VITRINA

Data security

Description as of November 18, 2026 · vitrina.cafe/en/security

This page briefly describes how the data of venues on the Vitrina platform is protected as of the date above. It describes how things are set up and is not a contractual commitment: the terms of data processing are set by the contract and the data processing agreement. We may change the measures provided the overall level of protection is not reduced.

A separate system for each venue

Each venue gets its own instance of the system with a separate database. The guest data of one venue is not kept in the same database as the data of other venues.

Where the system runs

The venue's server and database run at Railway, in an EU region (the Netherlands). The ordering website, the admin panel and this website are served by Vercel, and their server functions run in Frankfurt (Germany).

We are preparing our own server in an OVH data centre in Warsaw (Poland). As of the date of this description, no live venue runs on it.

Connections and network

The websites, admin panels and server answer only over HTTPS: an unencrypted request is redirected to HTTPS, and the browser remembers this rule (HSTS).

The DNS of the platform's domains is run by Cloudflare. Requests to the server of a venue that is already live on the platform pass through the Cloudflare network, which filters out denial-of-service attacks. The database has no address on the internet: only the venue's server reaches it, over the hosting provider's private network.

Backups

We copy the database of each venue regularly and encrypt it before upload (at present, for example, every night and with AES-256), and keep the copies in a separate Cloudflare R2 storage located in Eastern Europe; Cloudflare does not guarantee for this storage that it is in the EU. Cloudflare does not have the key to the copies.

Daily copies are kept for 30 days, copies from the first day of each month for 12 months. For its first 28 days a daily copy, and for its first 300 days a monthly copy, cannot be deleted or overwritten with any access key: the storage has a lock rule for this.

The copies are regularly restored into a separate empty database and the row counts of key tables are compared with the live system; as of the date of this description this happens every week. If a check fails or does not run on time, the system raises an alert.

Server access and keys

Our own server can be entered only with an SSH key: password login is turned off, and the administrator (root) cannot sign in from the internet. Railway and Vercel have no separate server login: they are managed through the provider account.

Access keys are issued narrowly: the nightly backup service has its own key, separate from the server's key, and the service that checks the copies can only read them. Service keys and passwords are set in the hosting settings, not in the code.

Staff sign-in

Staff passwords are stored only as a hash (bcrypt), and the number of sign-in attempts is limited.

Owners and managers can turn on two-step sign-in: after the password, a code sent to their e-mail is required. The owner can require it for the Owner and Manager roles. Other roles have no second step.

Important staff actions, such as deleting an employee, resetting a password, changes to the menu, tables and discounts, and actions at the POS, are recorded in an action log with who did them and when. The owner and the accountant see the log in the admin panel.

Payments

Guests enter their card number on the page of the payment provider (Stripe, Comgate, Paynow, LiqPay, monobank, WayForPay), not on ours, so card data does not reach our servers. For a saved card we keep only the provider's token, not the card number.

Personal data processing

For the data of a venue's guests, staff and couriers, the venue is the controller and Complete solution s. r. o. is the processor under Article 28 GDPR (for a venue in Ukraine: the owner and the manager of personal data under the Law of Ukraine on Personal Data Protection). The data processing agreement for Express is part of the Express Terms (vitrina.cafe/en/express-terms#dpa); the template (complete-solution.eu/legal/dpa) for other contracts and the list of sub-processors (complete-solution.eu/legal/sub-processors) are published on the company website.

Reporting a vulnerability

If you find a vulnerability in Vitrina, write to contact@complete-solution.eu and describe how to reproduce it. The same address is given in the security.txt (vitrina.cafe/.well-known/security.txt) file.

While testing, do not open other people's data, do not change or delete it, and do not disrupt the service. We do not run a bug bounty programme.