NORKART

Databehandleravtale

mellom

Firmanavn
som databehandlingsansvarlig
Org: NO 123456789

og

Norkart AS
som databehandler
Org: NO 934 161 181

1. Bakgrunn og formål

1.1 Partene har inngått en eller flere avtaler ("**Hovedavtalen**") hvor Norkart AS ("**Databehandleren**") behandler personopplysninger på vegne av **Firmanavn** (den "**Behandlingsansvarlige**").

1.2 Denne databehandleravtalen ("**Databehandleravtalen**") regulerer rettighetene og forpliktelsene knyttet til behandlingen av personopplysninger som gjøres i forbindelse med Hovedavtalen. Den har rang foran tidligere avtaler og bestemmelser partene imellom hva gjelder behandling av personopplysninger.

1.3 I tilfelle uoverensstemmelse mellom Hovedavtalen og Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal Databehandleravtalen gis forrang.

2. Definisjoner

2.1 "**Personvernlovgivning**": De til enhver tid gjeldende lover og regler om behandling av personopplysninger, inkludert personopplysningsloven (med henvisning til GDPR fra 25 Mai 2018).

2.2 "**Standardklausuler**": Standardklausuler for overføring av personopplysninger til databehandlere etablert i tredjeland, etablert ved EU-kommisjonens vedtak av 5. februar 2010 og/eller som etablert av EU-kommisjonen for en relevant tilsynsautoritet i henhold til GDPR artikkel 28(7) eller 28(8).

2.3 "**GDPR**": EUs personvernforordning 2016/679.

2.4 For øvrig skal ord og uttrykk ha samme mening som de er tillagt i gjeldende Personvernlovgivning.

2.5 **Omfang**

2.6 Denne Databehandleravtalen regulerer behandling av personopplysninger som finner sted på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen, inkludert (i) personopplysninger overført fra den Behandlingsansvarlige til Databehandler, (ii) personopplysninger som Databehandleren gis tilgang til gjennom den Behandlingsansvarlige, og (iii) personopplysninger som genereres i forbindelse med Databehandlerens utførelse av sine forpliktelser under Hovedavtalen.

2.7 Nærmere informasjon om databehandlingen, herunder behandlingens formål/art og hvilke personopplysninger/registrerte som inngår ("Behandlingsoversikt), fremgår av den Behandlingsansvarliges innloggingsside på Kundesenteret. Behandlingsoversikten angis pr produkt/tjeneste og den Behandlingsansvarlige vil basert på egen oversikt over hvilke tjenester som benyttes kunne identifisere hva slags personopplysninger Databehandleren behandler på den Behandlingsansvarliges vegne.

2.8 Dersom Behandlingsoversikten endres som følge av endringer som Databehandleren initierer, f.eks. i form av endringer i produkt/tjeneste, vil den Behandlingsansvarlige varsles skriftlig uten ugrunnet opphold. Dersom den Behandlingsansvarlige motsetter seg endringen hva gjelder behandling av personopplysninger, og partene ikke finner en løsning, kan den Behandlingsansvarlige si opp relevant produkt/tjeneste med én måneds skriftlig varsel.

3. Alminnelige forpliktelser

3.1 Databehandleren garanterer at den vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysninger oppfyller kravene i Personvernlovgivningen og ivaretar de registrertes rettigheter. Databehandleren skal kun behandle personopplysninger i henhold til dokumenterte instruksjoner fra den Behandlingsansvarlige.

3.2 Dersom Databehandleren er forpliktet under en godkjent adferdsnorm som vist til i GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i GDPR artikkel 42, vil Databehandlerens overholdelse av slik adferdsnorm være tilstrekkelig for å påvise tilstrekkelige garantier som nevnt i punkt 3.1.

4. Bistand til den behandlingsansvarlige

4.1 Databehandleren skal på forespørsel bistå den Behandlingsansvarlige, gjennom egnede tekniske og organisatoriske tiltak, med å oppfylle den Behandlingsansvarliges plikt til å besvare forespørsler fra de registrerte i henhold til GDPR kapittel III.

