Questionario di sicurezza

Le risposte pronte alle domande che l’ufficio sicurezza di un’azienda grande fa prima di comprare. Dicono quello che Russet fa oggi; dove una cosa manca, è scritto «manca» e cosa serve. Aggiornato al 19 novembre 2026.

Dove stanno i nostri dati e chi li tratta?

Il servizio gira in Germania (netcup GmbH, ISO 27001 e 27701); le copie di sicurezza stanno nei Paesi Bassi (Backblaze, SOC 2 Type 2), cifrate prima di uscire dal server. I vostri dati che vanno all’intelligenza artificiale raggiungono solo OpenAI (Stati Uniti e Irlanda), senza i nomi dei vostri clienti; il lavoro interno del team Russet, senza i vostri dati, anche Anthropic (Stati Uniti). La posta di Russet è presso Microsoft; le email di servizio partono da Scaleway (Francia); il collegamento alla banca, se lo attivate, passa da Enable Banking (Finlandia). Ogni azienda ha i suoi database, in cartelle separate. L’elenco completo dei fornitori, con paese e ruolo, è su /sicurezza e sulla privacy.

Come sono cifrati i dati, in transito e a riposo?

In transito sempre HTTPS con HSTS; i cookie di sessione sono legati al solo dominio di Russet. A riposo: i segreti (credenziali dei sistemi collegati, token, chiavi) e le copie di sicurezza sono cifrati con AES-256-GCM con chiavi che stanno solo sul server, in file leggibili dal solo servizio; il disco del server è del fornitore certificato. I database delle aziende sul server non sono cifrati a livello di file: li protegge l’accesso al server (solo il servizio) e la separazione per azienda.

Copie di sicurezza e ripristino: ogni quanto, dove, provati?

Una copia di ogni azienda ogni ora, cifrata, mandata in un secondo centro dati in Europa e riletta byte per byte subito dopo e nei giorni seguenti. Ogni copia vive 14 giorni, poi la cancella Russet stesso (l’ultima di un’azienda attiva resta). Il ripristino si fa in una cartella a parte, mai sopra i dati in uso, ed è provato dalle prove automatiche (restore-all, restore-atomicity) e dagli scenari scritti (docs/operations/SCENARI-RIPRISTINO.md). Manca la prova completa a calendario sul server vero: va fatta ogni sei mesi.

Come si controllano gli accessi delle persone?

Quattro ruoli (amministratore, responsabile crediti, addetto, sola lettura) decisi da chi amministra, con la matrice «chi vede e chi fa cosa» scritta in un posto solo e applicata da ogni pagina. Password e secondo passaggio obbligatorio per tutti, imposto dalle pagine d’accesso di Russet (passkey, app di autenticazione o codice email); titolare e amministratori devono avere una passkey o l’app; su un dispositivo che la persona sceglie di ricordare il secondo passaggio torna ogni 30 giorni; per le operazioni delicate Russet chiede di nuovo chi sei. Accesso con l’account aziendale (Microsoft Entra ID o Google), su richiesta e da attivare (oggi spento sul server): entrano le persone del gruppo che scegliete, con il ruolo del gruppo; chi esce dal gruppo non entra più (letto a ogni entrata e ogni giorno, o spinto dal vostro sistema via SCIM 2.0). Togliere una persona chiude subito le sue sessioni.

C’è un registro di chi ha fatto cosa?

Sì: ogni azione nello spazio dell’azienda (una persona, Russet da solo, un agente, la cura quotidiana) è una riga con chi o cosa, su quali dati, con quale regola, con quale risultato; si guarda su «Registro» con i filtri per persona, tipo e giorno, e si scarica in CSV. Le righe stanno nella catena firmata dei dati dell’azienda: non si modificano né si tolgono senza che la catena lo dica. Il registro tecnico del server non tiene indirizzi IP né contenuti.

Quali sub-fornitori trattano i dati e con quali garanzie?

netcup (server, Germania), Backblaze (copie, Paesi Bassi), Scaleway (email di servizio, Francia), il servizio di

accesso (ZITADEL) di CAOS AG (Svizzera; dati nell'Unione Europea), OpenAI (IA, Stati Uniti e Irlanda), Stripe (pagamenti, Irlanda), i servizi di notifica del browser. Ognuno con un accordo sul trattamento (art. 28); verso gli Stati Uniti le clausole contrattuali tipo e, dove applicabile, il Data Privacy Framework. Se aggiungiamo un fornitore lo diciamo prima alle aziende, che possono opporsi.

Come e quando vengono cancellati i nostri dati?

