Straume, 18.12.2025

Personvernerklæring

Personvern, behandling av personopplysninger

Denne personvernerklæringen gjelder for Grafisk Digital sine tjenester. Grafisk Digital AS, org. no. 987 083 433 (heretter kalt GD) er behandlingsansvarlig for personopplysninger som våre kunder overfører som grunnlag for dokumentbehandling og print-tjenester. Egne databehandleravtaler er inngått der det er behov for det.

Personopplysninger som behandles

GD mottar datafiler med personopplysninger fra oppdragsgivere for hvert enkelt oppdrag der GD skal generere og/eller distribuere dokumenter. Datagrunnlaget inneholder normalt bare de personopplysninger som skal inngå i de dokumenter som produseres/distribueres og eventuelt lagres i earkiv for kunden.

Eksempler på informasjon som behandles:
- Mottakernavn og postadresse
- Kundenummer, personnummer, telefonnummer og e-postadresse
- Informasjon om produkter og priser ved faktura/purring/inkasso
- Budskap i brev som kan være alt fra reklame til sensitive data unntatt offentligheten

Hvordan informasjon overføres?

GD tilrettelegger for dataoverføring ut fra våre oppdragsgiveres ønsker og forutsetninger.
GD tilrettelegger for og oppfordrer til bruk av sikker overføring av data.
Ved overføring av data fra GD benyttes sikker overføring.

Eksempel på sikker overføring av data:
- HTTPS når kunde bruker funksjonen send.no/send-fil som kan startes uten innlogging for filoverføringer til GD, og fra innlogget sesjon i SEND.no for overføring til fritt valgt mottaker.
- SFTP
- API (fra kundens egne systemer eller ved bruk av skriverdriveren SEND.no
- Krypterte filer overført på usikker tjeneste (FTP/epost)

Formålet med persondata hos GD

Alle personopplysninger som behandles er enten en del av dokumenter vi behandler, eller adresser/metadata som er knyttet til de samme dokumentene. Når GD har behandlet ferdig et dokument blir datagrunnlaget ikke brukt på nytt.

Hvordan lagres informasjonen?

Persondata mottatt i forbindelse med et kundeoppdrag lagres på nettverksdisk i GD's lokaler. Det tas normalt ikke backup av kundedatagrunnlaget. Datagrunnlaget lagres normalt i 3 måneder av hensyn til eventuelle avklaringer ved mistanke om feil/avvik knyttet til vår

produksjon eller faktureringen av denne. Informasjon som lagres for fakturering av oppdrag i ettertid inneholder ikke persondata. Ved evt avtale om dokumentarkiv hos GD gjelder egen avtale knyttet til denne tjenesten, og det tas nødvendig backup av slike data.

Hvordan slettes opplysningene?

Filer med persondata slettes automatisk etter 3 måneder om det ikke er slettet før. I enkelte tilfeller er det avtalt kortere frist for automatisk sletting. Filer i earkiv slettes etter avtalt lagringstid.

Når opphører ansvaret?

Ved utsendelse av brevpost opphører ansvaret når lukket konvolutt er hentet av postdistributør (Bring/Posten). Ved digital forsendelse opphører ansvaret når dokument/metadata er overført på avtalt måte. For earkiv opphører ansvaret når avtalt lagringstid er passert.

Utlevering av informasjon til tredjepart?

Personopplysningene deles ikke med utenforstående tredjeparter uten at dette er tydelig avtalt med oppdragsgiver eller er en naturlig del av et oppdrag. Ved eventuell bruk av underleverandør vil det bli tilbudt en databehandleravtale med underleverandør.

Overføring av adresseinformasjon til Posten, og fakturainformasjon og PDF-er til de aktører som er en naturlig del av en multikanal dokument-distribusjonsløsning regnes som en naturlig del av et distribusjonsoppdrag.

Rettigheter

Våre oppdragsgivere har rett til å kreve innsyn i hvordan vi behandler bedriftens filer/personopplysninger. Kunde kan også kreve retting, sletting og begrensninger i behandlingen av personopplysninger i henhold til personopplysningsloven.

Den enkelte person vi har personopplysninger om kan ikke henvende seg til GD vedrørende personvern, men må henvende seg til den part som eier datagrunnlaget som GD behandler.

Dersom du mener at GD ikke har overholdt sine plikter i henhold til personopplysningsloven overfor deg som kunde, har du rett til å klage til den aktuelle tilsynsmyndigheten. Dette gjøres ved å sende klage til Datatilsynet, kontaktinformasjon er tilgjengelig på www.datatilsynet.no.

