

Intern databehandler- og opbevaringspolitik

Effekten

(Effekten er binavn til **Project Execution ApS**, CVR 42075949)

Adresse: Liljevej 4, 2820 Gentofte

Web: www.effekten.dk

E-mail: support@effekten.dk

Dette dokument beskriver interne retningslinjer for behandling, opbevaring og sletning af personoplysninger hos Project Execution ApS (Effekten) i overensstemmelse med GDPR.

1. Formål

Formålet med denne politik er at sikre korrekt, lovlig og sikker behandling af personoplysninger samt dokumentation over for kunder, samarbejdspartnere og myndigheder.

2. Roller og ansvar

Project Execution ApS (Effekten) er dataansvarlig.

Direktionen er overordnet ansvarlig for GDPR-compliance.

Kun autoriserede medarbejdere har adgang til personoplysninger.

3. Databehandlere

Effekten anvender kun databehandlere, der lever op til GDPR-krav.

Der indgås skriftlige databehandleraftaler med alle relevante databehandlere.

Databehandlere må kun behandle data efter dokumenteret instruks fra Effekten.

4. Typer af systemer og data

Webshop- og ordresystemer (kunde- og ordredata).

Økonomi- og regnskabssystemer (fakturaer, betalinger).

E-mail og supportsystemer (kommunikation).

Dokumentation for installationer (fotos, rapporter).

5. Opbevaring og adgang

Personoplysninger opbevares i sikre IT-systemer med adgangskontrol.

Adgang gives kun efter arbejdsbetinget behov (need-to-know).

Fysiske dokumenter opbevares aflåst eller digitaliseres.

6. Opbevaringsperioder

Kunde- og fakturaoplysninger: minimum 5 år jf. bogføringsloven.

Installations- og servicedata: op til 5 år efter afslutning.

Support- og kommunikationsdata: op til 2 år.

Medarbejderrelaterede persondata opbevares i henhold til gældende lovgivning.

7. Sletning og anonymisering

Personoplysninger slettes eller anonymiseres, når de ikke længere er nødvendige.

Sletning sker løbende og mindst én gang årligt via intern gennemgang.

8. Datasikkerhed

Brug af stærke adgangskoder og to-faktor-login, hvor muligt.

Regelmæssig backup og opdatering af systemer.

Krypteret dataoverførsel (SSL).

9. Databrud

Mistanke om brud på persondatasikkerheden rapporteres straks til ledelsen.

Databrud vurderes og anmeldes til Datatilsynet inden 72 timer, hvis påkrævet.

10. Revision og opdatering

Denne politik gennemgås mindst én gang årligt.

Opdateringer dokumenteres og implementeres løbende.

Senest opdateret: 14.01.2026