Flok — PCI DSS Shared Responsibility Matrix

PCI DSS v4.0.1 · Version 1.0 · Effective 2026-08-19

• Owner ± Contributes / provides evidence - Not applicable

Requirement	Prov.	Flok	Tenant	Notes
1. Network security controls	•	±	-	Largely inherited from Vercel (static hosting); Flok owns database network configuration.
2. Secure configuration	•	±	±	Mostly inherited from Vercel; Flok owns database hardening; tenants configure their own Stripe/Payrexx account settings.
3. Protect stored account data	•	-	-	Flok never stores cardholder data. Neither does the tenant — card data lives only with the payment provider.
4. Protect cardholder data in transit	•	±	-	Flok enforces TLS on all pages. The redirect to the provider's checkout page happens over TLS; the card entry itself happens entirely on the provider's origin.
5. Anti-malware	•	•	-	Applies to Flok's own build and hosting infrastructure.
6. Secure development	•	•	-	Flok owns its SDLC, dependency updates, and patch management.
6.4.3 Payment page script management	•	±	-	Not required for SAQ A, but Flok restricts which scripts can run on pages in the checkout path via a Content-Security-Policy script-src allowlist. Automated script-change detection is not yet built.
7. Restrict access by business need to know	•	•	±	Flok's role-based access control scopes every user to their own tenant; tenants manage which of their own users hold which role.
8. Identify and authenticate users	•	•	•	Flok provides passwordless one-time-code login for the member portal and WebAuthn passkey login for staff/admin accounts; each tenant is responsible for who they grant access to.
9. Restrict physical access	•	-	-	Fully inherited from Vercel (Frankfurt) and Supabase (Zürich) — Flok operates no physical infrastructure of its own.
10. Log and monitor all access	•	±	-	Flok logs administrative changes across the platform via an audit log. Append-only logging of every read of a stored payment credential is part of ongoing hardening work.
11. Test security of systems and networks	•	±	-	Automated dependency and secret scanning run in CI today. A recurring third-party penetration test is not yet in place.
11.6.1 Detect unauthorised page changes	±	±	-	A restrictive Content-Security-Policy limits what can run on checkout pages. Dedicated tamper-detection tooling is not yet built.
12.8 Manage third-party service providers	•	•	•	Flok maintains this matrix and its subprocessor list; tenants should review both, and their own provider relationship, at least annually.
12.10 Incident response	•	±	±	Flok will notify affected tenants of a security incident that concerns their data; tenants remain responsible for notifying their own acquirer/provider per that provider's terms.
SAQ A eligibility — payment elements from the provider only	•	•	±	Flok-controlled: ticket checkout is a full-page redirect to Stripe or Payrexx. No card field is ever rendered by Flok. Tenants must not take card numbers by phone, email, or chat and enter them anywhere.
SAQ A eligibility — site not susceptible to script-based attacks	±	•	-	Flok-controlled: the redirect model means this criterion is not reached, since no Flok page renders a payment form.

Requirement	Prov.	Flok	Tenant	Notes
Annual SAQ A submission	-	-	•	Only the tenant, as the merchant, can complete and sign this. Flok records that a tenant has self-declared completion but does not verify or submit on the tenant's behalf.
Contract with acquirer / payment provider	-	-	•	Each tenant holds its own direct account and contract with Stripe or Payrexx. Flok is never merchant of record.