Before real users pay: a 20-minute self-check

For apps built with Lovable or Bolt on Supabase and Stripe. You can do every check yourself, in your own dashboards. Nobody needs access. If an answer is "no" or "not sure", that is where to look first.

Database (Supabase)

01 **Security Advisor shows no errors.** In Supabase, open Advisors. Watch for "RLS disabled", "security definer view", "function search_path mutable".

02 **Every table in `public` has RLS on** and a policy that names who may read and who may write.

03 **No `USING (true)` on tables with personal data,** unless you really want them public.

04 **Insert and update policies have a `WITH CHECK`** tied to `auth.uid()`, so nobody writes rows for someone else.

05 **Roles do not come from data the user can edit,** such as their own profile row or `user_metadata`.

06 **Private storage buckets are not public,** and their policies follow the same rules as the tables.

Keys and functions

07 **Only the anon key is in the browser.** Search the built site and repo for `service_role`, `sk_live`, `sk_test`, `whsec_`. Found one? Rotate it: deleting the line is not enough.

08 **Each edge function knows who may call it.** With JWT checks off, it checks the user or a secret in its own code. The public anon key is itself a valid JWT.

09 **Email, SMS and AI functions cannot be called** by anyone, for anyone, without limits.

Payments (Stripe)

10 **The amount is calculated on the server** from your prices or the order, never taken from the browser.

11 **The webhook verifies the Stripe signature** before it reads the event.

12 **An order is marked paid only when** payment ID, amount and currency match that order, and the order belongs to that user.

13 **The webhook is idempotent:** the same event twice does not create two orders or two credits.

14 **Live and test keys are not mixed,** and test mode is off in production.

15 **Refunds and admin actions are checked on the server** for an admin role.

Operations and GDPR

16 **Backups exist,** and you have restored one at least once.

17 **Sign-ins and payment events are in one place,** and someone gets an alert when something fails.

18 **You have a privacy policy and can delete a user's data on request,** and you know which region your data lives in.

19 **If your app talks to people through AI, it says so** (EU AI Act Art. 50, from 2 August 2026).

20 **Your custom domain has HTTPS** and basic security headers.

Most of these take minutes to check and hours to fix. Want a second pair of eyes?
Read-only audit, 390 €, written report. Write to info@lifkuru.com

lifkuru OÜ · Reg. code 17604498
Tallinn, Estonia · info@lifkuru.com