process aggregated and anonymous usage data (for example, general performance statistics, number of connections, types of devices used, etc.) to analyze the performance of our platform and find areas for improvement. This analysis helps us optimize the infrastructure, plan updates and improve the experience of the client and its end users in future versions. In these cases no personally identifiable information is analyzed, only overall metrics and data analysis.
- **Legal self-defense and regulatory compliance:** we keep certain activity records and log data to protect our legal rights in case of disputes, detect fraud or abuse of the service and comply with regulatory requirements. For example, some countries require access records to be kept for a minimum time for security reasons. Likewise, in a possible lawsuit we may need to prove actions taken (for example, consent given, dates of use, etc.), for which the logs serve as evidence. We will only use personal data for this purpose when necessary and in accordance with the law in force.

Under no circumstances will Vortex use the personal data of the Client or its end users for its own or third-party marketing purposes without their express consent. Nor do we build commercial profiles or make automated decisions affecting the Client based on the automatic processing of its personal data.

The automatic emails to end users (welcome, renewal, catalog news) are sent at the Client's instruction and on its behalf. Vortex never uses end users' data to promote its own services.

4. Data retention and deletion

Vortex will only store personal data for as long as needed to fulfil the purposes described in this Policy, unless a longer retention period is required or permitted by the applicable law. We apply internal data retention policies to make sure we do not keep personal information longer than required. In general:

- **Client account:** the Client's account data (registration, contact and billing information) is kept active for as long as the contractual relationship lasts and the Client keeps an operating account in Vortex. If the Client cancels the service, that information may be kept in our files for a limited additional period (usually a few months) while it may be needed for post-cancellation matters (for example, issuing a final invoice, resolving disputes or reactivating the service at the Client's request). After that period, the data will be securely deleted or anonymized, except to the extent we must keep some of it due to legal obligations.
- **End users:** the end-user data stored on the platform by the Client (for example, its user lists or settings) is kept until the Client deletes it and while the Client's account is active. Vortex does not purge or delete end-user data on its own initiative, since it acts as a store following the Client's instructions. The Client can add, change or delete that data with the tools provided (administration

tool, APIs, etc.). If the Client's account ends, the Client may ask by email, within the following 30 days, for an export of its data, as the Terms (https://www.vortexvip.org/en/terms) say; after that period, Vortex deletes all the associated end-user data, following a secure process.

- **Logs and technical records:** logs and technical records with minimal personal information (for example, IP addresses, login events) are kept for a short, predefined period, typically no longer than 3 months, unless they need to be kept longer because misuse or security incidents are detected. We keep these temporary records mainly to ensure the security of the platform and as evidence in case of lawsuits or legal investigations.

After the standard period, logs are deleted or anonymized so that they can no longer be linked to an individual. Where we must preserve a specific record beyond that period, the record will be isolated and protected until the legal need is resolved, after which it will be deleted immediately.

Once the purposes are fulfilled or the relationship with the Client has ended, and the periods above have passed, Vortex will securely delete or anonymize the personal data so it cannot be recovered. Anonymization means the data is transformed in such a way that it can no longer be associated with an identifiable person. Vortex reserves the right to keep and use anonymized data for legitimate business purposes (for example, overall statistics). Although Vortex makes regular security backups of its databases, any data actively deleted by the Client or by us as described above is also deleted from the backups.

4a. Request to delete your account and data

People who use our Clients' apps can ask for their account to be deleted as explained in the Privacy notice for end users (https://www.vortexvip.org/en/end-user-privacy) and on the Delete your account (https://www.vortexvip.org/en/delete-account) page. Vortex processes these requests on behalf of the responsible Client and lets it know.

5. Sharing information and disclosure to third parties

At Vortex we do not share the Client's personal data with third parties, except in the limited circumstances described below. Under no circumstances do we sell personal data to third parties for commercial purposes. The Client's information is confidential and handled with the utmost discretion. We may only disclose personal data to parties outside Vortex in any of these cases:

- **Subcontracted service providers:** Vortex may use trusted third-party services to support the infrastructure or certain functions of the Service (for example, cloud hosting, email delivery, the payment method the Client uses to pay its monthly fee, or support tools). To the extent necessary, some Client data may be processed or stored on these providers' systems, but always under our instructions and control, and only to provide the contracted service. For example, we use a secure data center to host the servers: the Client's information resides on those servers, but the hosting provider does not access or use that data on its own account. We contractually require all our providers to meet confidentiality obligations and security measures equivalent to ours, so that the data remains protected.
- **Legal requirements and court orders:** Vortex may disclose the Client's personal data if required by a competent government authority, through a duly grounded court or administrative order or legal mandate, or if needed to comply with an applicable law or regulation. In other words, if a court, a prosecutor or another body with legal powers requires us to hand over certain data (for example, in a

criminal investigation, a subpoena or to respond to legal proceedings), Vortex will assess the legal validity of the request and, if it is mandatory, will provide only the information strictly requested and necessary. Before any disclosure, we will carefully verify that the request is legitimate and comes from a competent authority. Whenever the law allows, Vortex will notify the Client of this kind of request before disclosing its data, so it can exercise its right of defense. Likewise, when the situation warrants it, Vortex may formally oppose requests it considers excessive or improper, to protect the confidentiality of its clients' data.

- **Protection of rights and safety:** we may disclose personal information if reasonably necessary to enforce our terms of service or to protect our rights, property or safety, or those of our clients or other people. For example, if we detect fraud, phishing or other unlawful activities on the platform, we may share information with the relevant authorities or with legal advisers, in order to stop that activity and take the corresponding legal action. Likewise, if a client takes actions that harm other users or the system, we may provide the information needed to investigate and stop those acts.

