NeighborlyEvents

Vendor packet

Everything a board, treasurer or management company needs to approve NeighborlyEvents as a vendor. Generated October 27, 2026.

Contents

- Terms of Service — version 1, effective September 9, 2026

The agreement between NeighborlyEvents and the communities, clubs and members who use it — accounts, data ownership, fees, refunds, grandfathering, termination.

- How the money works — version 1, effective September 9, 2026

The complete fee schedule and the mechanics behind it — where the fee comes from, how organizers are paid, refunds, chargebacks, fee changes, and tax reporting — written to match exactly what the platform does.

- Continuity memo — version 1, effective September 9, 2026

Where the service runs, how it is backed up, how your community's data comes out, and what happens if NeighborlyEvents winds down — one printable page.

- Data processing addendum — version 1, effective September 9, 2026

The standard processor addendum NeighborlyEvents signs with a community that asks for one — roles, what is processed, sub-processors, security, breach notification, return and deletion, audits, and California service-provider terms.

- Security overview — version 1, effective September 9, 2026

Authentication, what we collect and never collect, encryption, hosting and subprocessors, application security practices, compliance posture, and a completed vendor questionnaire.

Each document is also published on neighborlyevents.org, where the current version and its full change history live; the web version is authoritative. Documents on file that are not attached here are available on request from hello@neighborlyevents.org.

LEGAL

Terms of Service

Version 1 · Effective September 9, 2026 · https://www.neighborlyevents.dev/terms

1. Who we are and what these terms cover

NeighborlyEvents ("we", "us") is operated by Nicholas Schiavi, a sole proprietor doing business as NeighborlyEvents in California. These terms govern your use of the NeighborlyEvents website at neighborlyevents.org, the NeighborlyEvents mobile app, and the services they provide (together, the "Service").

The Service helps neighborhood associations, HOAs, clubs and their organizers run community life: publishing events, taking RSVPs and paid registrations, collecting club dues, coordinating volunteers, sending logistics email and push notifications, and keeping the records that go with all of that. Payments run through Stripe; the fee schedule and payment mechanics are published at How the money works, which forms part of these terms.

By using the Service you agree to these terms and to our Privacy Policy. If you use the Service on behalf of an association, club, management company or other organization, you confirm that you have authority to bind it, and "you" means that organization.

2. Accounts

There is no separate sign-up step. An account is created when you do something that needs one — RSVP, sign a petition, start a club, accept an organizer invitation — and you sign in with a one-time link or code sent to your email address. Keep control of that mailbox: anyone who can read it can sign in as you. Organizers may set a password in addition to the link.

You must give us accurate information, and you must be at least 18 years old to organize events or collect money through the Service. Organizers are responsible for the people they add to their team and for what those people do in the console.

3. Your community's data

You own your data. The content you and your members put into the Service — events, registrations, rosters, messages, photos, documents, poll and petition responses — belongs to the community that created it. You grant us the license needed to store, display, transmit and back it up in order to run the Service for you, and for no other purpose.

We do not sell it and we do not show ads. The Service contains no advertising and no third-party analytics or advertising trackers. The Privacy Policy lists the providers that process data on our instructions.

You can take it with you. The neighborhood owner (or a club's organizers) can build a whole-community archive — every event, registration, member, roster, dues record, poll, reservation and acceptance as CSV with a manifest — from the console, on every plan including the free one. The Continuity memo describes the archive and how long we keep data after an account or community closes.

Your members' privacy is your responsibility too. You must have a lawful basis for the member information you upload (for example, an association roster), and you must use the messaging tools for the community's own logistics — never for third-party marketing.

4. Acceptable use

Do not use the Service to break the law; to harass, threaten or discriminate against anyone; to send unsolicited bulk messages; to distribute malware; or to scrape or resell information about other people. Do not attempt to

access another community's data or to probe or disrupt the Service. Organizers must not misrepresent an event, its host, or how money collected will be used.

We may suspend or remove content or accounts that violate this section. We will tell you when we do, unless doing so would be unlawful or would put people at risk.

5. Fees and payments

Subscription plans are priced on the pricing page and billed by NeighborlyEvents through Stripe, monthly or yearly. Ticket sales and club dues carry a platform fee that is deducted from your payout; the attendee always pays the price you set. The complete fee schedule and the mechanics — payouts, refunds, chargebacks, taxes — are published at How the money works. Free events and free RSVPs never carry a fee.

To collect money through the Service you must complete Stripe Connect onboarding and remain in good standing with Stripe, whose Connected Account Agreement also applies to you. You are responsible for the taxes that apply to money you collect (see the tax section of How the money works).

6. Refunds and cancellation

Subscriptions. Cancel any time from your console. Your plan stays active until the end of the period you have paid for and does not renew. We do not refund the unused part of a billing period. Free trials that require a card are not charged if you cancel before the trial ends.

