ZORC AB · INTERN POLICY & KUNDINFORMATION

GDPR och dataskyddshantering — hur zorc.se säkerställer lagstadgad efterlevnad

Version: 1.0 · **Datum:** Juni 2026

Utfärdat av: Zorc AB · **Granskas:** Löpande, minst en gång per år

Tillämplig lagstiftning: GDPR (EU) 2016/679 · Dataskyddslagen (2018:218)

1. Bakgrund och syfte

EU:s dataskyddsförordning (GDPR) trädde i kraft den 25 maj 2018 och kompletteras i Sverige av **Dataskyddslagen (SFS 2018:218)**. Lagstiftningen ställer tydliga krav på hur personuppgifter ska hanteras — oavsett om det sker inom en organisation eller via externa tjänsteleverantörer.
Zorc AB utvecklar och driftsätter digitala system åt sina kunder. I den rollen behandlar vi regelmässigt personuppgifter på uppdrag av kunden, vilket innebär att vi träffar avtal om personuppgiftsbehandling och väljer underleverantörer med omsorg. Detta dokument beskriver det rättsliga ramverket, våra åtaganden och hur ansvar fördelas i de system vi bygger.

> TILLSYNSMYNDIGHET I SVERIGE
> **Integritetsskyddsmyndigheten (IMY)** är den svenska tillsynsmyndigheten för dataskyddsfrågor. IMY utövar tillsyn, tar emot anmälningar om dataintrång och kan utfärda sanktionsavgifter. Webbplats: *imy.se*

2. Gällande lagstiftning — vad innebär GDPR?

GDPR reglerar all behandling av personuppgifter som sker inom EU/EES, eller som rör EU-medborgare. Med *personuppgifter* avses all information som direkt eller indirekt kan identifiera en levande person — namn, e-postadress, IP-adress, användar-ID m.m.

De sju grundläggande principerna

1. **Laglighet, korrekthet och öppenhet** — Behandlingen måste ha en rättslig grund och vara transparent mot den registrerade.
2. **Ändamålsbegränsning** — Uppgifter får bara samlas in för specificerade, uttryckliga och berättigade ändamål.
3. **Uppgiftsminimering** — Bara de uppgifter som är nödvändiga för ändamålet får behandlas.
4. **Riktighet** — Uppgifter ska vara korrekta och hållas aktuella.
5. **Lagringsminimering** — Uppgifter får inte sparas längre än nödvändigt.
6. **Integritet och konfidentialitet** — Lämpliga tekniska och organisatoriska säkerhetsåtgärder krävs.
7. **Ansvarsskyldighet** — Den personuppgiftsansvarige ska kunna visa att förordningen följs.

Rättigheter för registrerade

- Rätt till tillgång (registerutdrag)
- Rätt till rättelse
- Rätt till radering ("rätten att bli glömd")
- Rätt till begränsning av behandling
- Rätt till dataportabilitet
- Rätt att invända mot behandling
- Rätt att inte bli föremål för automatiserat beslut

3. Personuppgiftsbiträdesavtal (DPA)

Ett **personuppgiftsbiträdesavtal** (Data Processing Agreement, DPA) är ett juridiskt bindande avtal som regleras av artikel 28 i GDPR. Det är obligatoriskt att ingå ett sådant avtal när en personuppgiftsansvarig anlitar ett personuppgiftsbiträde för att behandla personuppgifter för deras räkning.

Vad ett DPA-avtal ska innehålla

Enligt artikel 28.3 GDPR måste avtalet minst reglera:

- Föremålet för och varaktigheten av behandlingen
- Behandlingens art och ändamål
- Typen av personuppgifter och kategorier av registrerade
- Den personuppgiftsansvariges rättigheter och skyldigheter
- Att biträdet bara behandlar uppgifter på dokumenterade instruktioner
- Att biträdet säkerställer sekretess för personuppgifterna
- Lämpliga tekniska och organisatoriska säkerhetsåtgärder
- Villkor för anlitande av underbiträden
- Biträdets skyldighet att bistå den ansvarige med att uppfylla de registrerades rättigheter
- Radering eller återlämnande av data vid avtalets upphörande
- Rätt till revision och inspektion

> VIKTIGT ATT NOTERA
> Om ett DPA-avtal saknas vid anlitande av en extern tjänsteleverantör som behandlar personuppgifter på den ansvariges vägnar, är detta i sig ett brott mot GDPR — oavsett hur uppgifterna i övrigt hanteras. IMY kan utfärda sanktionsavgift enbart för detta.

