

Databehandleravtale (DPA)

Versjon 3.0 | Vedlegg 3 til Hovdabonnementsavtalen

Vedlegg 3 – Databehandleravtale

Version 3.0

1. Bakgrunn

1.1 Denne databehandleravtalen (DPA) regulerer Simpløyers behandling av personopplysninger som databehandler på vegne av Kunden som behandlingsansvarlig.

1.2 Når et begrep som brukes i denne DPA er definert i GDPR art. 4, skal begrepet ha den betydningen som er tilskrevet det i GDPR art. 4.

2. Formål

2.1 Formålet med behandlingen av personopplysninger i henhold til denne Avtalen er å levere Abonnementstjenestene til Kunden og gjøre det mulig for Kunden å utføre handlinger knyttet til HR-ledelse og administrasjon.

2.2 Kategoriene av registrerte og typer personopplysninger som behandles gjennom Abonnementstjenestene, kan variere avhengig av de spesifikke modulene som Kunden har anskaffet, som angitt i Bestillings skjemaet. Relevant informasjon finnes på Simpløyers Trust Center (Underdatabehandlere som brukes av Simpløyer).

3. Partenes forpliktelser

3.1 Simpløyers forpliktelser

3.1.1 Simpløyer skal behandle personopplysninger i henhold til de avtalte spesifiserte formålene i henhold til denne DPA. Simpløyer skal ikke behandle personopplysninger utover det som er nødvendig for de formål som er angitt i denne DPA uten forutgående skriftlig avtale med eller skriftlige instruksjoner fra Kunden.

3.1.2 Simpløyer skal, i den grad det er påkrevd i henhold til GDPR, bistå Kunden med å:

- gi Kunden informasjon som er nødvendig for å påvise at forpliktelsene i GDPR art. 28 (3) er oppfylt.
- i rimelig utstrekning bistå Kunden med å oppfylle Kundens forpliktelse til å svare på forespørsler fra den registrerte med det formål å utøve sine rettigheter som er fastsatt i GDPR kap. III.
- i rimelig utstrekning bistå Kunden med å oppfylle Kundens forpliktelser i henhold til GDPR art. 32-36, inkludert håndtering av avvik.
- Simpløyer skal varsle Kunden dersom Simpløyer mener at en instruksjon fra Kunden er i strid med gjeldende personvernbestemmelser.

3.1.3 All bistand skal utføres som Rådgivningstjenester, og i den utstrekning det er rimelig ut fra Kundens behov, behandlingens art og informasjonen Simpløyer har tilgang til. All bistand og arbeid i samsvar med nye og avtalte instruksjoner fra Kunden kan faktureres Kunden i henhold til Simpløyers til enhver tid gjeldende listepreiser, eller de priser som er avtalt i Bestillings skjemaet, med mindre annet er uttrykkelig angitt i denne DPA eller begrenset av Lov.

3.1.4 Simpløyer er underlagt taushetsplikt med hensyn til dokumentasjon og personopplysninger som Simpløyer har tilgang til i henhold til denne DPA. Denne bestemmelsen gjelder også etter opphør av DPA.

3.1.5 Simpløyer skal ikke utlevere personopplysninger til tredjeparter med mindre annet følger av denne DPA, er avtalt skriftlig, eller slik utlevering er påkrevd ved Lov. Personopplysninger som behandles av Simpløyer på vegne av Kunden, kan overføres til land hvor Simpløyer, dets underdatabehandlere eller underdatabehandlernes underdatabehandlere, driver sin virksomhet i henhold til bestemmelsene om bruk av underdatabehandlere i punkt 4.

3.1.6 Simpløyer er ansvarlig for å sikre at dataene lagres på en forsvarlig måte og senere slettes eller anonymiseres i samsvar med denne DPA.

3.2 Kundens forpliktelser

3.2.1 Kunden er forpliktet til å overholde kravene til behandlingsansvarlige i henhold til relevant nasjonal lovgivning som gjennomfører GDPR, inkludert underliggende forskrifter, og GDPR.

3.2.2 Kunden bekrefter at:

- Det foreligger tilstrekkelig rettslig grunnlag for behandling av personopplysninger;
- Kunden er ansvarlig for lovligheten av overføringen av personopplysninger til Simpløyer;
- Kunden er ansvarlig for nøyaktigheten, integriteten, innholdet, påliteligheten og lovligheten av personopplysningene som behandles;
- Kunden har informert de registrerte i samsvar med gjeldende lovkrav;
- Denne databehandleravtalen inneholder alle instruksjoner fra Kunden på tidspunktet for signering av Avtalen.

