

// SUPABASE

Så fungerar din data.

En guide för dig som är kund hos ZORC — om hur vi hanterar, skyddar och organiserar din data med Supabase.

- 01 Vad är Supabase?
- 02 Databas & tabeller
- 03 Inloggning
- 04 Row Level Security
- 05 Storage — Fillagring
- 06 Edge Functions
- 07 API & klientbibliotek
- 08 Säkerhet & best practices

// 01

Vad är Supabase?

Supabase är en modern dataplattform som ZORC använder för att hantera din data på ett säkert, transparent och skalbart sätt. Tänk på det som ett komplett databackend – platsen där din information lagras, organiseras och hämtas.

I grunden bygger Supabase på **PostgreSQL** – en av världens mest pålitliga databsteknologier, med över 35 års aktiv utveckling. Ovanpå det erbjuder Supabase moderna verktyg för inloggning, fillagring, API:er och serverless-funktioner – allt i ett samlat system.

- **Databas (PostgreSQL)**

Strukturerad lagring av all din affärsdata i tabeller med relationer

- **Inloggning (Auth)**

Säker autentisering för dina användare och system

- **Storage (Fillagring)**

Lagring och leverans av bilder, dokument och filer via CDN

- **API & Edge Functions**

Automatiska API:er och serverless-kod kopplad direkt mot din databas

Varför ZORC valde Supabase

Supabase är open source – koden är öppen och granskningsbar av vem som helst. Din data kan hostas inom EU (vi använder Frankfurt som standard) och plattformen låser inte in dig hos en enda leverantör. ZORC använder Supabase i alla sina moderna projekt, inklusive den egna webbplatsen.

// 02

Databas & tabeller

Din data lagras i en **relationsdatabas** baserad på PostgreSQL. Tänk på det som ett välorganiserat kalkylblad – fast enormt mycket kraftfullare, snabbare och säkrare.

Data organiseras i **tabeller**. Varje tabell representerar en typ av information — exempelvis "kunder", "ordrar" eller "dokument". Tabellerna är kopplade till varandra, vilket gör att systemet kan hämta komplex information effektivt med ett enda anrop.

Exempeltabell: kunder

id	namn	e-post	skapad
a1b2c3...	Anna Svensson	anna@exempel.se	2026-01-15
d4e5f6...	Erik Lindqvist	erik@foretag.se	2026-02-03
g7h8i9...	Maria Karlsson	maria@webb.se	2026-03-11

Varje **rad** är en post (en kund, en order). Varje **kolumn** är ett fält med en specifik datatyp. Supabase validerar alltid att data är i rätt format innan det sparas.

Databasen stöder också **realtid** — din app kan prenumerera på förändringar och uppdateras direkt när data ändras, utan att sidan behöver laddas om.

// 03

Inloggning (Authentication)

Supabase hanterar inloggning och identitet för alla användare i systemet. Lösenord lagras *aldrig* i klartext — de krypteras med bcrypt, industristandard för säker lösenordslagring.

ZORC konfigurerar inloggningsflödet efter projektets behov. Vanligaste metoderna vi implementerar:



E-post & lösenord

Klassisk inloggning. E-postadressen bekräftas vid registrering. Lösenordsåterställning via e-post ingår alltid.



Magic Link

En engångslänk skickas till e-posten. Inga lösenord sparas överhuvudtaget — enkelt och säkert.



Social inloggning (OAuth)

Inloggning via Google, GitHub, Microsoft eller annan tjänst. Inget nytt konto krävs.



Biometrisk inloggning Nytt

ZORC kan nu bygga in inloggning via fingeravtryck eller ansiktsgenkänning för enheter som stödjer det — telefoner, surfplattor och moderna laptops. Säkrare än lösenord och friktionsfritt för användaren.

Sessions och tokens

När en användare loggar in skapar Supabase en krypterad *session* och ett *JWT-token*. Det är detta token som bevisar vem användaren är vid varje anrop — och det löper automatiskt ut vid inaktivitet. Ingen session lagras permanent utan att användaren aktivt valt "håll mig inloggad".

// 04

Row Level Security (RLS)

Row Level Security — RLS — är den viktigaste säkerhetsfunktionen i Supabase. Det är ett inbyggt lager direkt i databasen som kontrollerar exakt vilken data varje inloggad användare har rätt att läsa och ändra, rad för rad.

ZORC aktiverar alltid RLS på alla tabeller med känslig eller användarspecifik data. Det är ett grundkrav i hur vi bygger — inte ett tillval.

HUR RLS FUNGERAR I PRAKTIKEN

A

Ser bara sina egna rader

B

Ser **bara** sina egna rader

ADM

Ser **alla** rader (admin-policy)

Reglerna definieras direkt i databasen, inte i applikationskoden. Det innebär att **ingen kan komma åt data de inte har rätt till** — inte ens om det skulle finnas ett fel i applikationskoden.

Vad detta betyder för dig som kund

Ingen annan kund i systemet kan se din data — oavsett om de är inloggade. RLS är skyddat på databasnivå och kan inte kringgås av API:et eller av framtida ändringar i applikationskoden.