In ogni momento scaricate tutto da «I tuoi dati». Quando l'abbonamento finisce, per 90 giorni potete ancora entrare a scaricare; poi, o prima se lo chiedete, cancelliamo entro 30 giorni (salvo quello che la legge ci chiede di tenere, come le fatture), con una procedura a due passi scritta (piano, poi esecuzione, con le impronte) che resta registrata; le copie di sicurezza le cancella Russet stesso, al più tardi quando scade il blocco contro la cancellazione (fino a 14 giorni).

Cosa succede in caso di incidente o violazione?

Lo stato di ogni parte del servizio e gli incidenti degli ultimi 30 giorni sono pubblici su /stato, minuto per minuto; gli allarmi arrivano sul telefono del fondatore. Se scopriamo una violazione che riguarda i vostri dati vi avvisiamo senza ritardo e comunque entro 48 ore: cosa è successo, quali dati, cosa abbiamo fatto, cosa vi consigliamo; vi aiutiamo con le comunicazioni al Garante e alle persone (artt. 33 e 34 GDPR). Chi trova una debolezza ci scrive all'indirizzo in security.txt. Manca un registro formale degli incidenti con causa e lezione: oggi stanno nella pagina di stato e nel diario di lavoro.

Continuità del servizio: cosa si perde al massimo, in quanto si riparte?

Al massimo un'ora di lavoro (la copia è oraria). Il server di riserva prende il posto di quello principale con tempi misurati e scritti (docs/operations/SUBENTRO.md); le quattro procedure di emergenza sono scritte per essere seguite senza aiuto (docs/operations/EMERGENZA.md). Chi vi risponde e in quanto tempo è su /assistenza. Russet oggi è una persona sola: la continuità delle persone (chi interviene se il fondatore non può) è il punto debole e va scritta nel contratto.

Come è sicuro il modo in cui sviluppate e rilasciate?

Ogni versione passa centinaia di prove automatiche, 26 file di prove solo di sicurezza (ogni indirizzo senza sessione, un'azienda che prova a leggerne un'altra, un database rubato, parole che non diventano comandi); le dipendenze sono fissate (package-lock); il pacchetto installato è verificato con l'impronta di ogni file prima di partire; le pagine non caricano script di terzi. Manca la revisione del codice da una seconda persona e manca un penetration test di terzi: si fa dopo il primo cliente.

Che uso fate dell'intelligenza artificiale sui nostri dati?

I modelli di OpenAI attraverso le interfacce per le aziende: i dati non addestrano i modelli, le risposte non si conservano (richieste al massimo 30 giorni per i controlli contro gli abusi). Al modello arriva solo il testo che serve: numeri e ruoli, mai nomi dei vostri clienti, password o chiavi. Ogni chiamata ha un tetto di spesa ed è registrata. Di base Russet propone e una persona decide; il software che la fabbrica scrive gira in un contenitore isolato, senza rete.

Avete SOC 2 o ISO 27001?

No, non ancora, e non lo diciamo. I fornitori sì (netcup ISO 27001 e 27701; Backblaze SOC 2 Type 2). I controlli di Russet sono messi in ordine come li chiedono SOC 2 e ISO 27001, con per ciascuno dove sta nel codice e la prova, e con scritto onestamente cosa manca: /sicurezza/controlli. La certificazione vera arriva dopo, con la burocrazia: un revisore accreditato e i documenti che mancano.

Controlli SOC 2 e ISO 27001

16 controlli ci sono, 9 in parte, 2 mancano. Ogni controllo come lo chiedono SOC 2 (Trust Services Criteria) e ISO/IEC 27001:2022 (Allegato A): dove sta in Russet, la prova, lo stato. Nessuna certificazione: questa è la mappa onesta per arrivarci, con la burocrazia dopo.