Event tickets and dues. Refunds to attendees and members are issued by the organizer, not by NeighborlyEvents; each organizer sets and publishes their own refund policy for their events. When an organizer issues a refund through the Service, the attendee receives the full amount they paid and the platform fee on that order is reversed as well. When an organizer cancels an event and refunds every registration at once, attendees still receive the full amount, but the platform fee on those orders is retained to cover payment-processing costs. Organizers can issue refunds through the Service from the moment of purchase until 30 days after the event ends; later refunds are handled by NeighborlyEvents support at the organizer's request. Nothing in the Service issues a refund automatically: if an organizer cancels an event, the organizer must refund each registration.

Chargebacks. If a cardholder disputes a charge with their bank, the process described under Chargebacks in How the money works applies.

7. Plan terms, grandfathering and changes to fees

Plan prices and entitlements are versioned. When we change a plan, existing subscribers stay on the version they subscribed to — price and features — for as long as that subscription remains active; only new subscriptions take the new version. This is how the plan catalog is built, not a promise layered on top of it.

We will give at least 60 days' written notice before a change to the published ticket or dues fee schedule takes effect, and no fee change is ever applied to money already collected. An agreement negotiated with a specific community may state different fee terms; where it does, the signed agreement governs.

8. Term and termination

You can stop using the Service at any time. Members can delete their account from the mobile app or by request; organizers can close their community by contacting us. We may suspend or terminate your access if you materially breach these terms and do not cure the breach after notice, or immediately where the breach is unlawful or endangers others.

If NeighborlyEvents itself winds down, we will give at least 90 days' notice and provide a full export of your community's data before the Service closes, as set out in the Continuity memo.

9. Availability and changes to the Service

We work to keep the Service available and improve it continuously. Our availability target is 99.9% in any month, measured at the application and excluding planned maintenance that we announce in advance and carry out outside peak hours. The target is a goal, not a guarantee: on self-serve plans we do not promise uninterrupted or error-free operation, and there is no service credit or other remedy for missing it. A negotiated agreement may include a service-level commitment with defined credits. We may add, change or retire features. If we retire a feature that a paid plan relies on, we will give reasonable notice.

10. Disclaimers and limitation of liability

The Service is provided "as is" and "as available". To the fullest extent permitted by law, we disclaim all warranties, express or implied, including merchantability, fitness for a particular purpose and non-infringement. We are not a party to the events organized on the Service and are not responsible for their conduct, safety or refunds beyond the mechanics described in these terms.

To the fullest extent permitted by law, our total liability to you for any claim arising out of the Service is limited to the amount you paid us in the twelve months before the claim arose, and we are not liable for indirect, incidental, special, consequential or punitive damages, or for lost profits, data or goodwill.

11. Indemnity

You will defend and indemnify us against claims arising from content you post, events you organize, money you collect, or your breach of these terms or of applicable law.

12. Governing law and disputes

These terms are governed by the laws of the State of California without regard to its conflict-of-laws rules. Any dispute arising out of these terms or the Service will be brought in the state or federal courts located in Orange County, California, and both sides consent to their jurisdiction.

13. Changes to these terms

We may update these terms. Material changes are announced to organizers by email at least 30 days before they take effect, and every change is recorded in the change history at the bottom of this page with its version number and date. Continuing to use the Service after a change takes effect means you accept it.

14. Contact

Questions about these terms: hello@neighborlyevents.org.

Change history

Version	Date	Change
1	Sep 9, 2026	First version, drafted from the platform's actual behavior. Sections 10–12 use standard SaaS terms; attorney review is scheduled before the first negotiated agreement.

FEES & PAYMENTS

How the money works

Version 1 · Effective September 9, 2026 · https://www.neighborlyevents.dev/pricing/fees

Fee schedule

Orders under $50 — flat fee per ticket, read at the order's average ticket price

Average ticket price in the order	Platform fee per ticket
$1.00 – $4.99	$0.75 (minimum)
$5.00 – $9.99	$1.00
$10.00 – $19.99	$1.25
$20.00 – $29.99	$1.50
$30.00 – $49.99	$2.00

Orders $50 and up — 5% of the order total + $0.30, capped at 12% of the order. Stripe's processing (2.9% + $0.30) is covered inside the platform fee. Free events never carry a fee. The same schedule applies on every plan.

Order	Platform fee
4 tickets at $10 ($40 order)	$5.00
2 tickets at $30 ($60 order)	$3.30
$120 of dues in one order	$6.30

Where the fee comes from

The platform fee is taken out of the organizer's payout. The attendee or member pays exactly the ticket price or dues amount you set — nothing is added at checkout. Stripe's card-processing cost (2.9% + $0.30 per charge) is paid by NeighborlyEvents out of the platform fee, never charged to you or your attendees on top.

The fee is calculated per order when the payment is captured, and the amount actually withheld is recorded on the registration or dues payment, so a later change to the schedule never touches money already collected.

One schedule on every plan

The schedule above applies on the free plan and on every paid plan alike; paid plans buy tools, not lower rates. The one exception is an agreement negotiated and signed with a specific community, which may state its own fee terms — where it does, the signed agreement governs.

