

Databehandleravtale

Behandling av personopplysninger i Digrs tjenester

Databehandler		Behandlingsansvarlig («Kunden»)
Firma	Digr AS	Firma
Org.nr	931 148 001	Org.nr
Adresse	Tullins gate 4c, 0166 Oslo	Adresse
Kontaktperson	Jon Ragnar Steg	Kontaktperson
E-post for varsler	hei@digr.no	E-post for varsler

1 Formål og virkeområde

- 1.1 Databehandleravtalen regulerer Digrs behandling av personopplysninger på vegne av Kunden, jf. personvernforordningen (GDPR) artikkel 28 og personopplysningsloven.
- 1.2 Databehandleravtalen gjelder for all behandling Digr utfører på vegne av Kunden, uansett hvilken avtale tjenesten leveres under, herunder Digital Grunnmur, WordPress-hosting og drift, markedsføring og rådgivning («Tjenesteavtalene»). Behandlingens formål, art, kategorier av registrerte og typer personopplysninger fremgår av Bilag A, for de tjenestene Kunden til enhver tid kjøper.
- 1.3 Databehandleravtalen erstatter tidligere databehandleravtaler mellom Partene fra det tidspunkt den er signert.
- 1.4 Der Kunden har egen konto eller lisens direkte hos en tredjepartsleverandør (for eksempel Google Analytics, Google Ads eller Meta), er denne leverandøren Kundens egen databehandler eller selvstendige behandlingsansvarlige, og ikke underdatabehandler for Digr. Digrs behandling av opplysninger om Kundens kontaktpersoner for å administrere kundeforholdet skjer med Digr som behandlingsansvarlig.

2 Instrukser

- 2.1 Digr skal kun behandle personopplysninger etter Kundens dokumenterte instruks. Tjenesteavtalene, denne databehandleravtalen, oppdrag Kunden gir skriftlig og Kundens valg og konfigurasjoner i tjenestene utgjør Kundens instruks.
- 2.2 Digr skal varsle Kunden dersom Digr mener at en instruks er i strid med personvernregelverket.

3 Kundens plikter

Kunden er ansvarlig for at behandlingen har gyldig behandlingsgrunnlag, herunder samtykke der det kreves for informasjonskapsler, sporing, målgrupper og utsendelser, og for at de registrerte har fått nødvendig informasjon.

4 Konfidensialitet og sikkerhet

- 4.1 Digr skal sørge for at personer som behandler personopplysningene, er underlagt taushetsplikt, og at tilgang kun gis til personer som trenger den.
- 4.2 Digr skal gjennomføre egnede tekniske og organisatoriske tiltak etter GDPR artikkel 32. Tiltakene er beskrevet i Bilag B.

5 Underdatabehandlere

- 5.1 Kunden gir Digr generell tillatelse til å benytte underdatabehandlere. Oppdatert oversikt over underdatabehandlere, med formål, behandlingssted og overføringsgrunnlag, er tilgjengelig på Digrs nettsider, for tiden **personvern.digr.no**, sammen med en datert logg over endringer.
- 5.2 Digr skal varsle Kunden per e-post minst 14 dager før en ny underdatabehandler tas i bruk for behandling av Kundens personopplysninger. Kunden kan innen fristen motsette seg endringen på saklig, personvernrelatert grunnlag. Finner Partene ingen løsning, kan Kunden si opp de berørte tjenestene med virkning fra endringen, uten at dette gir krav på kompensasjon.
- 5.3 Digr skal inngå skriftlig avtale med hver underdatabehandler som pålegger tilsvarende personvernforpliktelser som i denne avtalen, og er ansvarlig overfor Kunden for underdatabehandlerens oppfyllelse, innenfor rammene av punkt 12.
- 5.4 Kunden kan gi skriftlig instruks om at bestemte underdatabehandlere ikke skal benyttes for Kundens personopplysninger. Digr skal etterkomme instruksjonen så langt det er praktisk mulig, innen rimelig tid. Dersom instruksjonen gjør at en tjeneste ikke kan leveres som avtalt, eller bare kan leveres med merarbeid, skal Partene avtale nødvendige endringer i leveransen. Digr er ikke ansvarlig for avvik i leveransen som skyldes instruksjonen, og Kunden dekker Digrs merarbeid etter medgått tid. Instruksjonen gir ikke rett til å si opp eller heve avtalen eller den berørte tjenesten med kortere frist eller tidligere virkning enn det som følger av Tjenesteavtalen, og fritar ikke Kunden fra å betale vederlag frem til en oppsigelse får virkning.

