Security questionnaire

Ready answers to the questions a large company's security office asks before buying. They say what Russet does today; where something is missing, it says «missing» and what it takes. Updated on 19 November 2026.

Where is our data and who handles it?

The service runs in Germany (netcup GmbH, ISO 27001 and 27701); the backups are in the Netherlands (Backblaze, SOC 2 Type 2), encrypted before leaving the server. Your data that go to the AI reach only OpenAI (United States and Ireland), without your customers' names; the Russet team's internal work, without your data, also Anthropic (United States). Russet's mailbox is with Microsoft; the service emails leave from Scaleway (France); the bank link, if you switch it on, goes through Enable Banking (Finland). Each company has its own databases, in separate folders. The full list of suppliers, with country and role, is on /security and the privacy page.

How is data encrypted, in transit and at rest?

In transit always HTTPS with HSTS; session cookies are bound to Russet's domain only. At rest: secrets (connected systems' credentials, tokens, keys) and backups are encrypted with AES-256-GCM, with keys that live only on the server in files readable by the service alone; the server's disk is the certified provider's. The companies' databases on the server are not encrypted at file level: they are protected by the access to the server (the service alone) and the separation per company.

Backups and restore: how often, where, tested?

A copy of each company every hour, encrypted, sent to a second European data centre and read back byte by byte at once and over the following days. Each copy lives 14 days, then Russet itself deletes it (the last one of an active company stays). A restore goes into a separate folder, never over the data in use, and is tested by the automated tests (restore-all, restore-atomicity) and the written scenarios. Missing: the full scheduled drill on the real server, to be done every six months.

How is people's access controlled?

Four roles (administrator, credit manager, credit clerk, read only) decided by whoever administers, with the «who sees and who does what» matrix written in one place and applied by every page. Password and a mandatory second step for everyone, enforced by Russet's sign-in pages (passkey, authenticator app or e-mail code); owner and administrators must have a passkey or the app; on a device the person chooses to remember the second step comes back every 30 days; before sensitive operations Russet asks again who you are. Sign-in with the company account (Microsoft Entra ID or Google), on request and to be switched on (off on the server today): the people of the group you choose enter, with the group's role; whoever leaves the group no longer enters (read at every entry and every day, or pushed by your system via SCIM 2.0). Removing a person ends their sessions at once.

Is there a log of who did what?

Yes: every action in the company's space (a person, Russet on its own, an agent, the daily care) is a line with who or what, on which data, by which rule, with which result; it is read on «Log» with filters by person, kind and day, and downloaded as CSV. The lines sit in the signed chain of the company's data: they cannot be changed or removed without the chain saying so. The server's technical log keeps no IP addresses and no contents.

Which sub-processors handle the data and under which safeguards?

netcup (server, Germany), Backblaze (backups, Netherlands), Scaleway (service e-mails, France), the sign-in service (ZITADEL) by CAOS AG (Switzerland; data in the EU), OpenAI (AI, United States and Ireland), Stripe (payments, Ireland), the browsers' notification services. Each under a processing agreement (art. 28); to the United States the standard contractual clauses and, where applicable, the Data Privacy Framework. Before adding a supplier we tell the companies, who can object.

How and when is our data deleted?

At any time you download everything from «Your data». When the subscription ends, for 90 days you can still enter and download; then, or earlier if you ask, we delete within 30 days (except what the law requires us to keep, such as invoices), with a written two-step procedure (plan, then execution, with fingerprints) that stays on record; Russet itself deletes the backups, at the latest when the lock against deletion expires (up to 14 days).

What happens in case of an incident or a breach?

The state of every part of the service and the incidents of the last 30 days are public on /status, minute by minute; alerts reach the founder's phone. If we discover a breach affecting your data we tell you without delay and in any case within 48 hours: what happened, which data, what we did, what we recommend; we help you with the notices to the authority and to the people (arts. 33 and 34 GDPR). Whoever finds a weakness writes to the address in security.txt. Missing: a formal incident register with cause and lesson; today they are on the status page and in the work diary.

Service continuity: what is lost at most, how fast does it come back?

One hour of work at most (the backup is hourly). The spare server takes the main one's place with measured, written times (docs/operations/SUBENTRO.md); the four emergency procedures are written to be followed without help (docs/operations/EMERGENZA.md). Who answers you and how fast is on /support. Russet today is one person: the continuity of people (who steps in if the founder cannot) is the weak point and has to be written in the contract.

How secure is the way you develop and release?

Every version passes hundreds of automated tests, 26 test files on security alone (every address without a session, a company trying to read another's, a stolen database, words that never become commands); dependencies are pinned (package-lock); the installed package is checked against every file's fingerprint before it starts; the pages load no third-party scripts. Missing: code review by a second person and a third-party penetration test, due after the first customer.

What do you do with artificial intelligence on our data?

OpenAI's models through the business interfaces: the data does not train the models, answers are not stored (requests kept at most 30 days for abuse monitoring). Only the text needed reaches the model: numbers and roles, never your customers' names, passwords or keys. Every call has a spending cap and is recorded. By default Russet proposes and a person decides; the software the factory writes runs in an isolated container, without network.