GD og GDPR-etterlevelse

Databehandling og formål
GD benytter ikke persondata til andre formål enn det som er avtalt. Det forekommer ingen profilering.

Interne prosesser og systemer

- Alle interne prosesser og tjenester levert av GD er registrert, analysert og kategorisert i GDs system
- Systemer som inngår i prosesser og tjenester er analysert og dokumentert separat i henhold til GD GDPR Data Assessment Specification
- Analysen på prosess- og systemnivå utgjør GDs DPIA (Data Protection Impact Assessment)

Lagring og sikkerhet

- Data lagres i GDs interne nettverk.
- GD følger GDPR-forordningen og har implementert en systemutviklingsprosess basert på **ITIL-framework**.
- I forbindelse med implementeringen av GDPR-forordningen i mai 2024 gjennomførte GD et omfattende GDPR-prosjekt.
- Det pågår et kontinuerlig arbeid for å sikre at GD oppfyller alle lovmessige krav.

Opplæring og kompetanse

- Alle ansatte i GD gjennomfører obligatoriske e-læringskurs om GDPR og informasjonssikkerhet.
- Nyansatte får sikkerhetsopplæring ved oppstart.

Tilgang og taushetsplikt

- Interne ansatte har tilgang til personopplysninger i henhold til rolle og behov.
- Alle ansatte er underlagt taushetsplikt som oppfyller kravene til Behandlingsansvarlig.
- Taushetsplikten gjelder også etter at oppdraget er avsluttet.

Risikohåndtering

- Risikoer håndteres i henhold til interne rutiner.
- Risikovurderinger gjennomføres som en integrert del av vårt ISO/IEC 27001 baserte ISMS. Vi benytter en strukturert metode basert på prinsippene i ISO/IEC 27005 og NSMs anbefalinger for risikostyring.

Tekniske og organisatoriske tiltak

- Access Management-prosess implementert
- Access Review-prosess implementert
- Sikkerhetsopplæring for nye ansatte
- E-læring om GDPR og informasjonssikkerhet
- Kontinuerlig monitorering

Internasjonale overføringer (kapittel V GDPR)

Det ønskes å nevnes her at all distribusjon av fysiske og digitale utsendelser fra Grafisk Digital skjer fra Bergen til bedrifter i Norge og Norden. Ingen data sendes eller deles med underleverandør.

Dersom oppdraget medfører overføring av personopplysninger til tredjeland utenfor EØS, er Leverandøren pliktig å sikre at beskyttelsesnivået er tilsvarende det som gjelder innenfor EØS og dokumentere gyldig overføringsgrunnlag.

Overføring kan skje til land eller sektorer som EU-kommisjonen har vurdert som tilstrekkelige gjennom en adekvansbeslutning, jf. artikkel 45.

For overføringer til USA kan Leverandøren benytte EU–US Data Privacy Framework (DPF) når mottakeren er sertifisert under ordningen. I slike tilfeller er ytterligere mekanismer ikke nødvendig.

Leverandøren skal dokumentere mottakerens DPF-sertifisering og følge prinsippene i rammeverket.

Dersom adekvansbeslutning eller DPF ikke kan benyttes, vil Leverandøren etablere EUs standardkontrakter (SCCs) i korrekt modul og gjennomføre en Transfer Impact Assessment (TIA) med nødvendige supplerende tiltak. Slike tiltak kan omfatte ende-til-ende-kryptering, pseudonymisering og retningslinjer for håndtering av myndighetstilganger, i tråd med anbefalingene fra Det europeiske personvernrådet (EDPB).

Unntak etter artikkel 49 kan kun benyttes i særlige situasjoner, for eksempel ved uttrykkelig samtykke eller når overføringen er nødvendig for å oppfylle en avtale, og skal ikke brukes for gjentatte eller omfattende overføringer.

For alle overføringer til tredjeland skal Leverandøren dokumentere valgt overføringsgrunnlag, gjennomført TIA med vurdering av tredjelandets lovgivning og praksis, implementerte tekniske og organisatoriske tiltak, dataminimering og lagringsbegrensning, samt revisjon av underleverandørkjeden.

Leverandøren skal kontinuerlig overvåke rettsutviklingen, herunder endringer i adekvansbeslutninger, og oppdatere grunnlag og tiltak ved behov.

Kontaktinformasjon

Telefon 41 75 14 00
post@grafiskdigital.no
Grafisk Digital AS, Skjenet 11, 5354 Straume