Free events are free

Events with $0 tickets, RSVP-only events and volunteer sign-ups carry no fee at all, on every plan, with no limit on how many you run.

How you get paid

To collect money you connect a Stripe account to your community or club through Stripe Connect (an "Express" account, in Stripe's terms). Stripe handles identity verification and bank details; NeighborlyEvents never sees your bank account.

Tickets and dues. Each payment is processed as a single charge that is routed to your connected Stripe account at the moment it is captured, with only the platform fee kept back. The money lands in your Stripe balance immediately; it does not sit in a NeighborlyEvents account. Stripe then pays your balance out to your bank on its standard schedule for your country (in the United States, a rolling two-business-day schedule by default); you can change the payout schedule or request instant payouts from your Stripe dashboard.

Partner events. Events that split revenue among several payees — vendors, a host neighborhood, a club — work differently: attendee payments are collected on NeighborlyEvents' Stripe account and held there, then settled to each payee by transfer after the event ends. Settlement runs automatically once an event is over, and the organizer's payee list determines who receives what. Until settlement, those funds are held by NeighborlyEvents.

Refunds

Refunds are issued by the organizer from the registration or dues page in the console, or by NeighborlyEvents support at the organizer's request through the same ledger — NeighborlyEvents does not decide who gets a refund. When a refund is issued:

- the attendee receives the full amount that was actually charged (a discount applied at purchase is respected, and a price change after purchase is irrelevant);
- the platform fee on that order is reversed too, so the refund costs your payout nothing beyond returning the ticket price;
- Stripe does not return its processing cost on a refund, and NeighborlyEvents absorbs it;
- the attendee is emailed a confirmation and sees the money on their statement within five to ten business days.

When an organizer **cancels an event** and refunds everyone at once, attendees still receive the full price, but the platform fee on those orders is not returned to the organizer's payout: it covers the card-processing cost Stripe keeps on every refund, so a cancellation is not a cost to NeighborlyEvents and the organizer bears the fee on the cancelled tickets.

Refunds through the console are available from the moment of purchase until 30 days after the event ends. After that, contact support: an exception is issued through the same ledger and the attendee receives the same confirmation.

For partner events — events whose revenue is split among vendors and a host — refunds through the console close once the event has been settled to its payees. An exception issued by support after settlement comes out of NeighborlyEvents' balance and is not clawed back from those payees.

Chargebacks

A chargeback happens when a cardholder disputes a charge with their bank instead of asking you for a refund. Because ticket and dues charges settle through NeighborlyEvents' Stripe account, the dispute is filed against NeighborlyEvents, and NeighborlyEvents submits the response to the card network. Here is what happens:

1. Stripe notifies us, and the card network holds the disputed amount while it decides — typically several weeks.
2. We record the dispute, email the organizer with the reason and the evidence deadline, and hide the Refund button on that order while the dispute is open.
3. The organizer replies with what only they have — the registration confirmation, the check-in record, messages with the attendee, their published refund policy — or tells us to concede.
4. We file the response. When the card network decides, we email the organizer the outcome.

If the dispute is won, nothing changes. If it is lost, the card network returns the amount to the cardholder and

charges a dispute fee. Today NeighborlyEvents absorbs both the returned amount and the dispute fee, and the organizer's payout is not adjusted. If dispute volume ever makes that unsustainable, the policy changes only with the notice described under changes to the fee schedule below.

Changes to the fee schedule

We will give at least 60 days' written notice to every organizer with a connected Stripe account before a change to this schedule takes effect. A change never applies to money already collected. Subscription plan terms are versioned separately: existing subscribers keep the price and entitlements they signed up for.

Taxes and reporting

Who is the merchant. Ticket and dues charges are processed on NeighborlyEvents' Stripe account and routed to your Stripe Express account as described above.

Form 1099-K. Stripe's 1099 reporting is not enabled for NeighborlyEvents' connected accounts today, so no 1099-K is issued to your organization through the platform. Under current federal rules a 1099-K is required only when a payee receives more than $20,000 across more than 200 transactions in a calendar year; NeighborlyEvents will enable Stripe's reporting before any community approaches that threshold and will tell the community in advance. Some states set lower thresholds. Your organization remains responsible for its own tax filings, and every payment is available to you in the console and in the whole-community export.

Sales tax. NeighborlyEvents does not calculate, collect or remit sales tax on tickets or dues. Whether your event tickets or membership dues are taxable depends on your organization and your state; that determination, and any collection, is yours. Nothing on this page is tax advice.

Records. Every registration and dues payment keeps the amount charged, the platform fee withheld, refunds and dispute history. Organizers can export registrations per event as CSV, and the financial summary for an event shows gross, fees, refunds and net.

Subscription billing

Plans are billed by NeighborlyEvents through Stripe Checkout, monthly or yearly, to the card of whoever completes checkout. You can cancel any time; the plan stays active until the end of the paid period and does not renew, and unused time is not refunded. Card-up-front trials are not charged if cancelled before the trial ends. Subscription charges are separate from your connected Stripe account — they never touch your ticket or dues money.