4. Ansvarsfördelning — vem är ansvarig för vad?

GDPR definierar tydligt de olika rollerna i en behandlingskedja. Det är avgörande att förstå vilken roll varje aktör har, eftersom det styr vilka skyldigheter och vilket rättsligt ansvar som gäller.

Roll	Aktör	Definition & ansvar
Personuppgiftsansvarig	**Kunden / uppdragsgivaren**	Bestämmer ändamål och medel för behandlingen. Bär det primära juridiska ansvaret gentemot de registrerade och tillsynsmyndigheten. Ansvarar för att ingå DPA med zorc.se.
Personuppgiftsbiträde	**Zorc AB**	Behandlar personuppgifter på uppdrag av kunden, enligt dokumenterade instruktioner. Ansvarar för att ingå DPA-avtal med underleverantörer (underbiträden) och hålla kunden informerad.
Underbiträde	**Supabase, Resend, Anthropic**	Behandlar personuppgifter på zorc.se:s uppdrag. Får bara anlitas med den personuppgiftsansvariges (kundens) godkännande. Underbiträdets DPA-avtal med zorc.se gäller.

KLARLÄGGANDE OM ANSVAR

Det är **alltid kunden (uppdragsgivaren)** som är personuppgiftsansvarig för de personuppgifter som behandlas i systemet vi bygger — inte zorc.se. Zorc.se agerar biträde och kan inte ensidigt bestämma ändamålen för behandlingen. Den registrerades primära rättigheter riktas mot den personuppgiftsansvarige, d.v.s. kunden.

5. Zorc.se:s underleverantörer och GDPR-efterlevnad

I de system zorc.se bygger används ett antal externa tjänsteplattformar som kan behandla personuppgifter. Nedan beskrivs varje leverantör, deras roll och hur GDPR-efterlevnad säkerställs.

5.1 Supabase — Databasinfrastruktur

Supabase är den primära backend-plattform vi använder för databaser, autentisering och filhantering. Supabase erbjuder hosting i **EU (Stockholm, eu-north-1)**, vilket innebär att personuppgifter stannar inom Sverige och EES-området.

- Supabase Inc. har ingått **EU Standard Contractual Clauses (SCCs)** och erbjuder ett DPA.
- Data krypteras i vila (AES-256) och under transport (TLS 1.2+).
- Row Level Security (RLS) möjliggör granulär åtkomstkontroll på databasnivå.
- Zorc.se konfigurerar alltid EU-region och ingår DPA med Supabase för kundprojekt.

> ZORC.SE:S ÅTGÄRD
> Samtliga kundprojekt konfigureras med EU-datacenter (Stockholm). DPA med Supabase ingås per projekt eller via ramavtal. Kunden informeras om valet av region och underbiträde i samband med projektstart.

5.2 Resend — E-posthantering

Resend används för transaktionell e-post (t.ex. välkomstmail, lösenordsåterställning, notifieringar). E-posthantering innebär per definition behandling av personuppgifter i form av e-postadresser och innehåll.

- Resend erbjuder ett **DPA** och har implementerat EU SCCs för datatransfer.
- Resend lagrar loggdata om skickade e-postmeddelanden — dessa ska minimeras och radering konfigureras.
- Zorc.se konfigurerar retention-perioder och minimerar vilka personuppgifter som inkluderas i e-postloggar.

> ZORC.SE:S ÅTGÄRD
> DPA ingås med Resend. E-postmallar utformas för att minimera personuppgifter i e-postloggar. Retention-perioder för loggdata konfigureras till kortast möjliga tid som uppfyller tekniska krav.

5.3 Anthropic — AI-hantering

Anthropic (Claude API) används för AI-funktioner i de system vi bygger. Hantering av eventuella personuppgifter som skickas i prompts kräver särskild omsorg.

- Anthropic erbjuder ett **Data Processing Addendum (DPA)** för API-användning.
- Genom Anthropics **API-policy tränas inte modeller på kunddata** — detta skiljer sig från consumer-produkten Claude.ai.
- Zorc.se säkerställer att känsliga personuppgifter *inte* skickas i klartext i prompts — data pseudonymiseras eller anonymiseras där så är möjligt.
- Prompts och svar lagras inte av Anthropic längre än vad som krävs för säkerhetsövervakning (30 dagar per standard).

> **SÄRSKILD UPPMÄRKSAMHET VID AI-ANVÄNDNING**
> Det är **aldrig tillåtet att skicka känsliga personuppgifter** (hälsodata, personnummer, finansiell information) i klartext till ett AI-API utan en genomförd konsekvensbedömning (DPIA) och utan stöd i DPA-avtalet. Zorc.se implementerar pseudonymisering som standardåtgärd i alla AI-integrationer.