Outside these cases, Vortex does not disclose personal data to any other entity or person. We do not share it with advertisers, with sister companies for cross-marketing, or with interested third parties, unless the Client itself asks us to or explicitly authorizes it (for example, if in the future the Client needs to integrate Vortex with an external partner and asks us to transfer data to it under certain conditions). In that case, it will be documented and governed by a specific agreement. If a merger, acquisition or sale of the Vortex company or its assets is ever considered, which could involve transferring client data to a new entity, we will inform the Client in advance. The successor must respect at least the same level of protection as this Policy. If the Client does not agree with the transfer of its data in that context, it will have the right to ask for its deletion before the transaction is completed.

Current sub-processors:

- 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; the website uses its cookieless analytics.
- Google Play: app distribution.

We will notify Clients 30 days in advance before adding or changing a sub-processor.

6. Information security

Vortex applies appropriate technical and organizational security measures to protect personal data against unauthorized access, alteration, disclosure or destruction. These measures include, among others: encryption of communications between the app or client and our servers with HTTPS/TLS; firewalls and intrusion detection systems in our infrastructure; strict internal access control; encrypted storage of passwords; a robust security structure with dynamic access tokens; and regular backups to prevent data loss. We also run security tests and constant updates to mitigate new vulnerabilities.

Notwithstanding the above, the Client acknowledges that no method of electronic transmission or storage is 100% secure. Therefore, although we strive to protect its personal information, we cannot guarantee absolute security. It is important that the Client also keeps safe practices: for example, protecting its login credentials, using strong passwords and notifying Vortex immediately if it suspects its

account has been compromised. Vortex will not be responsible for breaches or unauthorized access mainly due to the Client's negligence (for example, deliberately sharing its password with third parties, or installing malicious software on its own equipment that steals credentials).

If Vortex confirms a security incident affecting the personal data of the Client or its end users (for example, unauthorized access to our systems that compromises confidential information), it will notify the Client without delay and no later than 48 hours after confirming it, with what is known: what happened, which data and how many people were affected, what measures were taken, and a contact. This way the Client can meet its own deadlines (in Costa Rica, 5 business days to notify PRODHAB and the people affected; in Brazil, 3 business days to notify the ANPD). We will also meet the obligations to notify data protection authorities or data subjects that the laws of any jurisdiction require.

7. The Client's rights over personal data

As the owner of its personal data, the Client has a series of rights under the applicable data protection laws. Depending on the jurisdiction, they may include: the right to access the personal data we hold about it; the right to correct inaccurate or incomplete data; the right to ask for the deletion of its data when no longer needed (right to be forgotten); the right to data portability (to obtain a copy in a structured format); the right to withdraw consent at any time when the processing is based on consent; and the right to object to or ask for the restriction of certain processing in specific circumstances. Vortex will help the Client exercise these rights to the extent they are enforceable and relevant.

For example, the Client can update much of its basic information (such as contact details or passwords) through customer service or in the Vortex administration console, as far as the console allows. For other requests about its personal data, the Client can contact us through the designated support channels (soportevortextv@gmail.com). We will handle requests within the relevant legal time limits and, if needed, ask for the additional information required to verify the identity of the requester (for security). If a request is rejected (for example, because it conflicts with a legal obligation or is excessive), we will give the Client the reasons, unless a law forbids it.

The Client can ask, whenever it needs to, for an export of its own personal data and that of its end users held in its instance (for example, in CSV or JSON), without the technical structure or internal components of the database. Only exports in special formats may have a cost.

We reiterate that, regarding the end-user data loaded by the Client, Vortex is a data processor and cannot directly handle requests from those users without the Client's instructions. If an end user exercises rights directly with us, we will forward the request to the Client so it can decide what is appropriate.

8. International data transfers

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.

When the law of the Client's country requires a mechanism to transfer data to other countries (for example, contractual clauses), that mechanism is included in the Data Processing Agreement Vortex signs with the Client. Our commitment is that, wherever it is stored or processed, the Client's personal data enjoys a level of protection equivalent to that offered in its country.

9. Legal processes and judicial cooperation

As stated, Vortex may need to cooperate with judicial or administrative authorities regarding the Client's data. Our general policy is to protect the confidentiality of our Clients' data to the fullest extent legally possible. If we receive a request to hand over data:

- We will verify the legitimacy and scope of the request. We only comply with orders issued under the law, by competent authorities, and we will stick to the specifications of the order (handing over only the data requested, nothing more).
- We will notify the Client immediately, before disclosing information, so it is aware and can intervene, unless the law forbids it (for example, an order with a confidentiality clause). In emergency notices (for example, data preservation orders) we will do our best to warn the Client promptly.

Vortex hands over data about a Client or its end users 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 the Client beforehand, unless the law forbids it.

10. Contact and questions

For any question, concern or exercise of privacy rights, the Client can contact us by email at soportevortextv@gmail.com (or the equivalent designated channel). We will answer as soon as possible and, in any case, within reasonable time limits. If the Client believes its right to data protection has been infringed and is not satisfied with our answer, it may have the right to file a complaint with the data protection authority of its 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).

Thank you for the trust placed in Vortex. We are committed to handling personal data transparently and securely, as set out above.

We also remind you that Vortex does not provide legal advice to Clients or direct support to the Client's end users on privacy matters; any question from an end user about their data must be channeled through the Client itself, which is responsible for that data towards the user.

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