Change history

Version	Date	Change
1	Sep 9, 2026	First version. Schedule renders from the fee engine; mechanics describe current behavior with owner decisions marked.

FOR BOARDS

Continuity memo

Version 1 · Effective September 9, 2026 · https://www.neighborlyevents.dev/continuity

Purpose

Boards ask the same three questions before approving software from a small vendor: where does it run, how do we get our data out, and what happens if the company goes away. This page answers them on one printable sheet. Every statement describes the service as it is today; changes are recorded in the history at the bottom.

Where the service runs

- **Application.** Amazon Web Services, US West (N. California) region: containers on ECS Fargate behind an application load balancer, with Cloudflare in front for DNS and TLS. Deployments are automated through AWS CodePipeline from a single source repository.
- **Database.** Supabase-managed PostgreSQL in the same region. Supabase is a managed provider; NeighborlyEvents does not operate its own database servers.
- **Files and email.** Uploaded photos, flyers and documents live in Amazon S3. Email is sent through Amazon SES.
- **Second deployment.** A second copy of the application runs on owner-operated hardware and serves neighborlyevents.dev against the same database. It is application-tier redundancy — if AWS compute is unavailable the service can be reached there — and it is **not** a database failover: both deployments depend on the single managed database.

Backups and recovery

- **Database.** Supabase takes a full physical backup of the production database every day (around midnight UTC) and retains seven days of them on our plan. A backup can be restored into a fresh project without touching production, which is how restores are tested. Point-in-time recovery is available as an add-on and is not enabled today.
- **Restore test.** Last run 9 September 2026: the previous night's backup was restored into a fresh project, the row counts for users, events and registrations and the latest registration timestamp matched production as of the backup time, and the test project was then deleted. Repeated at least every six months.
- **Uploaded files.** The S3 buckets keep prior versions of every object — 90 days for community uploads, one year for financial documents — so an accidental overwrite or deletion can be reversed.
- **Configuration and secrets** are held in encrypted configuration in the source repository, and the infrastructure is defined as code, so the environment can be recreated from the repository.

Your data is portable

- **Whole-community archive.** From the organizer console (Data export), the neighborhood owner can build a single download of everything the community holds: events with registrations, check-ins and question responses; members with the address on file; organizers; clubs with rosters, dues, polls and votes; facilities and reservations; volunteer roles, shifts and assignments; refunds and payment disputes; communications history (what was sent to whom and when); policy acceptances; and gallery photos by reference. Clubs have the same export for their own data. It is available on every plan, including the free plan, and every export is logged with who requested it.
- **Formats.** Plain CSV files plus a JSON manifest that names every file and column; no proprietary formats.

Photos and documents are referenced by URL, not copied. The archive is kept for seven days after it is built and then removed.

- **Per-surface exports.** Organizers can also export from individual screens as CSV: a single event's registrations, budgets, reimbursement ledgers, contest results and inventory. Members can request a copy or deletion of their own account data.

If NeighborlyEvents winds down

If the service is going to close, every organizer will receive at least 90 days' written notice, the whole-community archive will be provided before closure, and data will be deleted 90 days after the service closes unless you ask for earlier deletion.

Source code escrow

Source-code escrow is available on request, at cost, for negotiated agreements: an independent escrow agent holds the application code, deployment scripts and the credentials needed to run it, and releases them to the community if NeighborlyEvents ceases operations. Communities on self-serve plans rely on the export and wind-down commitments above.

Key-person risk, plainly

NeighborlyEvents is built and operated by a single founder. What limits the risk of that: the service runs entirely on managed, mainstream infrastructure (AWS, Supabase, Stripe, Cloudflare) with no bespoke servers to inherit; deployments and infrastructure are fully scripted from one repository; money never sits with NeighborlyEvents for ticket sales and dues — it settles to your own Stripe account (see How the money works); and your data is exportable in open formats.

Contact

Continuity questions, including escrow and data-return requests: hello@neighborlyevents.org.

Change history

Version	Date	Change
1	Sep 9, 2026	First version. Hosting described as-is; whole-community export shipped; backup cadence and restore test pending owner confirmation.

LEGAL

Data processing addendum

Version 1 · Effective September 9, 2026 · https://www.neighborlyevents.dev/dpa

1. Parties and purpose

This Data Processing Addendum ("DPA") forms part of the agreement between Nicholas Schiavi, a sole proprietor doing business as NeighborlyEvents in California ("NeighborlyEvents", the "Processor") and the community, association, club or organization that uses the Service (the "Customer", the "Controller") under the Terms of Service. It applies whenever NeighborlyEvents processes personal data on the Customer's behalf. Where this DPA and the Terms conflict on the processing of personal data, this DPA governs.

The Customer executes this DPA by countersigning a copy; NeighborlyEvents provides one on request to hello@neighborlyevents.org. Its text is published here so that a board can review it before asking.

2. Roles

The Customer decides which of its members' and attendees' data enters the Service and for what purpose, and is the controller of that data. NeighborlyEvents processes it only to provide the Service and is the processor. For the limited data NeighborlyEvents collects for its own purposes — account credentials, billing records, operational logs and security records — NeighborlyEvents is an independent controller under its Privacy Policy.

