

Pachet de răspunsuri NIS2 / DORA — SalesOS

Generat la 20.10.2026 · Ultima revizuire 2026-10-22

Versiune de lucru: răspunsurile organizaționale sunt în curs de confirmare.

Contact securitate: security@salesoscrm.com · Contact confidențialitate: privacy@salesoscrm.com

Găzduire și locația datelor

- Aplicația, baza de date, fișierele și copiile de siguranță sunt găzduite în UE (Germania (UE)) de Hetzner Online GmbH.
- SalesOS nu mută datele clienților în afara SEE; subprocesatorii din afara SEE sunt enumerați mai jos și sunt folosiți doar când funcția respectivă este activată.
- Procesare AI doar în UE (Setări > AI): Claude rulează pe Amazon Bedrock sau Google Vertex AI într-o regiune UE, iar funcțiile AI fără variantă în UE sunt oprite.

Criptare

- În tranzit: TLS 1.2 sau mai nou pe fiecare conexiune către aplicație și API.
- În repaus: credențialele integrărilor, secretele API, secretele de autentificare în doi pași și câmpurile cu date personale care nu sunt căutate (telefonul mobil și adresa contactului) sunt criptate în baza de date cu AES-256.
- Parolele sunt stocate ca hash bcrypt; codurile de recuperare și cheile API ca hash-uri ireversibile.

Controlul accesului

- Autentificare în doi pași (TOTP) pentru fiecare utilizator, pe care o companie o poate face obligatorie.
- Autentificare unică (SSO) cu Microsoft Entra ID, Google Workspace sau orice furnizor OpenID Connect.
- Liste de IP-uri permise pentru sesiuni și chei API, durata sesiunii și deconectarea la inactivitate setate per companie.
- Permisuni pe roluri; datele fiecărei companii sunt izolate per client, iar fiecare eveniment de securitate este scris în jurnalul de audit.

Copii de siguranță și continuitate

- Copii de siguranță zilnice, criptate, ale bazei de date, păstrate 30 zile. Stocate în UE, separat de serverul aplicației.
- Restaurarea se testează cel puțin trimestrial. Obiectivul punctului de recuperare: 24 ore; obiectivul timpului de recuperare: 8 ore.

Datele voastre, ieșirea voastră

- Un proprietar poate exporta oricând toate datele companiei (Regulamentul UE privind datele): o arhivă ZIP cu fiecare tabel în JSON și toate fișierele, printr-un link semnat care expiră.
- Fără taxe de ieșire. Datele sunt șterse după încetarea contractului, conform acordului de prelucrare a datelor.

Incidente

- Raportați o problemă de securitate la security@salesoscrm.com. Confirmăm primirea în cel mult o zi lucrătoare.
- Clienții afectați sunt informați despre o încălcare a securității datelor personale în cel mult 24 ore de la confirmare, cu ce se știe și ce măsuri luăm.

NIS2 — măsurile de securitate ale furnizorului (art. 21)

Aveți politici de analiză a riscurilor și de securitate a informațiilor?

Da. Riscurile sunt revizuite la fiecare versiune; acest pachet este revizuit cel puțin anual (ultima revizuire: 2026-10-22).

Cum gestionați și raportați incidentele?

Evenimentele de securitate (autentificări eșuate, IP-uri blocate, modificări 2FA, cereri de chei API, exporturi) sunt jurnalizate și alertează administratorii clientului. Clienții sunt informați despre incidentele care îi afectează în 24 ore; acolo unde intrăm sub incidența NIS2, trimitem CSIRT-ului o avertizare timpurie în 24 ore și o notificare în 72 ore.

Cum asigurați continuitatea activității și copiile de siguranță?

Copii de siguranță zilnice, criptate, ale bazei de date, păstrate 30 zile în UE. RPO 24 h, RTO 8 h. Restaurarea se testează cel puțin trimestrial.

