SÄKERHET OCH DATAHANTERING

Så förvaras, skyddas och återställs er data i GoGood CRM

Underlaget vänder sig till er IT- och inköpsgranskning. Det beskriver var datan lagras, hur den krypteras, hur behörigheter styrs och vad som händer vid ett avbrott. Uppgifterna kontrollerades i den körande miljön den 31 oktober 2026. Punkter som vi inte själva kan kontrollera är markerade som att de bekräftas med driftleverantören.

Lagring	PostgreSQL-databas och filutrymme i EU-regionen (Irland) hos Lovable Cloud.
Transport	All trafik går över HTTPS/TLS med HSTS (ett år, inklusive underdomäner).
Behörigheter	Radnivåskydd (RLS) aktivt på alla tabeller i databasen.
Filer	Fem filutrymmen, samtliga privata. Ingen fil är publikt läsbar.
Nycklar	API-nycklar till integrationer krypteras och är bara åtkomliga för servern.
Ändringslogg	Vem som ändrar priser, kunder, roller och behörigheter loggas.
Konton	Bara via inbjudan. Fri registrering är avstängd.
Inaktivitet	Automatisk utloggning efter 8 timmar utan aktivitet.
Granskning	Nytt: Fördjupad säkerhetsgranskning av koden genomförd. Allvarliga fynd är åtgärdade.

Kort sammanfattat
– Datan lagras i EU och delas aldrig mellan säljbolag.
– Ingen kund kan se en annan kunds data. Behörigheten avgörs per rad i databasen.
– Integrationsnycklar är krypterade och kan inte läsas av någon inloggad användare.
– Certifieringar (SOC 2 / ISO 27001) finns inte ännu, se sidan 5.

Vad som behövs från er

Databehandling (DPA)	Ett personuppgiftsbiträdesavtal tecknas innan ni lägger in riktig kunddata.
Kontaktlista	Namn på dem som ska ha konto och vilken roll de ska ha. Vi skickar inbjudningar.
Krav	Säg till i god tid om ni kräver certifiering eller extern granskning.

VAR DATAN LAGRAS

Lagring

Databas	PostgreSQL hos Lovable Cloud, region EU (Irland). Innehåller kunder, besök, ordrar, distribution, statistik och avtal.
Filutrymme	Fem utrymmen för foton, planogram, logotyper och bilagor. Samtliga är privata, med en storleksgräns på 2–20 MB per fil.
Leverans	Webbsidan levereras via Cloudflare. Själva datan hämtas från EU-lagringen.
Underleverantörer	Fortnox och andra kopplingar får bara de uppgifter som respektive koppling kräver.

Kryptering

Transport	HTTPS/TLS till webbläsare och mobil. HSTS med max-age ett år och includeSubDomains tvingar fram krypterad förbindelse.
Lagrad data	Databas och filer ligger på lagring som krypteras av molnleverantören (bekräftas med driftleverantören).
Lösenord	Sparas som hash, aldrig i klartext.
Integrationsnycklar	Inloggningsnycklar till Fortnox och kommande system krypteras (AES-256) innan de sparas. Krypteringsnyckeln förvaras i ett separat, skyddat hemlighetslager, inte i databasen.
Power BI-nycklar	Lagras som hash med en kort synlig del. Varje nyckel kan dras tillbaka och visar när den senast användes.

BEHÖRIGHETER OCH ÅTKOMST

Behörigheter

Systemet är byggt för flera säljbolag som aldrig ska se varandra. Varje rad i databasen hör till ett bolag, och reglerna avgör vad en inloggad person får läsa eller ändra.

Radnivåskydd	Aktivt på alla tabeller. Rader som reglerna inte släpper fram syns inte.
Bolagsisolering	Kunder, ordrar och besök kopplas till ett säljbolag när de sparas. En användare når bara de bolag som den tillhör.
Bolagsbundna åtgärder	Nytt: Att skicka order till Fortnox och flytta kunder mellan säljare kontrolleras mot det egna bolaget på servern.
Roller	Ägare, admin, säljare och läsare. Ändringar av roller loggas.
Läsare	En roll som kan se men inte ändra något.
Visa som	Behöriga kan öppna en annan användares vy med en riktig, tidsbegränsad session inom samma bolag.
Konton	Det går inte att skapa ett konto själv. Nya användare kommer in bara via inbjudan.
Utloggning	Efter 8 timmar utan aktivitet loggas användaren ut automatiskt.
Automatiska jobb	Nytt: Synk och rättningar körs bara av systemets egen schemaläggare med en hemlig nyckel. Utomstående kan inte starta dem.
Beräknade värden	Nytt: Besöksbetyg räknas alltid fram på servern och kan inte skrivas direkt av användare.

Ändringslogg
– Loggar vem som skapar, ändrar och tar bort priser, prislistor, artiklar, kunder, kundansvar, klassificeringar, roller och behörigheter.
– Både gammalt och nytt värde sparas, med tidpunkt.
– Bara bolagets admin kan läsa loggen, och bara för det egna bolaget.
– Loggen kan inte ändras eller raderas av användare.

BACKUPS OCH ÅTERSTÄLLNING

Om systemet kraschar

Säkerhetskopiering sköts av driftleverantören. De exakta villkoren bekräftas skriftligt innan avtal.

Kopior	Databasen säkerhetskopieras automatiskt av driftleverantören. Intervall och hur långt bak man kan återställa bekräftas med leverantören.
Innehåll	Databasens struktur och innehåll, inklusive inloggningsuppgifter.
Filer	Om filer i filutrymmena ingår i kopiorna bekräftas med driftleverantören.
Belastningsskydd	En databasfråga från en inloggad användare avbryts efter 15 sekunder.

Egen export
– Statistik och listor kan laddas ner som kalkylark direkt i appen.
– Datan kan hämtas till ert eget Power BI med en nyckel som går att dra tillbaka.

GRANSKNING OCH ÖPPNA PUNKTER

Fördjupad säkerhetsgranskning

Den 31 oktober 2026 granskades koden automatiskt med avseende på inloggning, behörigheter, dataexponering och nycklar. 7 av 8 fynd är åtgärdade, inklusive samtliga allvarliga.

Åtgärdat	Skyddade automatiska jobb, bolagsbundna Fortnox- och kundåtgärder, servergenererade besöksbetyg och spärr så att bara orderns säljare eller admin kan markera plockning.
Kvar (låg risk)	Länkar till planogram-filer kan fungera i upp till 5 minuter efter att åtkomsten dragits in.

Vad som inte finns idag

Certifiering	SOC 2 och ISO 27001 saknas. Vi kan svara på er egen kontrollista.
Tvåstegsinloggning	Planerad för admin och ägare, med valfri kodapp. Ännu inte aktiverad.
Backupvillkor	Intervall, lagringstid och återställning bekräftas med driftleverantören.
Penetrationstest	Ingen extern manuell granskning har gjorts ännu.

Så svarar vi på er granskning

– Vi visar tabeller, regler och filutrymmen tillsammans med er.
– Skicka er kontrollista, så fyller vi i den skriftligt.
– Avtal om databehandling och sekretess tecknas innan riktig kunddata läggs in.