3. Description of the processing

- **Subject matter.** Running the Customer's community: events, registrations and check-ins, club rosters and dues, volunteer scheduling, facility reservations, polls, petitions, and the communications that go with them.
- **Duration.** For as long as the Customer's account is active, plus the retention period in section 9.
- **Nature and purpose.** Storage, display, transmission (email and push notifications the Customer sends), payment processing through Stripe, and generation of the reports and exports the Customer requests.
- **Categories of data subjects.** The Customer's residents, members, event attendees, volunteers, club organizers, vendors and sponsors.
- **Categories of personal data.** Name, email address, phone number, home address where the Customer verifies residency, registration and attendance records, answers to registration questions the Customer writes, payment amounts and Stripe identifiers (never card numbers), photos the Customer or its members upload, and device push tokens.
- **Special categories.** None are required by the Service. The Customer must not collect special-category data through custom registration questions without a lawful basis of its own.

4. Processing on instructions

NeighborlyEvents processes personal data only on the Customer's documented instructions, which are: the Terms, this DPA, and the Customer's use of the Service's features. NeighborlyEvents will inform the Customer if, in its opinion, an instruction infringes applicable data-protection law. NeighborlyEvents does not sell personal data, does not use it for advertising, and does not use it to train machine-learning models.

5. Confidentiality

Only people who need access to operate the Service have it, and they are bound by confidentiality obligations. Platform administrator access to a community's data is limited to support and is visible in the interface while it is in

use.

6. Security

NeighborlyEvents maintains the technical and organizational measures described on the Security overview, including encryption in transit, encryption at rest at the storage layer, passwordless authentication, scoped access by community, static security analysis and dependency scanning in the release pipeline, and rate limiting. NeighborlyEvents may update these measures provided the overall level of protection does not decrease.

7. Sub-processors

The Customer authorizes the sub-processors listed on the Security overview. NeighborlyEvents will publish a change to that list, with a note in the page's change history, at least 30 days before a new sub-processor handles personal data, and will email organizers about it. A Customer that objects on reasonable data-protection grounds may terminate the affected part of the Service and receive a pro-rated refund of any prepaid fees. NeighborlyEvents remains responsible for its sub-processors' performance.

8. Assistance to the Customer

Taking into account the nature of the processing, NeighborlyEvents will assist the Customer in responding to requests from data subjects (access, correction, deletion, portability) — members can delete their own account in the mobile app, and the whole-community export provides portability in open formats — and in meeting the Customer's obligations regarding security, breach notification and data-protection impact assessments, to the extent the Customer cannot do so through the Service itself.

9. Return and deletion

During the term, the Customer can export its data at any time (whole-community archive; per-event exports). When the Customer closes its account, or on a wind-down of the Service, NeighborlyEvents provides the archive and deletes the Customer's personal data 90 days later, unless earlier deletion is requested or retention is required by law (for example, payment records). Backups are overwritten on their own cycle.

10. Personal-data breach

NeighborlyEvents will notify the Customer without undue delay, and within 72 hours of confirming a personal-data breach affecting the Customer's data, with what happened, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Notifications go to the Customer's organizer notification address.

11. Audits

On request, and no more than once a year unless required by a supervisory authority or following a breach, NeighborlyEvents will make available the information reasonably necessary to demonstrate compliance with this DPA: the Security overview, the internal policy set, and answers to a reasonable written questionnaire. An on-site or third-party audit may be agreed in a negotiated contract, at the Customer's expense, with reasonable notice and scope.

12. Location of processing

Personal data is processed and stored in the United States, in the AWS US West (N. California) region and the sub-processors' US facilities. NeighborlyEvents does not transfer the Customer's personal data outside the United

States.

13. California residents

Where the California Consumer Privacy Act applies, NeighborlyEvents acts as a service provider to the Customer. It will not sell or share the personal data, will not retain, use or disclose it for any purpose other than performing the Service, will not combine it with personal data received from other sources except as permitted, and will notify the Customer if it can no longer meet these obligations. The Customer may take reasonable steps to stop and remediate unauthorized use.

14. Liability, term and governing law

The limitations of liability in the Terms apply to this DPA. This DPA lasts as long as NeighborlyEvents processes personal data for the Customer. It is governed by the law that governs the Terms.

Change history

Version	Date	Change
1	Sep 9, 2026	First version. Standard processor terms; attorney review is scheduled before the first negotiated agreement.

SECURITY & PRIVACY

Security overview

Version 1 · Effective September 9, 2026 · https://www.neighborlyevents.dev/security

Summary

NeighborlyEvents is a hosted web and mobile service for community events. Sign-in is passwordless, card numbers never touch our servers, we run no advertising or third-party analytics, and the data your community puts in belongs to your community. This page states what we do and do not do so that a security review can be completed from it; the vendor questionnaire at the bottom answers the standard questions row by row.

