

INDICATIVE REVIEW

Hatchpad Ltd.
(fictional)

AI spend, privacy, and control

Contents

Opinion	02
Expenditure	03
Findings	04
Work programme	05
Audit sample	06

Prepared for the directors

September 2026

Delivery

5 October 2026 · v1.2

Not a statutory audit, a penetration test, or a legal opinion.

Indicative report. Savings ranges are estimated from the data you sent; this is not legal or tax advice.

ILLUSTRATIVE SAMPLE · FICTIONAL DATA

Opinion

Indicative opinion on AI spend and customer-data control for this period.

Control

Low

Cross-account data access, AI chat without notice, and duplicate unused tools.

Scope. B2B webapp launched in weeks: dashboard, customer login, AI chat. They asked for AI spend review; the report also covers privacy and database risk before a fine or claim.

Figures for the period

	MONTHLY	ANNUAL (×12)
Spend in the period	€412	€4,944
Indicative savings	€71–€125/mo	€852–€1,500 (estimate)

Matters this week

- 1

Close cross-account access between customers
Legal priority: until this is fixed and tested, do not onboard more customers with sensitive data.

€0
- 2

Bring the AI chat into compliance (notice + vendor contract)
Make clear what is sent to OpenAI and update the privacy page before promoting the assistant further.

€0
- 3

Cancel GitHub Copilot (duplicate of Cursor)
Direct license savings; the team already works only in Cursor.

€28

Expenditure

Tools in this period. The invoice is a closed snapshot, not the token pace inside the month.

TOOL	TYPE	COST/MO	USAGE	VERDICT
OpenAI (web assistant)	Usage (tokens/API)	€124	Product chat; the review showed it receives the user's email and name	WATCH
Supabase (database)	Other	€48	Customer data and files; incomplete access rules (see findings)	WATCH
Cursor	Seats	€40	Daily product development	KEEP
Vercel (hosting)	Other	€34	Production website	KEEP
Anthropic (internal tests)	Usage (tokens/API)	€72	Occasional experiments; overlaps with Cursor	REDUCE
GitHub Copilot	Seats	€28	No use in 30 days	CANCEL
Make (automations)	Agents	€66	Onboarding and emails; runs overnight with no need	REDUCE
Total		€412		

Composition

Monthly spend split by tool type

Seats	€68 · 17%	Usage (tokens/API)	€196 · 48%
Agents	€66 · 16%	Other	€82 · 20%

Reading this snapshot

Without a token series (usage by day) we do not project how the month will close or which model to cut. What this invoice does yield is the seat match and a cap for the next one.

People on the export against seats on the invoice. Cursor: 2 on the invoice, 2 on the export. GitHub Copilot: 2 on the invoice, 0 on the export. Gap: 2.

Cap to set in the panel. OpenAI (web assistant) €124 · Anthropic (internal tests) €72 · Make (automations) €66. Sum of usage caps €262. The cap is this invoice's amount. If the next one exceeds it, that is a spike against this snapshot, not a forecast.

Findings

Ordered by exposure, then by monthly savings.

F - 01

Indicative exposure €15,000–
€80,000

Customers can see data that is not theirs

Observation

The production site does not separate accounts properly: a user logs in and sees another company's projects and names. This is a serious database failure, common when the app was assembled quickly from templates.

Implication

This is not a monthly saving: it is exposure to claims, stopping sales, notifying the Spanish Data Protection Agency if a leak is confirmed, and GDPR fines (for SMEs, reputational and legal damage usually far exceeds savings on AI licenses).

Recommendation

Fix database access rules, test with two trial accounts, and keep a screenshot showing it no longer happens.

F - 02

Indicative exposure €5,000–
€35,000

The AI chat processes personal data without saying so

Observation

The assistant sends email and name to OpenAI. The privacy page does not explain this, and there is no data processing agreement (DPA) with the vendor.

Implication

Risk of GDPR non-compliance (information and legal basis) and of a customer or employee filing a complaint before you fix it.

Recommendation

Clear text in the chat and in the privacy policy, minimize what is sent to the model, and put a DPA in place with OpenAI.

F - 03

Indicative exposure €3,000–
€25,000

Personal data kept in logs for too long

Observation

Server logs store emails and paths with customer names and have no defined deletion period.

Implication

If those logs leak or an auditor requests them, it is the same problem as an app breach; fines for excessive retention.

Recommendation

Stop logging sensitive data, set a retention period (for example 30 days), and record it in the record of processing activities.

F - 04

Savings €28/mo

Copilot paid for with nobody using it

Observation

The invoice bills 2 seats. The member export has 0 people. The team develops in Cursor.

Cost

€28 a month wasted.

Recommendation

Cancel on GitHub and review licenses every quarter.

Work programme

This week

- 1 Fix cross-customer data access and document the test.
- 2 Update privacy and the AI chat notice; start a DPA with OpenAI.
- 3 Cancel Copilot and shorten log retention.

This month

- 1 Bring the record of processing activities (GDPR) up to date with what the app actually does.
- 2 Review database backups (encryption and who can export).
- 3 Set caps at €124 on OpenAI, €72 on Anthropic, and €66 on Make. If the next invoice exceeds them, that is a spike: this snapshot is not enough to project the month close.

Next conversation

A 45-minute review to prioritize legal risk and AI spend for teams that launched the app very quickly.

Book a review, €590

Notes

- 1 Legal exposure figures are indicative orders of magnitude, not fine predictions.
- 2 This document is not legal advice; for penalties and notifications, consult a lawyer and your DPO.
- 3 Illustrative example with fictional Hatchpad.
- 4 Without a token series (usage by day) we do not project the month close or which model to cut. The cap is this invoice's amount.

Appendix A · Audit sample

A security and privacy review written for leadership and finance. In a real engagement we cross this with your AI invoices.

Scope

Security and privacy review — Hatchpad (production web app)

App published on the internet (customer login, cloud database). Review without access to your admin panel: tests as a third party would run them.

01 · CRITICAL

One customer can see another customer's data

A normal account can open files and company names that are not theirs. Typical when the database was left open during rapid development.

What to do: Separate data by customer in the database and test it with two trial accounts before selling further.

If you do not act: Claims from affected people, service shutdown, and a GDPR fine: high exposure for an SME (tens of thousands of euros in the worst case).

02 · HIGH

Personal data in logs with no deletion period

Emails and names stay in server logs longer than needed; there is no clear policy for how long they are kept.

What to do: Stop logging sensitive data, shorten retention, and document it in the record of processing activities (GDPR).

If you do not act: Breach of minimization and storage limitation (GDPR art. 5); a fine and a duty to notify the authority if there is a leak.

03 · HIGH

AI chat with no notice to the user

The product assistant sends the user's name and email to OpenAI without explaining it in the privacy policy or a data processing agreement with the vendor.

What to do: Update the privacy policy, tell users in the chat, and sign a DPA with the AI vendor.

If you do not act: Processing without a clear legal basis; complaints and a marketing freeze until it is regularized.

04 · MEDIUM

Unencrypted database backups

Automatic backups exist, but encryption is not documented and it is unclear who can download them.

What to do: Turn on encryption with the database provider and limit who can export data.

If you do not act: If a backup leaks, it is as serious as a breach of the live app.

Illustrative sample for the auditamia report. Hatchpad is fictional.