6 Overføring til tredjeland

Personopplysninger kan overføres til land utenfor EØS, herunder ved tilgang fra slike land, kun dersom det foreligger gyldig overføringsgrunnlag etter GDPR kapittel V, for eksempel beslutning om tilstrekkelig beskyttelsesnivå (herunder EU-US Data Privacy Framework) eller EU-kommisjonens standardkontraktsbestemmelser (beslutning 2021/914). Overføringsgrunnlaget for hver underdatabehandler fremgår av oversikten i punkt 5.1.

7 Bruk av kunstig intelligens

Digr kan benytte KI-verktøy i leveransen, forutsatt at verktøyet er en godkjent underdatabehandler etter punkt 5. Digr skal kun benytte tjenestenivåer der leverandøren ikke bruker Kundens personopplysninger til å trene sine modeller. Resultater fra KI-verktøy kvalitetssikres av Digr før de benyttes i leveransen.

8 Bistand til Kunden

Digr skal, ut fra behandlingens art og tilgjengelig informasjon, bistå Kunden med å besvare henvendelser fra de registrerte og med Kundens plikter etter GDPR artikkel 32–36. Henvendelser fra registrerte eller tilsynsmyndigheter videresendes til Kunden uten ugrunnet opphold. Bistand utover det som er rimelig og ordinært, faktureres etter medgått tid.

9 Brudd på personopplysningssikkerheten

Digr skal varsle Kunden skriftlig uten ugrunnet opphold, og senest 48 timer etter at Digr ble kjent med et brudd på personopplysningssikkerheten som berører Kundens personopplysninger. Varselet skal så langt mulig beskrive bruddets art, berørte registrerte og opplysninger, sannsynlige konsekvenser og iverksatte tiltak. Det er Kunden som avgjør om bruddet skal meldes til Datatilsynet og de registrerte.

10 Dokumentasjon og revisjon

Digr skal på forespørsel gi Kunden informasjon som er nødvendig for å vise at databehandleravtalen overholdes. Dersom slik dokumentasjon ikke er tilstrekkelig, kan Kunden, eller en uavhengig revisor underlagt taushetsplikt, gjennomføre revisjon høyst én gang per år med minst 30 dagers skriftlig varsel. Kunden dekker egne kostnader og Digrs medgåtte tid, med mindre revisjonen avdekker vesentlige brudd på denne avtalen. Revisjon fra tilsynsmyndigheter skal alltid tillates.

11 Varighet og sletting

Databehandleravtalen gjelder så lenge Digr behandler personopplysninger på vegne av Kunden. Ved opphør av en tjeneste skal Digr, etter Kundens valg, slette eller tilbakelevere personopplysningene som gjelder tjenesten innen 30 dager, med mindre lov krever lagring. Opplysninger i sikkerhetskopier slettes i takt med ordinære rutiner, og senest innen 90 dager. Digr bekrefter slettingen skriftlig på forespørsel.

12 Ansvar

- 12.1 Ansvarsbegrensningene i Tjenesteavtalene gjelder også for krav etter denne databehandleravtalen, og ansvarsgrensene er felles for krav etter Tjenesteavtalene og databehandleravtalen.
- 12.2 Dersom Tjenesteavtalen for den aktuelle tjenesten ikke har ansvarsbegrensning, gjelder følgende: Digr er kun ansvarlig for direkte tap som skyldes uaktsomhet fra Digrs side. Digr er ikke ansvarlig for indirekte tap, herunder tapt fortjeneste, tap av data, krav fra tredjeparter og overtredelsesgebyr eller andre sanksjoner ilagt Kunden. Digrs samlede

ansvar per kalenderår er begrenset til vederlaget (eksklusive merverdiavgift) Kunden har betalt for den aktuelle tjenesten i de siste 12 månedene før det første kravet oppstod.