// 05

Storage — Fillagring

Supabase Storage hanterar lagring av filer — bilder, PDF:er, videoklipp och andra dokument. Det är en integrerad del av plattformen och delar samma behörighetsmodell som databasen.

Filer organiseras i **buckets** — tematiska mappar på toppnivå. Varje bucket konfigureras som offentlig eller privat:

Offentlig bucket

Filer är tillgängliga via URL utan inloggning. Passar för offentligt material som profilbilder och produktbilder.

Ex: logotyper, publika bildgallerier

Privat bucket

Rekommenderat

Filer kräver signerade URL:er med tidsbegränsad åtkomst. Ingen kan komma åt filen utan rätt behörighet.

Ex: fakturor, kontrakt, personliga dokument

RLS kan tillämpas även på filer — du styr exakt vem som kan ladda upp, läsa och ta bort. Filerna serveras via ett globalt CDN (Content Delivery Network) för snabb nedladdning oavsett var i världen användaren befinner sig.

// 06

Edge Functions

Edge Functions är serverless-kod som körs nära slutanvändaren, i Supabase infrastruktur — utan att ni behöver underhålla egna servrar. De aktiveras av händelser: när ett formulär skickas, en betalning genomförs, en fil laddas upp eller ett schema triggas.

Typiska fall där ZORC implementerar Edge Functions:

- **E-postutskick** — bekräftelsemail, notifikationer och automatiska påminnelser
- **Betalningshantering** — webhooks från Stripe och andra betaltjänster som uppdaterar er databas
- **AI-integrationer** — anrop till OpenAI, Anthropic och liknande tjänster från servern
- **Affärslogik** — validering och beräkningar som inte ska köras i webbläsaren av säkerhetsskäl

Edge Functions körs i säkra, isolerade miljöer och skalas automatiskt vid belastningstoppar. De kräver noll serverunderhåll och ingen driftsättning av er sida — ZORC hanterar hela livscykeln.

// 07

API & klientbibliotek

Supabase genererar automatiskt ett komplett **REST API** direkt från din databas — ingen extra kod behövs. Det är via detta API som din webbplats eller app kommunicerar med databasen för att läsa och skriva data.

ZORC använder Supabase JavaScript-klient i alla projekt. Den hanterar kommunikationen med API:et och inkluderar inbyggt stöd för autentisering, realtid och fillagring — utan att du behöver skriva HTTP-anrop för hand.

API-nycklar — vad de är och hur de används

anon key

Publik

Används av klienten (webbläsaren) för att kommunicera med databasen. Säker att exponera — RLS begränsar vad som faktiskt är åtkomligt. Utan RLS på plats vore denna nyckel en säkerhetsrisk.

service_role key

Hemlig — aldrig publik

Kringgår alla RLS-regler och har full åtkomst till all data. Används *uteslutande* i Edge Functions och server-side kod. Exponeras aldrig i webbläsaren eller källkoden.

ZORC:s rutin för nycklar

Vi lagrar `service_role`-nyckeln enbart i krypterade miljövariabler på servern. Den finns aldrig i källkoden, versionshanteringen (Git) eller i webbläsaren — och roteras vid misstänkt exponering.

// 08

Säkerhet & best practices

Nedan är de säkerhetsprinciper ZORC alltid tillämpar i Supabase-projekt. Ingen av dessa är valfri — de är inbyggda i hur vi levererar.



EU-datacenter (Stockholm)

All data lagras inom EU, i enlighet med GDPR. ZORC:s standardval är Stockholm – nära, snabbt och inom EU:s dataskyddslagstiftning.



Kryptering i vila och under transit

All data krypteras när den lagras (AES-256) och under överföring (TLS 1.3). Det är omöjligt att läsa data i klartext, även vid fysisk access till serverhårdvaran.



Automatisk backup

Supabase skapar dagliga säkerhetskopior. På Pro-plan och högre finns point-in-time recovery – vi kan återställa din data till exakt ett givet ögonblick tillbaka i tiden.



RLS på alla känsliga tabeller

ZORC aktiverar Row Level Security på samtliga tabeller som hanterar personuppgifter eller känslig affärsdata. Som beskrivet i kapitel 4 är detta ett grundkrav i alla leveranser.



GDPR-efterlevnad & DPA

Supabase tecknar DPA (Data Processing Agreement). ZORC säkerställer att rätt avtal finns på plats och att dataminimering, ändamålsbegränsning och raderingsrutiner implementeras i systemet.

Sammanfattat

Din data lagras på EU-servrar, krypteras i vila och transit, skyddas av databasnivå-regler som inte kan kringgå, säkerhetskopieras dagligen och hanteras i enlighet med GDPR. ZORC ser till att alla dessa lager är på plats och konfigurerade rätt från dag ett.



ZORC

Har du frågor om hur din data hanteras?
Vi svarar alltid inom 24 timmar.

support@zorc.se

010-650 02 14

zorc.se →