3.2.3 Kunden skal sikre at personopplysninger behandles i samsvar med GDPR, svare på henvendelser fra de registrerte og sørge for at det iverksettes tilstrekkelige tekniske og organisatoriske tiltak for å sikre personopplysningene som behandles, i samsvar med GDPR artikkel 32.

3.2.4 Kunden er forpliktet til å rapportere sikkerhetsbrudd til relevante tilsynsmyndigheter og, hvis aktuelt, til den registrerte uten unødig forsinkelse i samsvar med gjeldende lovgivning.

3.2.5 Kunden er ansvarlig for å sikre at tilpassede datafelt i seg selv eller gjennom sitt innhold ikke bryter med gjeldende lover og forskrifter, herunder om personopplysninger. Det samme gjelder bruk av kombinasjoner av datafelt, for eksempel i rapporter mv.

3.2.6 Hvis Kunden har til hensikt å bruke tjenesten også for ansatte i andre selskaper enn sitt eget, skal Kunden selv innhente selskapenes tillatelse til å behandle personopplysninger om de berørte ansatte. For selskaper og ansatte som er bosatt utenfor EU/EØS, skal Kunden selv overvåke og være ansvarlig for at lovkravene i henhold til gjeldende utenlandsk lovgivning overholdes.

4. Bruk av underdatabehandlere

4.1 Simpløyer bruker underdatabehandlere til å oppfylle deler av sine ulike forpliktelser, herunder hosting av tjenestene. Simpløyer er ansvarlig for underdatabehandlerens utførelse på samme måte som om Simpløyer selv sto for utførelsen.

4.2 Simpløyer er forpliktet til å inngå separate databehandleravtaler med alle sine underleverandører for å sikre oppfyllelse av vilkårene i denne DPA og GDPR art. 28.

4.3 Underdatabehandlere som er relevante for modulen som Kunden har anskaffet, som spesifisert i Bestillingskjemaet, er oppført på Simpløyers Trust Center. Lenken vil holdes oppdatert for å gjenspeile eventuelle endringer i underdatabehandlerens engasjement.

4.4 Kunden skal varsles om endringer eller tillegg av nye underdatabehandlere minst tretti (30) kalenderdager før endringen trer i kraft eller den nye underdatabehandleren får tilgang til personopplysninger. Kunden må protestere skriftlig mot endringen innen tretti (30) kalenderdager. Med mindre Kunden protesterer skriftlig innen fristen, kan Databehandleren bruke den nye underdatabehandleren til de angitte behandlingsaktivitetene. Dersom Kunden protesterer i god tro innen den angitte fristen, vil Simpløyer gjøre rimelige anstrengelser for å endre Abonnementstjenestene for å unngå at underdatabehandleren det protesteres mot behandler Kundens personopplysninger. Hvis Simpløyer ikke er i stand til å gjennomføre slike endringer innen rimelig tid, som ikke skal overstige tretti (30) dager fra mottak av Kundens skriftlige innsigelse, har Kunden rett til å si opp de relevante delene av Abonnementstjenestene.

4.5 Overføring av personopplysninger til underdatabehandlere i land utenfor EU/EØS som ikke er anerkjent av EU-kommisjonen som land som gir et tilstrekkelig nivå av beskyttelse av personopplysninger, skal kun skje i henhold til gyldige mekanismer for slike overføringer, for eksempel EUs standardklausuler for overføring av personopplysninger til tredjeland eller andre gjeldende grunnlag for overføring til tredjeland i samsvar med GDPR kapittel 5.

5. Informasjonssikkerhet

5.1 Simpløyer skal gjennom egnede planlagte, systematiske, organisatoriske og tekniske tiltak sikre tilstrekkelig informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet i forbindelse med behandling av personopplysninger i henhold til GDPR artikkel 32.

5.2 Simpløyer skal kunne dokumentere sikkerhetstiltakene. Dokumentasjonen må gjøres tilgjengelig på forespørsel fra Kunden.

5.3 Simpløyer skal sikre tilfredsstillende personopplysningssikkerhet med hensyn til:

- konfidensialitet, dvs. at opplysningene ikke er tilgjengelige for personer som ikke har lovlig tilgang til opplysningene,
- integritet, dvs. at dataene ikke endres på en uautorisert eller utilsiktet måte, og
- tilgjengelighet, dvs. at dataene er tilgjengelige og operative for legitim og autorisert bruk.

5.4 Simpløyer skal ha rutiner og systematiske prosesser for å følge opp brudd på personopplysningssikkerheten («Avvik»). Hvis Avviket er forårsaket av Kunden eller forhold som ligger innenfor Kundens kontroll, kan Simpløyer fakturere Kunden for arbeid knyttet til oppfølging av Avviket som Rådgivningstjenester i samsvar med Simpløyers gjeldende listepriiser eller de priser som er avtalt i Bestillingsskjemaet.