> **ZORC.SE:S ÅTGÄRD**
> DPA ingås med Anthropic via API-avtalet. Personuppgifter pseudonymiseras innan de skickas till Claude API. Kunden informeras om vilka typer av data som behandlas via AI-integrationen och ges möjlighet att godkänna eller begränsa.

6. Zorc.se:s övergripande säkerhetsåtgärder

Utöver leverantörsspecifika åtgärder tillämpar zorc.se följande rutiner i alla kundprojekt:

- **Privacy by Design och Privacy by Default** — Dataskyddsåtgärder integreras i systemarkitekturen från start, inte som ett efterhandsgrepp.
- **Minsta möjliga behörighet** — Användare och tjänstekonton ges enbart de rättigheter som krävs för deras funktion.
- **Kryptering** — All kommunikation sker via TLS. Känsliga fält i databaser krypteras på applikationsnivå.
- **Åtkomstloggning** — Åtkomst till personuppgifter loggas och kan granskas vid incident.
- **Hanteringsrutiner vid dataintrång** — Vid ett bekräftat dataintrång informerar zorc.se kunden inom 24 timmar. Kunden (personuppgiftsansvarig) är skyldig att anmäla till IMY inom 72 timmar.

- **Radering och gallring** — Systemen byggs med stöd för automatisk gallring av personuppgifter i enlighet med kundens bestämda lagringstider.
- **DPIA vid behov** — Vid ny teknik, storskalig behandling eller känsliga uppgifter genomför vi konsekvensbedömning för dataskydd (DPIA) tillsammans med kunden.

7. Risker med bristande GDPR-efterlevnad

Att inte uppfylla GDPR-lagstiftningen innebär allvarliga konsekvenser — juridiska, ekonomiska och affärsmässiga. Nedan sammanfattas de viktigaste riskerna.

Risk	Allvarlighet	Konsekvens
Sanktionsavgift från IMY	HÖG	Upp till **20 miljoner EUR** eller **4 % av global omsättning** (det högre beloppet). Tillämpas vid allvarliga överträdelser, t.ex. otillåten dataöverföring eller avsaknad av rättslig grund.
Lägre nivå sanktionsavgift	HÖG	Upp till **10 miljoner EUR eller 2 % av omsättning** för administrativa brister — t.ex. saknat DPA-avtal, bristande dokumentation eller utebliven anmälan av dataintrång.
Skadestånd till registrerade	HÖG	Enskilda registrerade kan kräva skadestånd för materiell och immateriell skada (t.ex. kränkning, stress, förlorad kontroll). Artikel 82 GDPR.
Tillsynsåtgärder från IMY	MEDEL	IMY kan utfärda förelägganden om att upphöra med behandling, kräva åtgärder inom viss tid, eller förbjuda dataöverföring till tredje land.
Reputationsskada	MEDEL	Dataintrång och GDPR-brott publiceras av IMY. Mediebevakning och förtroendeskada mot kunder och partners kan bli långvarig och svår att reparera.
Affärsmässiga konsekvenser	MEDEL	Kunder och samarbetspartners kan häva avtal vid allvarliga dataskyddsbrister. Offentlig upphandling kräver allt oftare dokumenterad GDPR-efterlevnad.

SENASTE PRAXIS I SVERIGE

IMY har på senare år ökat sin tillsynsaktivitet markant. Ingår ett bolag DPA-avtal med en underleverantör som hanterar personuppgifter utanför EES **utan adekvat skyddsåtgärd** (t.ex. SCCs), kan det leda till sanktionsavgift — oavsett om ett faktiskt intrång har skett. Avsikten spelar ingen roll; det är den faktiska behandlingen som bedöms.

8. Sammanfattning av zorc.se:s åtaganden

Zorc.se agerar alltid som **personuppgiftsbiträde** när vi bygger system som behandlar kundens personuppgifter. Vi åtar oss att:

- Ingå ett DPA-avtal med kunden (personuppgiftsansvarig) innan behandling påbörjas.
- Säkerställa att samtliga underleverantörer (Supabase, Resend, Anthropic) har godkända DPA-avtal och adekvata skyddsåtgärder på plats.
- Informera kunden om vilka underbiträden som används och ge möjlighet att invända.
- Implementera tekniska och organisatoriska skyddsåtgärder i enlighet med Privacy by Design.
- Bistå kunden vid hantering av registrerades rättigheter och vid eventuella dataintrång.
- Enbart behandla personuppgifter enligt kundens dokumenterade instruktioner.

KONTAKT FÖR DATASKYDDSFRÅGOR

Frågor om GDPR, DPA-avtal eller dataskyddshantering i era projekt kan riktas till:
support@zorc.se · 010 650 02 14