Privacy Policy

How OpsCore Eventz handles personal information

Version 1.0 · Effective 29 August 2026

Review before you publish this

This document is supplied as a starting point that matches what the software actually does. It has not been reviewed by a lawyer. Your counsel should check it against your jurisdiction, your procurement terms and your records-retention obligations before you rely on it.

1. Roles

The organization running an event decides what personal information to collect and why. In data protection terms that organization is the controller, and the platform is the processor acting on its instructions.

This policy describes what the platform does with personal information. The organization running your event is responsible for telling you why it is collecting what it collects, and for answering requests about it.

2. What the platform holds

The information held depends on what each organization's registration form asks for. Across the platform the categories are:

• Identity and contact details — name, email address, telephone number, employer or district, job title, postal address.

• Registration records — the event registered for, the answers given on the registration form, session selections, dietary and accessibility requirements where asked for.

• Attendance records — check-in and check-out times, session attendance, credit hours earned and certificates issued.

• Financial records — amounts due and paid, invoice and purchase order references, the card brand and last four digits, and the payment processor's reference.

• Account and security records — sign-in times, IP address and browser user agent for administrative actions, and the audit trail of changes made.

• Consent records — which consent statement was accepted, its version, the exact text shown at the time, and when it was accepted.

3. What the platform does not hold

Card numbers, expiry dates and security codes are never stored. Where an organization uses a payment processor, card details go to that processor directly; the platform keeps only the brand, the last four digits and the processor's reference.

Credentials for external integrations are stored so that they cannot be read back through the interface. Once saved, an administrator sees a masked hint only.

4. Why it is held

To register you for an event and confirm your place; to communicate with you about that event; to run check-in and record attendance; to issue certificates and credit hours; to invoice and record payment; to meet the organization's own record-keeping and audit obligations; and to keep the platform secure.

5. Who it is shared with

Personal information is scoped to the organization that collected it. Staff of one organization cannot see another organization's registrants.

Information is shared outside the platform only where the organization has configured it: with a payment processor to take payment, with a finance system to record a transaction, with an email or SMS provider to deliver a message, or with an identity provider for single sign-on.

Public event pages show only what the organizer has chosen to publish. Registrants are not listed publicly, and internal notes, financial details and other registrants' answers are never shown on a public page.

6. How long it is kept

Each organization sets retention periods for its own records, according to its statutory obligations — for education and public-sector bodies these are often long.

Retention periods configured in the platform are recorded as policy and shown to administrators. They are applied by administrators rather than executed automatically: the platform does not currently delete records on a schedule of its own. Where a record must be removed, an administrator carries that out and the action is written to the audit log.

7. Your rights

Depending on where you live you may have the right to ask for a copy of your information, to have it corrected, to have it deleted, or to object to how it is used.

Requests are handled by the organization that collected the information, not by the platform. The platform gives that organization a record of each request, its status and its outcome, so the handling is auditable.

An attendee with a portal account can see and correct their own contact details, and can see their registrations, payments, certificates and messages, at any time.

8. Security

Access is controlled by named accounts, roles and server-side permission checks. Multi-factor authentication is available and can be required. Sessions can be ended everywhere for a user immediately.

Administrative changes are written to an append-only audit log that records who acted, what changed, and the before and after values.

Security incidents are recorded with their detection time, severity, what data was affected, containment and resolution, so that notification obligations can be assessed against a real record.

9. Cookies

The platform sets a session cookie when you sign in, which is necessary for the service to work and is removed when you sign out. It does not use advertising or cross-site tracking cookies.

10. Contact

To exercise a right or ask a question about your information, contact the organization that ran the event you registered for. Their contact details are on the event page and on your confirmation email.