5.5 Simpløyer skal uten ugrunnet opphold varsle Kunden om Avviket.

5.6 Simpløyer skal gi Kunden slik informasjon som er nødvendig for at Kunden skal kunne overholde gjeldende Lov om behandling av personopplysninger og for at Kunden skal kunne svare på forespørsler fra tilsynsmyndigheten ved Avvik. Det er Kundens ansvar å rapportere Avvik til relevant tilsynsmyndighet i samsvar med gjeldende Lov.

6. Sikkerhetsrevisjoner

6.1 Kunden erkjenner at Kundens rett til å gjennomføre revisjoner i henhold til GDPR er oppfylt ved at Simpløyer sørger for at en uavhengig tredjepart, utpekt av Simpløyer, regelmessig gjennomfører en revisjon av Abonnementstjenestene. Resultatene av revisjonen gjøres tilgjengelig for Kunden på forespørsel.

7. Varighet av DPA

7.1 Denne DPA gjelder fra den dato det aktuelle Bestillingsskjemaet er signert av begge parter og frem til Avtalen utløper eller frem til Simpløyers forpliktelse til å utføre Abonnementstjenestene opphører av en eller annen grunn, med unntak av bestemmelsene i Avtalen som fortsetter å løpe etter opphør.

8. Ved opphør

8.1 Etter utløpet av Avtalen er Simpløyer forpliktet til å anonymisere alle personopplysninger som omfattes av denne DPA, og deretter slette alle personopplysninger som Kunden er behandlingsansvarlig for. På forespørsel skal Simpløyer gi Kunden en skriftlig erklæring, hvorefter Simpløyer garanterer at alle personopplysninger eller data nevnt ovenfor er anonymisert og at Simpløyer ikke har beholdt noen kopi, utskrift eller lagret personopplysninger på noe annet medium.

8.2 Kunden kan få tilgang til sine personopplysninger ved oppsigelse av Avtalen i henhold til Vilklårene.

9. Varslinger

9.1 Varslinger i henhold til denne DPA skal sendes skriftlig til Kundens kontaktperson som angitt i Bestillingsskjemaet.

Vedlegg A – Insights / integrasjonsgrensesnitt («API»)

Vedlegg A gjelder kun hvis Kunden har kjøpt tilgang til Insights (et integrasjonsgrensesnitt), heretter omtalt som «API». Simpløyer API-er eksponerer integrasjonsgrensesnitt som utvalgte brukere hos Kunden kan få tilgang til, noe som gjør det mulig for Kunden å overføre informasjon, inkludert personopplysninger, fra Kundens data generert i Simpløyer, for videre behandling og analyse i tredjepartsprogramvare.

API-en er beskyttet av en API-nøkkel som brukes til å autentisere den eller de enkelte tjenestene som skal samhandle med grensesnittet. Kunden får utlevert denne nøkkelen og er selv ansvarlig for å bruke den og kun autentisere de systemene, og de brukerne, som skal ha tilgang til tjenesten.

Simpløyer er ansvarlig for tilgjengeligheten og konfidensialiteten av data frem til endepunktene. Etter at data har forlatt endepunktet, er det Kunden som er ansvarlig for all bruk av tjenesten og all bruk av data som er gjort tilgjengelig via endepunktet.

Vedlegg B – Oppdragsmodulen

Vedlegg B gjelder kun dersom Kunden har kjøpt oppdragsmodulen. Når det gjelder utlevering av data fra denne modulen, kan Simpløyer ikke utlevere svarinformasjon til Kunden på annen måte enn i anonymisert og aidentifisert form. Svarinformasjon betyr svarene ansatte har gitt på medarbeiderundersøkelser som er samlet inn ved hjelp av oppdragsmodulen.

Kunden er også ansvarlig for å sikre at deres bruk av, og innholdet i spørsmålene og svarene som er lagret i oppdragsmodulen. Kunden bør unngå å stille spørsmål som involverer eller resulterer i svarinformasjon som inneholder personopplysninger de ikke trenger eller har juridisk grunnlag for å behandle.

Vedlegg C – Varslingsmodulen

Vedlegg C gjelder kun hvis Kunden har kjøpt varslingsmodulen og aktivert den for bruk.

I tråd med EU-direktiv 2019/1937 om varsling tilbyr Simpløyer en digital tjeneste for å legge til rette for og støtte varslingsprosessen.

Kunden er ansvarlig for å sikre at meldingene behandles og lagres i samsvar med gjeldende regelverk, dvs. både nasjonale varslingsregler og reglene i GDPR. Systemet sletter automatisk data i meldinger to år etter at de ble opprettet.