Do you hold SOC 2 or ISO 27001?

No, not yet, and we do not say we do. The suppliers do (netcup ISO 27001 and 27701; Backblaze SOC 2 Type 2). Russet's controls are put in the order SOC 2 and ISO 27001 ask, each with where it lives in the code and its proof, and with what is missing written honestly: /security/controlli. The real certification comes later, with the paperwork: an accredited auditor and the missing documents.

SOC 2 and ISO 27001 controls

16 controls in place, 9 partly, 2 missing. Every control as SOC 2 (Trust Services Criteria) and ISO/IEC 27001:2022 (Annex A) ask it: where it lives in Russet, the proof, the state. No certification: this is the honest map to get there, the paperwork afterwards.

- ORG-1 · Written security policies and responsibilities — partly: One approved, dated security policy with a yearly review: today the rules are written page by page (security, access, emergencies), not collected and signed.
- ORG-2 · Risk and threat assessment — partly: A risk register with likelihood, impact, owner and periodic review: today risks are handled as automated tests, not listed in a register.
- ORG-3 · Suppliers: list, role, country, agreements — in place
- ORG-4 · People: screening, confidentiality, training — missing: Russet today is one person, with no employees: when the first one arrives, a contract with a confidentiality clause, screening and yearly security training are needed.
- ACC-1 · Roles and permissions per person (four roles, one matrix) — in place
- ACC-2 · Strong sign-in: password and second step for everyone; passkeys and authenticator app — in place
- ACC-3 · Company account sign-in (Microsoft Entra ID, Google) and people from the company group (SCIM 2.0, group read) — partly: On request, to be switched on: today it is off on the server. Tested with fake Microsoft and Google answering like the real ones; it is switched on, and tested with a real tenant, when a company asks and the founder registers Russet's application with both.
- ACC-4 · Leavers are out: removal, sessions ended, access review — partly: The periodic access review is automatic only for who comes from the company group; for people invited by hand a quarterly reminder to the administrator is missing.
- ACC-5 · Sessions: lifetime, remembered devices, verification before sensitive operations — in place
- ACC-6 · Separation between companies: separate databases, no request reads another's data — in place
- ACC-7 · Russet support access only with the owner's permission, time-boxed, reason written — in place
- DAT-1 · Encryption in transit (HTTPS, HSTS) and of secrets on the server (AES-256-GCM) — in place
- DAT-2 · Minimisation: no IP addresses written, bank statement read and discarded, names never to the AI — in place
- DAT-3 · Deletion and return: data downloadable at any time, 90 days after the end, then deleted within 30; backups deleted by Russet after 14 — in place
- DAT-4 · Antivirus on every kept file; files only read are not saved — in place
- DAT-5 · Browser rules on every page: Content Security Policy, no embedding, no cache, no third-party scripts — in place
- OPS-1 · Hourly backups, encrypted before leaving, in a second European data centre; read back and compared byte by byte — in place
- OPS-2 · Continuity: restore into a separate folder tested, written scenarios, measured failover of the spare — partly: The full restore drill on the real server, with date and times written, has to be repeated on a calendar (every six months): today it is tested in code and documented, not yet scheduled.
- OPS-3 · Log of every company action (who or what, data, rule, result) in the signed chain; technical log without IP addresses or contents — in place
- OPS-4 · Monitoring: public status minute by minute, alerts on the founder's phone, incidents of the last 30 days — in place
- OPS-5 · Incidents: companies told within 48 hours, written procedures, a channel to report a weakness (security.txt) — partly: An incident register with cause, fix and lesson for each one, even when customers' data is not affected: today the service's incidents are on the status page, the lessons in the work diary.
- OPS-6 · Changes: every version passes the automated tests; the installed package is checked against every file's fingerprint; pinned dependencies — partly: Code review by a second person before installation: today one person writes and installs, with the automated tests as the check.
- OPS-7 · Vulnerabilities: security tests on the code at every version; third-party penetration test — partly: A third-party penetration test with its report: never done. It costs a few thousand euros and comes after the first customer.
- OPS-8 · Physical and server security: provider's data centre certified ISO 27001; secrets in files readable by the service alone — in place
- OPS-9 · Artificial intelligence: spending cap on every call, recorded; no training on the data; names never to the model; generated software runs isolated — in place
- PRI-1 · GDPR: art. 28 agreement, privacy notice, people's requests within a month, suppliers under agreement — partly: The art. 28 agreement text reviewed by the lawyer and signed with the contract: today the commitments are on the Security page, the text to sign does not exist yet.
- PRI-2 · Russet's own SOC 2 / ISO 27001 certification — missing: The real certification comes later, with the paperwork: an

accredited auditor, 6–12 months, the documents of the «partly» and «missing» lines above. The suppliers (netcup ISO 27001/27701, Backblaze SOC 2 Type 2) are already certified.