4.2 Databehandleren skal på forespørsel bistå den Behandlingsansvarlige med å sikre overholdelse av GDPR artikkel 32 – 36, tatt i betraktning behandlingens art og informasjonen som er tilgjengelig for Databehandleren.

4.3 Bistand som nevnt i dette punkt 4.1 og 4.2 vil ytes på de timepriser som er avtalt mellom partene, eller, dersom det ikke er avtalt, på Databehandlerens gjeldende timepriser.

5. Tekniske og organisatoriske sikkerhetstiltak

5.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen. Tiltakene skal ha til formål å verne personopplysningene mot tilfeldig eller ulovlig sletting eller tilfeldig tap, endringer eller uautorisert overføring eller tilgang. Databehandleren garanterer imidlertid ikke at sikkerhetsbrudd eller øvrige brudd på personopplysningssikkerheten kan forekomme.

5.2 Databehandleren har angitt sine sikkerhetstiltak i Vedlegg 1. Disse anses generelt egnet for å oppfylle det nødvendige sikkerhetsnivået som nevnt i punkt 5.1.

5.3 Databehandleren skal påse at kun relevant personell har tilgang til personopplysninger og at disse er underlagt avtalefestet eller lovfestet taushetsplikt.

6. Bruk av underleverandører

6.1 Databehandleren kan engasjere andre databehandlere (underdatabehandlere) til å utføre oppgaver under denne Databehandleravtalen. Dette skal i så fall skje gjennom avtaler som pålegger tilsvarende forpliktelser som i denne Databehandleravtalen og som gir tilstrekkelige garantier for at det blir gjennomført tekniske og organisatoriske tiltak hos underdatabehandleren for å ivareta Personvernlovgivningen. Databehandleren har fullt ansvar overfor den Behandlingsansvarlige for at underdatabehandleren oppfyller sine forpliktelser.

6.2 Den Behandlingsansvarlige kan på forespørsel få en oversikt over underdatabehandlerne. På forespørsel kan den Behandlingsansvarlige også kreve fremlagt databehandleravtaler med underdatabehandlerne (forretningsmessig og annet sensitivt materiale kan dog skjules).

6.3 Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte nye underdatabehandlere eller om å skifte ut underdatabehandlere og dermed gi den Behandlingsansvarlige muligheten til å motsette seg slike endringer. Den Behandlingsansvarlige kan ikke motsette seg endringen uten saklig grunn og denne grunnen veier tyngre enn Databehandlerens interesse i å gjøre endringen.

7. International Dataoverføring

7.1 Databehandleren kan kun overføre personopplysninger utenfor EU/EØS etter dokumenterte instruksjoner fra den Behandlingsansvarlige.

7.2 Ved slik eventuell instruksjon har Databehandleren fullmakt, på vegne av den Behandlingsansvarlige, til å inngå en databehandleravtale med underdatabehandleren som inneholder EUs standardklausuler i uendret form, dersom dette er nødvendig for å gjøre overføringen lovlig.

8. Brudd på personopplysningssikkerheten

8.1 Databehandleren skal skriftlig underrette den Behandlingsansvarlige om eventuelle brudd på personopplysningssikkerheten. Varselet skal gis senest 48 timer etter at Databehandleren ble oppmerksom på bruddet.

8.2 Den Behandlingsansvarlige har, der det er relevant, ansvaret for å varsle den relevante tilsynsmyndighet og de registrerte om brudd på personvernopplysningssikkerheten.

9. Revisjon

9.1 Databehandleren skal foreta jevnlige revisjoner av sin behandling av personopplysninger. Databehandleren skal dokumentere og på forespørsel gjøre tilgjengelig for den Behandlingsansvarlige informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og Personvernlovgivningen.

9.2 På forespørsel kan den Behandlingsansvarlige få oversendt eventuelle revisjonsrapporter om personvern utarbeidet av tredjepart på vegne av Databehandleren. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter for sine eksterne revisorer og for tilsynsmyndigheter.

9.3 På forespørsel har den Behandlingsansvarlige, gjennom revisor eller lignende tredjepart som er underlagt konfidensialitet, rett til å gjøre revisjoner av Databehandleren. Forespørselen skal gis med minst 14 dagers varsel. Revisjoner kan ikke gjøres mer enn én gang pr år, med mindre det er påkrevd etter Personvernlovgivningen.