Authentication and sessions

- **Members sign in without passwords.** The website sends a single-use, expiring sign-in link; the mobile app sends a six-digit code that expires in ten minutes and is cancelled after five wrong attempts. No password is stored for these accounts.
- **Organizers may also set a password.** Passwords are stored as bcrypt hashes. Sign-in attempts are throttled per account and per source address.
- **Web sessions** are HTTP-only, secure cookies that expire after 30 days.
- **Mobile sessions** use a short-lived access token (30 minutes) with a rotating refresh token; both are stored only as SHA-256 digests, and a device can be signed out remotely.
- **Administrative access** to the platform is limited to NeighborlyEvents staff accounts with an admin flag; organizer consoles are scoped to the community or club the organizer belongs to.

What we collect, and what we don't

We collect what the community needs to run itself: name, email address, an optional phone number, and — where a community verifies residency — a home address. Organizers may add custom registration questions. We do **not** collect card numbers (Stripe does), we do not sell or share personal data for advertising, and neither the website nor the app contains third-party analytics or advertising trackers. The Privacy Policy has the complete statement.

Encryption

- **In transit.** TLS on every connection, with HTTP Strict Transport Security; plain HTTP is redirected.
- **At rest.** The database (Supabase) and file storage (Amazon S3) encrypt data at rest at the storage layer; the database's daily backups are encrypted the same way. Third-party API keys that communities supply are additionally encrypted at the application layer. Personal fields such as email addresses and home addresses are stored in the encrypted database but are not additionally encrypted at the application layer, because the application searches on them.

Payments

Payments are processed by Stripe. Card details are entered into Stripe's own components and go directly to Stripe; NeighborlyEvents stores only Stripe's identifiers and the amounts. Organizers receive money through their own Stripe Connect account, and NeighborlyEvents never holds bank account details. See How the money works.

Hosting and subprocessors

The service runs on Amazon Web Services (US West) with a Supabase-managed PostgreSQL database in the same region, behind Cloudflare. The providers below process data on our instructions to deliver their function. We will update this list, with a note in the change history, before adding a provider that handles personal data.

Provider	What it does for us	Data it processes	Location
Stripe	Payment processing, Connect payouts to organizers, subscription billing	Payer name and email, payment amounts and identifiers. Card details are entered directly with Stripe and never reach our servers.	United States
Amazon Web Services (ECS, S3, SES, CloudWatch)	Application hosting, file storage, transactional email, logs	All application traffic; uploaded photos, flyers and documents; email addresses and message content; application logs	United States (us-west-1)
Supabase	Managed PostgreSQL database	All application data	United States (us-west-1)
Cloudflare	DNS, TLS termination, edge caching of public pages	All web traffic in transit	Global edge network; United States origin
Anthropic	The organizer AI assistant	The event, registration and community data the assistant reads to answer an organizer's request, and the request itself	United States
Google (Maps Platform, Firebase Cloud Messaging, Google Wallet)	Address autocomplete and geocoding; Android push delivery; Google Wallet event passes	Addresses typed for residency verification; device push tokens and notification text; attendee name and confirmation code on a saved pass	United States
Apple (Apple Push Notification service, Apple Wallet)	iOS push delivery; Apple Wallet event passes (signed on our servers)	Device push tokens and notification text	United States
Slack	Internal operations alerts to the NeighborlyEvents team	Alert summaries, which can include a member's name and email (for example, a new support request or a payment dispute)	United States

Access control and auditing

Every organizer console is scoped to one community or club; an organizer of one community cannot read another's data. Registration state changes are logged with who made them and when. Platform administrators can act as an organizer for support, and that impersonation is visible in the interface while it is active.

Application security practices

- Static security analysis (Brakeman) runs in continuous integration and again as a gate in the deploy script; a finding blocks the deploy.
- The application runs on supported, current versions of Ruby and Rails, and dependencies are kept current.
- Security headers are set on every response (HSTS, `X-Content-Type-Options`, `Referrer-Policy`, `Permissions-Policy`). A Content Security Policy is deployed in report-only mode while its allowlist is tightened toward enforcement.
- Sign-in, sign-in-link requests, verification codes and anonymous form submissions are rate-limited.
- Uploaded financial documents are stored in a private bucket and served only through authenticated,

streamed downloads — never by public URL.

Policies and runbooks

The internal policy set is written down and versioned with the application's source, reviewed at least annually, and available to customers on request:

- Information security policy — scope, ownership, and how the set is reviewed and changed.
- Access control — who can reach production systems and customer data, how accounts are protected, and how access is removed.
- Change management — every change ships through version control and a pipeline that runs static security analysis, dependency audits, linting and the test suite before deploy.
- Secrets management — encrypted credentials, who holds the keys, and rotation.
- Vulnerability management — scanning, triage timelines by severity, and coordinated disclosure.
- Incident response — detection, severity, containment, customer notification within 72 hours, and the post-incident report.
- Backup and recovery — cadence, retention, the restore procedure, and how often it is tested.
- Data retention and deletion — what is kept for how long, and how deletion requests are honored.
- Vendor and sub-processor management — selection criteria, the published list, and advance notice of changes.
- Acceptable use and device security — the standards the operator's own equipment and accounts meet.
- Business continuity — the continuity memo's commitments and the runbook behind them.