- ORG-1 · Politiche di sicurezza scritte e responsabilità — in parte: Un documento unico di politica della sicurezza approvato e datato, con il riesame annuale: oggi le regole sono scritte pagina per pagina (sicurezza, accesso, emergenze), non raccolte e firmate.
- ORG-2 · Valutazione dei rischi e delle minacce — in parte: Un registro dei rischi con probabilità, impatto, proprietario e riesame periodico: oggi i rischi sono trattati come prove automatiche, non elencati in un registro.
- ORG-3 · Fornitori: elenco, ruolo, paese, accordi — c'è
- ORG-4 · Persone: verifiche all'assunzione, riservatezza, formazione — manca: Russet oggi è una persona sola, senza dipendenti: quando arriva la prima, servono il contratto con la clausola di riservatezza, la verifica e la formazione annuale sulla sicurezza.
- ACC-1 · Ruoli e permessi per persona (quattro ruoli, matrice in un posto) — c'è
- ACC-2 · Accesso forte: password e secondo passaggio per tutti; passkey e app di autenticazione — c'è
- ACC-3 · Accesso con l'account aziendale (Microsoft Entra ID, Google) e persone dal gruppo aziendale (SCIM 2.0, lettura del gruppo) — in parte: Su richiesta, da attivare: oggi è spento sul server. Provato con Microsoft e Google finti che rispondono come quelli veri; si accende, e si prova con un tenant vero, quando un'azienda lo chiede e il fondatore registra l'applicazione di Russet nei due servizi.
- ACC-4 · Chi esce non entra più: rimozione, sessioni chiuse, riesame degli accessi — in parte: Il riesame periodico degli accessi è automatico solo per chi entra dal gruppo aziendale; per le persone invitate a mano manca un promemoria trimestrale all'amministratore.
- ACC-5 · Sessioni: durata, dispositivi ricordati, verifica prima delle operazioni delicate — c'è
- ACC-6 · Separazione tra aziende: database separati, nessuna richiesta legge i dati di un'altra — c'è
- ACC-7 · Accesso dell'assistenza Russet solo col permesso del titolare, a tempo, con il motivo scritto — c'è
- DAT-1 · Cifratura in transito (HTTPS, HSTS) e dei segreti sul server (AES-256-GCM) — c'è
- DAT-2 · Minimizzazione: niente indirizzi IP scritti, estratto conto letto e buttato, nomi mai all'IA — c'è
- DAT-3 · Cancellazione e restituzione: dati scaricabili sempre, 90 giorni dopo la fine, poi cancellati entro 30; copie cancellate da Russet dopo 14 — c'è
- DAT-4 · Antivirus su ogni file conservato; i file letti soltanto non si salvano — c'è
- DAT-5 · Regole del browser su ogni pagina: Content Security Policy, niente incorporamento, niente cache, niente script di terzi — c'è
- OPS-1 · Copie ogni ora, cifrate prima di uscire, in un secondo centro dati in Europa; rilette e confrontate byte per byte — c'è
- OPS-2 · Continuità: ripristino in una cartella a parte provato, scenari scritti, subentro della riserva misurato — in parte: La prova di ripristino completo sul server vero, con la data e i tempi scritti, va ripetuta a calendario (ogni sei mesi): oggi è provata nel codice e documentata, non ancora a calendario.
- OPS-3 · Registro di ogni azione dell'azienda (chi o cosa, dati, regola, risultato) nella catena firmata; registro tecnico senza indirizzi IP né contenuti — c'è
- OPS-4 · Monitoraggio: stato pubblico minuto per minuto, allarmi sul telefono del fondatore, incidenti degli ultimi 30 giorni — c'è
- OPS-5 · Incidenti: avviso alle aziende entro 48 ore, procedure scritte, canale per segnalare una debolezza (security.txt) — in parte: Un registro degli incidenti con causa, rimedio e lezione per ciascuno, anche quando non riguardano i dati delle aziende: oggi gli incidenti del servizio sono nella pagina di stato, le lezioni nel diario di lavoro.
- OPS-6 · Cambiamenti: ogni versione passa le prove automatiche; il pacchetto installato è verificato con l'impronta di ogni file; dipendenze fissate — in parte: La revisione del codice da parte di una seconda persona prima dell'installazione: oggi scrive e installa una persona sola, con le prove automatiche come controllo.
- OPS-7 · Vulnerabilità: prove di sicurezza sul codice a ogni versione; penetration test di terzi — in parte: Un penetration test di una società terza, con il rapporto: non è mai stato fatto. Costa qualche migliaio di euro e si fa dopo il primo cliente.
- OPS-8 · Sicurezza fisica e del server: centro dati del fornitore certificato ISO 27001; segreti in file leggibili dal solo servizio — c'è
- OPS-9 · Intelligenza artificiale: tetto di spesa su ogni chiamata, registrata; niente addestramento sui dati; nomi mai al modello; il software generato gira isolato — c'è

- PRI-1 · GDPR: accordo art. 28, privacy, richieste delle persone entro un mese, fornitori con accordo — in parte: Il testo dell’accordo art. 28 riletto dall’avvocato e firmato col contratto: oggi gli impegni sono scritti sulla pagina Sicurezza, il testo da firmare non c’è ancora.
- PRI-2 · Certificazione SOC 2 / ISO 27001 di Russet — manca: La certificazione vera arriva dopo, con la burocrazia: un revisore accreditato, 6–12 mesi, i documenti delle righe «in parte» e «manca» qui sopra. I fornitori (netcup ISO 27001/27701, Backblaze SOC 2 Type 2) sono già certificati.