

Security & sub-processors

Where your data is processed, who processes it, and how long we keep it.

This page is written to answer a security review without a call. Everything here applies to every account on every plan, including the free one. If your team has a question this page does not answer, email support@veriphone.io and we will answer it directly — and add it here.

What we hold, and for how long

Veriphone's job is to take a phone number, validate it, and hand back what we know about it. We are deliberately built so that most of that leaves nothing behind.

- **API requests are not stored.** A phone number sent to `/verify` is processed in memory and returned in the response. It is not written to any database, not written to our application logs, and not present in our usage analytics.
- **Request logs keep URLs for 30 days.** If you call the API with a GET request, the phone number is part of the request URL, and infrastructure request logs retain that URL for 30 days before deleting it automatically. Sending parameters in a POST body avoids this entirely.
- **Uploaded CSV files are kept until you delete them.** You can delete any file and its results from the dashboard at any time; deletion removes the stored objects, not just the listing. We may delete files and their results more than 90 days after upload, so download your results within that window.
- **Closing your account deletes your files.** Account deletion removes your uploaded files and result files in the same operation.
- **Usage analytics are aggregate only** — request counts, credit consumption, country distribution. No phone numbers.

The full contractual version of all of this is in our Data Processing Agreement, Annex I.

Where it is processed

All customer data is stored in the **European Economic Area** — our services run in Belgium, and uploaded files, job metadata and operational logs are held in EU multi-region storage spanning Belgium and the Netherlands. Standard validation never leaves our own systems.

Current Carrier Lookup is the one exception, and it is deliberate. Answering "which carrier serves this number today" cannot be done from a static dataset. To answer it we send **the queried number, and nothing else**, to a third-party number portability data provider located in the **United Kingdom** — no account identifier, no file, no other column from your upload. That provider holds and controls its own reference dataset and answers the query from it, so it acts as an **independent controller of that dataset rather than as our sub-processor**; it is engaged under a written contract with confidentiality and data protection terms. See clause 5.5 of the DPA.

Veriphone is operated by Epic Grove Ltd, a company registered in England and Wales (company number 17285617). Transfer mechanisms are set out in clause 10 of the DPA.

Sub-processors

There is one, and it covers the whole service — both Phone Validation and Current Carrier Lookup.

- **Google Cloud EMEA Limited** (Ireland) — the infrastructure Veriphone runs on: compute, storage, database and logging, in the EEA locations above.

The list is short because sub-processors are *legal entities*, not products. Google Cloud's breadth means our entire infrastructure sits behind that single company, so one name covers what would otherwise read as four or five vendors.

The services we use to run our own business — payment processing, our own email, our CRM — never receive a number you submit for verification, an uploaded file, or a result. They handle our relationship with you as a customer, which makes us the controller for that data rather than your processor, so they are covered by our Privacy Policy rather than by this page.

We give **30 days' notice** before adding or replacing any sub-processor. To be notified, email privacy@veriphone.io and ask to be added to the list.

Security measures

- **Encryption in transit** — TLS on every endpoint.
- **Encryption at rest** — AES-256 with Google-managed keys, across storage, database and logs.
- **Access control** — API access requires an account-specific key. Administrative access to production is restricted through our cloud provider's identity and access management to the people who need it.
- **Segregation** — uploaded files are stored under a per-account path and served only through authenticated, account-scoped endpoints.
- **Minimisation** — the single-lookup path writes nothing to disk.
- **Resilience** — Google Cloud managed infrastructure, with multi-region EU storage.
- **Vulnerability management** — dependencies are updated as part of the regular release process.

What we don't have

We would rather you learn this here than three weeks into a procurement process:

- **No SOC 2, ISO 27001 or equivalent certification.** We do not hold one today and we will not claim otherwise. Clause 9.3 of the DPA lets us satisfy an audit request with our security documentation and a completed questionnaire instead.
- **No customer-managed encryption keys**, and no choice of storage region beyond the EU locations above.
- **No single sign-on** on the dashboard.

If any of these is a hard requirement, tell us before you spend time on an evaluation.

Reporting a vulnerability

Email security@veriphone.io with enough detail to reproduce the issue. We will acknowledge within two business days. Please give us a reasonable opportunity to fix an issue before disclosing it publicly. We do not currently run a paid bug bounty.

Documents

- Data Processing Agreement — pre-signed, no signature required from us (PDF)
- This page as a PDF — for attaching to a security questionnaire
- Terms of Service
- Privacy Policy · GDPR compliance
- Enterprise Agreement — if your policy requires a signed MSA, an SLA, or a negotiated DPA