Ce subprocesatori folosiți și unde?

Vedeți lista subprocesatorilor din acest pachet. Subprocesatorii din afara SEE sunt folosiți doar când funcția respectivă este activată, pe baza clauzelor contractuale standard.

Cum este tratată securitatea în dezvoltare și mentenanță?

Fiecare modificare trece prin revizuire de cod și o suită automată de teste, inclusiv teste că fiecare rută API verifică permisiunile și izolarea pe client. Dependențele sunt actualizate regulat.

Ce criptografie folosiți?

TLS 1.2+ în tranzit; AES-256 pentru secrete și date personale necăutate în repaus; bcrypt pentru parole; HMAC-SHA256 pentru codurile de recuperare și linkurile semnate.

Oferiți autentificare multifactor și control al accesului?

Da: autentificare în doi pași TOTP (poate fi obligatorie per companie), SSO prin OpenID Connect, liste de IP-uri permise, limite de sesiune și permisiuni pe roluri. SAML nu este oferit.

Personalul vostru primește instruire de securitate?

Da, la angajare și anual. Accesul personalului la producție este limitat la persoane numite și necesită autentificare în doi pași.

DORA — clauze contractuale pentru furnizorii TIC (art. 28 și 30)

Unde sunt prestate serviciile și unde sunt prelucrate și stocate datele?

În UE (Germania (UE)), cu subprocesatorii enumerați în acest pachet.

Cum asigurați disponibilitatea, integritatea și confidențialitatea datelor?

Izolare pe client la fiecare interogare, criptare în tranzit și în repaus, copii de siguranță zilnice, jurnal de audit și controalele de acces de mai sus.

Ne veți asista când apare un incident TIC legat de serviciul vostru?

Da, fără cost suplimentar: notificare în 24 ore, jurnalele și înregistrările de audit relevante și un raport scris al incidentului.

Veți coopera cu autoritățile competente?

Da, inclusiv cu autoritatea de supraveghere a clientului și cu persoanele desemnate de aceasta.

Avem drepturi de audit, acces și inspecție?

Da, cu notificare rezonabilă, conform acordului de prelucrare a datelor; acest pachet și exportul jurnalului de audit răspund la majoritatea întrebărilor fără o vizită.

Care sunt drepturile de reziliere și strategia de ieșire?

Clientul poate rezilia conform contractului; înainte și timp de 30 de zile după reziliere, un proprietar poate descărca gratuit exportul complet al datelor (Regulamentul UE privind datele). Apoi datele sunt șterse.

Cum gestionați subcontractarea funcțiilor critice?

Subprocesatorii sunt enumerați în acest pachet și în acordul de prelucrare; clienții sunt informați în avans despre modificări și pot obiecta.

Subprocesatori

Furnizor	Scop	Locație
SalesOS hosting (EU data centre)	Găzduirea aplicației, baza de date și copiile de siguranță	EU
Resend	Trimiterea emailurilor tranzacționale și de campanie	US
Google (Gmail, Calendar)	Sincronizarea emailului și a calendarului utilizatorilor conectați	US / EU
Anthropic	Funcții AI: rezumate, agenți, redactare	US
Amazon Web Services (Bedrock)	Funcții AI cu procesare AI doar în UE (Claude într-o regiune UE)	EU
Google Cloud (Vertex AI)	Funcții AI cu procesare AI doar în UE (Claude într-o regiune UE)	EU

Furnizor	Scop	Locație
OpenAI	Transcriere și funcții AI, unde sunt selectate	US
Fathom	Înregistrări și transcrieri ale apelurilor	US
Meta (WhatsApp Business)	Mesagerie WhatsApp	US / EU
People Data Labs	Îmbogățirea datelor de contact și de companie	US
Apollo.io	Îmbogățirea datelor de contact și de companie	US
Hunter.io	Găsirea și verificarea adreselor de email	EU
SmartBill	Facturare și e-Factura	RO