

NIS2 / DORA answer pack — SalesOS

Generated on 18.10.2026 · Last reviewed 2026-10-22

Draft: the organisational answers are being confirmed.

Security contact: security@salesoscrm.com · Privacy contact: privacy@salesoscrm.com

Hosting and data location

- Application, database, files and backups are hosted in the EU (Germany (EU)) by Hetzner Online GmbH.
- Customer data is not moved outside the EEA by SalesOS itself; sub-processors outside the EEA are listed below and used only when the matching feature is switched on.
- EU-only AI processing (Settings > AI): Claude runs on Amazon Bedrock or Google Vertex AI in an EU region, and AI features with no EU option are switched off.

Encryption

- In transit: TLS 1.2 or later on every connection to the application and API.
- At rest: integration credentials, API secrets, two-factor secrets and personal data fields that are not searched (contact mobile number and address) are encrypted in the database with AES-256.
- Passwords are stored as bcrypt hashes; recovery codes and API keys as one-way hashes.

Access control

- Two-factor authentication (TOTP) for every user, which a company can make mandatory.
- Single sign-on with Microsoft Entra ID, Google Workspace or any OpenID Connect provider.
- IP allowlists for app sessions and API keys, session lifetime and idle timeout set per company.
- Role-based permissions; every company's data is isolated by tenant and every security event is written to the audit log.

Backups and continuity

- Daily encrypted database backups, kept for 30 days. Stored in the EU, separate from the application server.
- Restores are tested at least quarterly. Recovery point objective 24 hours, recovery time objective 8 hours.

Your data, your exit

- An owner can export all company data at any time (EU Data Act): one ZIP with every table as JSON plus all files, behind a signed link that expires.
- No exit fees. Data is deleted after the contract ends, per the data processing agreement.

Incidents

- Report a security issue to security@salesoscrm.com. We acknowledge within one business day.
- Affected customers are told about a personal data breach within 24 hours of it being confirmed, with what is known and what we are doing.

NIS2 — supplier security measures (art. 21)

Do you have risk analysis and information security policies?

Yes. Risks are reviewed with every release; this pack is reviewed at least yearly (last review: 2026-10-22).

How do you handle and report incidents?

Security events (failed sign-ins, blocked IPs, 2FA changes, API key requests, exports) are logged and alert the customer's administrators. Customers are notified of incidents affecting them within 24 hours; where we are in scope of NIS2 we send the CSIRT an early warning within 24 hours and a notification within 72 hours.

How do you ensure business continuity and backups?

Daily encrypted database backups, kept 30 days in the EU. RPO 24 h, RTO 8 h. Restores are tested at least quarterly.

Which sub-processors do you use, and where?

See the sub-processor list in this pack. Sub-processors outside the EEA are used only when the matching feature is on, under standard contractual clauses.

How is security handled in development and maintenance?

Every change goes through code review and an automated test suite, including tests that every API route is permission-checked and tenant-isolated. Dependencies are updated regularly.

What cryptography do you use?

TLS 1.2+ in transit; AES-256 for secrets and unsearched personal data at rest; bcrypt for passwords; HMAC-SHA256 for recovery codes and signed links.

Do you support multi-factor authentication and access control?

Yes: TOTP two-factor authentication (can be made mandatory per company), SSO via OpenID Connect, IP allowlists, session limits and role-based permissions. SAML is not offered.

Do your staff receive security training?

Yes, at onboarding and yearly. Staff access to production is limited to named people and requires two-factor authentication.

DORA — ICT third-party contract terms (art. 28 and 30)

Where are the services provided and the data processed and stored?

In the EU (Germany (EU)), with the sub-processors listed in this pack.

How do you ensure availability, integrity and confidentiality of data?

Tenant isolation on every query, encryption in transit and at rest, daily backups, an audit log and the access controls above.

Will you assist us when an ICT incident related to your service occurs?

Yes, at no extra cost: notice within 24 hours, the relevant logs and audit entries, and a written incident report.

Will you cooperate with competent authorities?

Yes, including the customer's supervisory authority and its appointees.

Do we have audit, access and inspection rights?

Yes, on reasonable notice, as set out in the data processing agreement; this pack and the audit log export answer most questions without a visit.

What are the termination rights and the exit strategy?

The customer can terminate under the contract; before and for 30 days after termination an owner can download the full tenant export (EU Data Act) at no cost. Data is then deleted.

How do you handle subcontracting of critical functions?

Sub-processors are listed in this pack and the DPA; customers are told of changes in advance and may object.

Sub-processors

Provider	Purpose	Location
SalesOS hosting (EU data centre)	Application hosting, database and backups	EU
Resend	Sending transactional and campaign email	US
Google (Gmail, Calendar)	Email and calendar sync for connected users	US / EU
Anthropic	AI features: summaries, agents, drafting	US
Amazon Web Services (Bedrock)	AI features under EU-only AI processing (Claude in an EU region)	EU
Google Cloud (Vertex AI)	AI features under EU-only AI processing (Claude in an EU region)	EU
OpenAI	Speech-to-text and AI features where selected	US
Fathom	Call recordings and transcripts	US

Provider	Purpose	Location
Meta (WhatsApp Business)	WhatsApp messaging	US / EU
People Data Labs	Contact and company enrichment	US
Apollo.io	Contact and company enrichment	US
Hunter.io	Email finding and verification	EU
SmartBill	Invoicing and e-Factura	RO