9.4 Revisjoner kan først og fremst innebære gjennomgang av dokumentasjon, rutiner, systemer og relevante tekniske og organisatoriske sikkerhetstiltak. Den Behandlingsansvarlige skal gjøre sitt ytterste for å gjennomføre revisjoner uten at

dette er til hinder for Databehandlerens virksomhet. Den Behandlingsansvarlige skal videre påse at personell som utfører revisjoner er underlagt taushetsplikt.

9.5 Dersom en revisjon avdekker brudd på denne Databehandleravtalen eller Personvernlovgivningen, skal Databehandleren rette slike brudd innen rimelig tid.

9.6 Hver av partene dekker i utgangspunktet sine egne kostnader forbundet med revisjon. Den Behandlingsansvarlige skal også dekke Databehandlerens nødvendige kostnader for revisjoner den Behandlingsansvarlige har initiert (hvor arbeid for Databehandleren dekkes i samsvar med de timepriser som er avtalt mellom partene, eller, dersom det ikke er avtalt, i samsvar med Databehandlerens gjeldende timepriser).

9.7 Databehandleren skal varsle den Behandlingsansvarlige dersom tilsynsmyndighet krever tilgang til eller informasjon om behandlingen av personopplysninger i henhold til denne Databehandleravtalen, med mindre dette er forbudt ved lov eller myndighetspålegg.

10. Ansvarsbegrensning

10.1 Med mindre annet er avtalt i Hovedavtalen, skal Databehandleren være ansvarlig for den Behandlingsansvarliges direkte tap ved Databehandlerens eventuelle mislighold av denne Databehandleravtalen. Indirekte tap dekkes ikke. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste av enhver art, tapte besparelser og krav fra tredjeparter. Erstatningsansvaret i løpet av ett år er oppad begrenset til beløpet betalt av den Behandlingsansvarlige til Databehandleren under Hovedavtalen det året. Ansvarsbegrensningen gjelder ikke der det er utvist grov uaktsomhet eller forsett.

11. Varighet og oppsigelse

11.1 Denne Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen.

11.2 Ved Databehandleravtalens opphør skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, returnere alle personopplysninger og alle kopier til den Behandlingsansvarlige eller slette alle personopplysningene og bekrefte overfor den Behandlingsansvarlige at det er gjort, med mindre Databehandleren er forhindret ved lov fra å gjøre det. Dersom det er tilfelle, skal Databehandleren besørge sikker lagring av personopplysningene, men ikke lenger aktivt behandle dem.

11.3 Oppsigelse av denne Databehandleravtalen skal ikke hindre Databehandleren fra å fortsette å behandle anonymiserte opplysninger for analytiske, statistiske og andre formål.

Undertegning

Denne avtale er undertegnet i 2 – to eksemplarer, hvorav partene har hvert sitt.

Behandlingsansvarlig For Virksomheten: **Firmanavn**	**Databehandler** For Leverandøren: **Norkart AS**
Dato, sted og underskrift 20. april 2018	**Dato, sted og underskrift** **Sandvika,**  20. april 2018
Navn og stilling ,	**Navn og stilling** Pål Normann Johansen, Markedsdirektør

VEDLEGG 1: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Databehandleren skal oppfylle følgende minimumskrav for tekniske og organisatoriske sikkerhetstiltak:

Eksempler på sikkerhetstiltak som kan beskrives (se GDPR art. 32):

1. Pseudonymisering og kryptering av personopplysninger.

2. Hvordan databehandler sikrer fortrolighet, konfidensialitet, integritet, tilgjengelighet og robustheten i systemene og tjenestene som benyttes til behandling av personopplysninger.

3. Hvordan databehandler sikrer at tilgjengelighet og tilgang til personopplysninger kan gjenopprettes innen rimelig tid dersom det skjer en teknisk eller fysisk hendelse innen rimelig tid.

4. Hvordan databehandler sikrer jevnlig testing, vurdering og evaluering av effektiviteten av de tekniske og organisatoriske virkemidlene som benyttes for å sikre informasjonssikkerhet.