- 12.3 Ansvarsbegrensningene gjelder ikke ved grov uaktsomhet eller forsett, og påvirker ikke de registrertes rettigheter etter GDPR artikkel 82.

13 Rangordning, lovvalg og vernetting

Ved motstrid gjelder denne databehandleravtalen foran Tjenesteavtalene i spørsmål om behandling av personopplysninger. Avtalen er underlagt norsk rett, med Oslo tingrett som avtalt vernetting.

For Digr AS

Signatur

Navn / tittel

Dato (eller tidspunkt for e-signatur)

For Kunden

Signatur

Navn / tittel

Dato (eller tidspunkt for e-signatur)

Bilag A – Behandlingens omfang

Bilaget gjelder de tjenestene Kunden til enhver tid kjøper av Digr. Formålet er i alle tilfeller at Digr skal kunne levere tjenestene til Kunden.

Tjeneste	Kategorier av registrerte	Typer personopplysninger
WordPress-hosting og drift	Kundens ansatte og andre brukere av nettsidens administrasjon; besøkende; personer som sender inn skjema	Navn, e-post, brukernavn, passord (kryptert), publisert innhold, skjemainnsendinger, IP-adresser og tekniske logger
SEO-verktøy (Yoast, Rank Math)	Brukere av nettsidens administrasjon	Brukernavn og e-post i den grad Digr har tilgang til nettsidens administrasjon
Cookie Consent	Besøkende på nettsiden	Samtykke-ID, samtykkevalg og tidspunkt, forkortet IP-adresse, nettleser- og enhetsinformasjon
Tag management, analyse og server-side tracking	Besøkende på nettsiden	IP-adresse, klient- og informasjonskapsel-ID-er, enhets- og nettleserdata, sidevisninger og hendelser; ved konverteringer eventuelt hashet e-post eller telefonnummer
Dashboard og rapportering	Kundens brukere av dashboardet	Navn og e-post for brukertilganger. Rapportdata er normalt aggregerte
Semrush	Kundens brukere med dedikert bruker	Navn og e-post. Analysedata inneholder normalt ikke personopplysninger
Leadovervåking	Besøkende på nettsiden, herunder ansatte hos besøkende virksomheter	IP-adresse, virksomhet identifisert fra IP-adresse, besøkte sider og tidspunkt; eventuelt navn, rolle og kontaktinformasjon til kontaktpersoner hos virksomheten
Markedsføring og annonsering	Kundens kunder, abonnenter og potensielle kunder	E-post og telefonnummer (normalt hashet) for målgrupper i annonseplattformer, annonseinteraksjoner og konverteringsdata
E-post og nyhetsbrev	Abonnenter og mottakere av utsendelser	Navn, e-post, samtykke til utsendelse, åpnings- og klikkdata
Rådgivning, prosjektarbeid og kommunikasjon	Personer som fremgår av materiale Kunden deler med Digr, herunder Kundens ansatte og kunder	Opplysninger i dokumenter, e-post, dataeksporter og møter, herunder opptak og transkripsjon av møter, i den grad det er nødvendig for oppdraget

Bilag B – Tekniske og organisatoriske sikkerhetstiltak

- Tilgangsstyring etter tjenstlig behov, personlige brukerkontoer og tofaktorautentisering der det støttes
- Passordhåndtering i passordhvelv; ingen deling av passord i klartekst
- Kryptering under overføring (TLS) og kryptering av lagrede data der tjenesten støtter det
- Løpende oppdatering av programvare, utvidelser og systemer som Digr drifter

- Sikkerhetskopiering av nettsider som hostes av Digr
- Taushetserklæring, databehandlertillegg og opplæring i personvern og informasjonssikkerhet for alle som behandler personopplysninger, også utenfor EØS
- Vurdering av underdatabehandlere og overføringer til tredjeland før bruk, og oversikt over verktøy og underdatabehandlere
- Rutiner for avvikshåndtering, fjerning av tilganger ved opphør og sletting av data