Backups and continuity

See the Continuity memo for hosting, backup cadence, the most recent restore test, data export and wind-down commitments.

Incident response

We will notify affected customers without undue delay and within 72 hours of confirming a personal-data breach, with what happened, what data was involved, and what we are doing about it. Operational alerts — errors, delivery failures, payment disputes, unusual database load — page the operator in real time.

Compliance posture

- **SOC 2.** NeighborlyEvents is not SOC 2 certified. The controls described on this page are documented and in operation; a formal audit is planned when customer volume warrants it.
- **Privacy law.** Members can request a copy or deletion of their personal data; account deletion is self-serve in the mobile app and by request on the web.
- **Data processing addendum.** Available. The standard template is published at /dpa; we execute it with the community on request.
- **Insurance.** NeighborlyEvents does not currently carry technology errors-and-omissions or cyber liability insurance and cannot provide a certificate of insurance. Coverage will be bound before or at the first paid community agreement; ask and we will confirm the timeline.

Reporting a vulnerability

Please report security issues to security@neighborlyevents.org (also published at `/.well-known/security.txt`). We acknowledge reports within two business days and ask for a reasonable window to fix before public disclosure.

Vendor security questionnaire

The standard questions, answered for NeighborlyEvents as it is today. "Partial" and "No" answers are stated as such — an honest gap is more useful to a reviewer than a soft yes.

Organization and policies

Question	Answer	Status
Is there a designated owner accountable for security?	Yes. The founder-operator is accountable for security end to end; there is no separate security team.	Partial
Are security policies documented?	Yes. A written policy set (information security, access control, change management, secrets, vulnerability management, incident response, backup and recovery, data retention, vendor management, device security, business continuity) is versioned with the application's source, reviewed at least annually, and available to customers on request; the security overview and continuity memo are its customer-facing summary.	Yes
Do employees receive security awareness training?	Not applicable — NeighborlyEvents has no employees; a single operator runs the service.	N/A
Are background checks performed on staff with data access?	Not applicable — single operator, no staff.	N/A

Access control

Question	Answer	Status
How do users authenticate?	Passwordless single-use email links on the web and expiring six-digit codes in the app (five attempts, ten minutes). Organizers may additionally set a password, stored as a bcrypt hash. Sign-in attempts are throttled per account and per source address.	Yes
Is multi-factor authentication supported?	Possession of the email mailbox is the factor for passwordless sign-in. There is no second factor on the optional password path.	Partial
Is access role-based and scoped?	Yes — member, organizer, club organizer, volunteer and platform admin roles; every organizer console is scoped to one community or club.	Yes
Can vendor staff access customer data?	Platform admin accounts can, for support. An admin acting as an organizer is shown as such in the interface while it is active.	Yes
How are sessions managed?	Web sessions are HTTP-only, secure cookies expiring after 30 days. Mobile sessions use 30-minute access tokens with rotating refresh tokens, stored only as SHA-256 digests, revocable per device.	Yes
Are access rights reviewed periodically?	Organizer team membership is managed by each community's owner. There is no scheduled platform-wide access review.	Partial

Data protection

Question	Answer	Status
Is data encrypted in transit?	Yes — TLS on every connection with HTTP Strict Transport Security; plain HTTP is redirected.	Yes
Is data encrypted at rest?	Yes at the storage layer — the managed database and S3 buckets encrypt at rest. Third-party API keys supplied by communities are additionally encrypted at the application layer; personal fields such as email and home address are not, because the application searches on them.	Yes
How are encryption keys and secrets managed?	Storage keys are provider-managed. Application secrets live in encrypted configuration in the source repository; the master key is held by the operator and the deploy pipeline only.	Yes
How is customer data segregated?	Logically — one database, with every query scoped by community or club through the application's authorization layer. There are no per-tenant databases.	Yes
Is payment card data stored?	Never. Card details are entered into Stripe's components and go directly to Stripe; we store Stripe identifiers and amounts only.	Yes
What is the data retention policy?	Data is kept while the account or community is active and deleted on request. After a community closes its account, or after a service wind-down, its data is deleted 90 days later unless earlier deletion is requested.	Yes
How is data securely deleted?	Account deletion anonymizes personal fields, removes the address, and revokes every device token. Deleted files are removed from storage; prior object versions expire under the bucket lifecycle (90 days for community uploads, one year for financial documents).	Yes
Are backups encrypted?	Yes. The managed database provider takes a full physical backup daily, encrypted at rest like the primary; uploaded files are versioned in S3 with server-side encryption.	Yes

Application security

Question	Answer	Status
Is there a secure development lifecycle?	Every change goes through version control, an automated test suite, and static security analysis (Brakeman) in continuous integration and again as a gate in the deploy script.	Yes
Are vulnerability scans performed?	Static analysis (Brakeman) on every build and again as a deploy gate; Dependabot opens daily pull requests for Ruby gem and GitHub Actions advisories; JavaScript dependency pins are audited in CI on every build.	Yes
Has an independent penetration test been performed?	No third-party penetration test has been performed.	No
Is there a vulnerability disclosure process?	Yes — coordinated disclosure via /.well-known/security.txt with a two-business-day acknowledgement. There is no paid bounty.	Partial
How are injection and cross-site attacks prevented?	Framework-level parameterized queries, strong parameter filtering, CSRF tokens on every state-changing form, and output escaping by default.	Yes
Are security headers and a Content Security Policy in place?	HSTS, X-Content-Type-Options, Referrer-Policy and Permissions-Policy are enforced on every response. A Content Security Policy is deployed in report-only mode while its allowlist is tightened toward enforcement.	Partial

Question	Answer	Status
Is rate limiting in place?	Sign-in, sign-in-link requests, verification codes and anonymous form submissions are throttled in the application. There are no custom edge WAF rules beyond Cloudflare's defaults.	Partial
Is there logging and monitoring?	Application logs are centralized; errors, email delivery failures, payment disputes and unusual database load alert the operator in real time.	Yes
Are secrets kept out of source code?	Yes — encrypted credentials only; the pipeline never prints them.	Yes

Infrastructure and availability

Question	Answer	Status
Where is the service hosted?	Amazon Web Services, US West (N. California) — containers on ECS Fargate behind an application load balancer — with a Supabase-managed PostgreSQL database in the same region, S3 for files, SES for email, and Cloudflare in front.	Yes
Is the infrastructure redundant?	Multiple application containers behind a load balancer, plus a second application deployment on owner-operated hardware serving the same database. The database itself is a single managed instance; there is no multi-region database failover.	Partial
How often is data backed up and for how long is it kept?	The database is backed up in full daily (around midnight UTC) and seven days of backups are retained; a backup can be restored into a fresh project without touching production. Uploaded files keep prior versions for 90 days (community uploads) and one year (financial documents). Point-in-time recovery is not enabled today.	Yes
Are restores tested?	Yes. Most recently on 9 September 2026 the daily backup was restored into a fresh project and verified against production (row counts and latest registration timestamp) before the test project was deleted. Repeated at least every six months.	Yes
Is there an uptime commitment?	No contractual SLA on self-serve plans; the published target is 99.9% monthly availability, a goal rather than a guarantee. Releases are rolling deployments behind a load balancer across two application tasks in separate availability zones, so deploys take no downtime; the main sources of unavailability are planned database maintenance, done outside peak hours with notice, and provider incidents (AWS publishes 99.99% monthly SLAs for the ECS and load-balancer services the application runs on). Negotiated agreements may include an SLA with service credits.	Partial
How are changes managed?	All changes ship through version control and an automated pipeline; database migrations run as part of each deploy; a failed static-analysis or test step blocks the deploy.	Yes
How is the network secured?	Application containers run in private subnets; only the load balancer is reachable from the internet; storage buckets are private except the public assets bucket that serves uploaded event images.	Yes

Incident response and continuity

Question	Answer	Status
Is there an incident response plan?	Operational alerts page the operator in real time. Affected customers are notified without undue delay and within 72 hours of a confirmed personal-data breach, with what happened, what data was involved, and what is being done about it.	Yes
What is the breach notification timeline?	Without undue delay and within 72 hours of confirming a personal-data breach.	Yes
Is there a business continuity plan?	Yes — the continuity memo covers infrastructure-as-code recreation, data export, and the wind-down notice commitment.	Yes
What is the key-person risk?	Real, and stated plainly — a single operator. Mitigations are in the continuity memo — managed infrastructure, scripted deployments, money settling to the customer's own Stripe account, exportable data.	Partial

Privacy and compliance

Question	Answer	Status
Is there a published privacy policy?	Yes, at /privacy, with an app-store-grade disclosure of what is collected.	Yes
Are data-subject access and deletion supported?	Yes — self-serve account deletion in the mobile app, deletion and data copies on request on the web.	Yes
Is personal data sold or used for advertising?	No. No advertising, no data sale, no third-party analytics or advertising trackers.	Yes
Is a subprocessor list published?	Yes, above on this page; changes are recorded in the document's change history.	Yes
Which certifications are held (SOC 2, ISO 27001)?	None. NeighborlyEvents is not SOC 2 or ISO 27001 certified; the controls on this page are documented and in operation, and a formal audit is planned when customer volume warrants it.	No
Is a data processing addendum available?	Yes. The standard data processing addendum is published at /dpa and executed with the community on request.	Yes
What insurance coverage is carried?	None today. Technology E&O and cyber liability coverage will be bound before or at the first paid community agreement; a certificate of insurance is not available until then.	No
Where is data stored geographically?	United States only.	Yes

Change history

Version	Date	Change
1	Sep 9, 2026	First version, drafted from the codebase; SOC 2 posture, insurance, DPA and incident commitments pending owner confirmation.