DATABEHANDLERAVTALE

Denne databehandleravtalen er inngått mellom:

(1) Kunden, (heretter kalt "**Behandlingsansvarlig**") og

(2) NG Secure AS, (heretter kalt "**Databehandler**")

(Behandlingsansvarlig og Databehandler er i fellesskap omtalt som «**Partene»**)

1. Bakgrunn og formål

Behandlingsansvarlig og Databehandler har inngått denne databehandleravtalen, ("**Databehandleravtalen**"), for å sikre at enhver behandling av Personopplysninger som finner sted som en nødvendig del av Partenes avtale om NG Secures tjenester ("**Avtalen**") skjer i henhold til enhver tid gjeldende personvernforordning (GDPR) og personopplysningsloven "**Personvernregelverk**").

Formålet med behandlingen er leveranse av tjenester knyttet til makulering og destruksjon i henhold til Avtalen.

Denne Databehandleravtalen fastsetter den Behandlingsansvarlige og Databehandlerens rettigheter og plikter når Databehandleren utfører Behandling av Personopplysninger på vegne av den Behandlingsansvarlige i tilknytning til Avtalen, herunder skal Databehandleravtalen sikre at Personopplysninger ikke brukes urettmessig eller kommer uberettigede i hende.

2. Definisjoner

«**Behandlingsansvarlig**», «**Databehandle**r», «**Personopplysning**», «**Registrerte**» og «**Behandling**» skal forstås i henhold til de definisjoner som følger av personvernforordningen artikkel 4.

Med «**Underdatabehandler**» menes i denne Databehandleravtalen den som Behandler Personopplysninger på vegne av Databehandler. Behandlingen skal skje innenfor de rammene som gjelder for Databehandler selv og etter det som følger av skriftlig databehandleravtale med Databehandler. Databehandler kan bli ansvarlig dersom denne Behandlingen av Personopplysninger ikke skjer i tråd med det avtalte eller i samsvar med gjeldende Personvernregelverket.

3. Vedlegg

Som «**Vedlegg 1»** til denne Databehandleravtalen følger den Behandlingsansvarliges instruks for Databehandlerens behandling av Personopplysninger, en beskrivelse av de sikkerhetstiltak som Databehandleren som et minimum skal gjennomføre og informasjon om hvordan revisjoner av Databehandleren og eventuelle Underdatabehandlere skal utføres.

4. Behandlinger og overordnet ansvar

Databehandler kan kun behandle Personopplysninger som er nødvendig for å oppfylle formålet med Avtalen mellom Partene og innenfor de rammene Behandlingsansvarlig fastsetter.

Behandlingsansvarlig har både en rett og en plikt til å bestemme hvilket formål og hvilke hjelpemidler som skal brukes for Behandlingen.

Personopplysningene skal ikke lagres lengre enn nødvendig for å oppfylle formålet. Databehandler har ikke råderett over Personopplysningene, og kan dermed ikke Behandle disse til egne formål, heller ikke dersom opplysningene anonymiseres.

Dersom Databehandler ved lov, eller i medhold av lov, er pålagt å behandle Personopplysninger på andre måter enn etter Behandlingsansvarliges instruksjon, må Databehandler varsle Behandlingsansvarlig før Behandlingen finner sted.

5. Type behandling av Personopplysninger

Databehandler vil utføre makulerings og/eller destruksjonstjenester av dokumenter, digitale lagringsmedier eller varer og produkter i henhold til Avtalen. I forbindelse med den inngåtte Avtalen vil Databehandler motta og midlertidig oppbevare dokumenter, digitale medier, eller varer og produkter som vil kunne inneholde Personopplysninger. Dokumenter, digitale medier eller varer og produkter som inneholder Personopplysninger vil videre makuleres eller destrueres.

Databehandler vil ikke på noen måte lese, aksessere eller på annen måte behandle informasjon som er lagret på overlevert materiale eller i dokumenter fra Behandlingsansvarlig utover det som er nevnt ovenfor.

6. De Registrerte

Databehandler har ingen kjennskap til hvilke kategorier av Registrerte og type Personopplysninger som vil kunne være lagret på digitale medier, dokumenter eller varer og produkter behandlet under Avtalen og denne Databehandleravtalen. Behandlingsansvarlig er selv ansvarlig for å ivareta en slik oversikt.

7. Hvor lagres/prosesseres personopplysningene

Databehandler skal som det klare utgangspunkt levere tjenesten innenfor EU/EØS. Dette betyr at all Behandling av Personopplysninger skal utføres innenfor EU/EØS.

Dette betyr videre at all aktivitet som krever tilgang til Personopplysninger, samt all aktivitet fra Underdatabehandlere skal ytes fra lokasjoner innenfor EU/EØS.

Databehandler kan ikke overføre Personopplysninger til USA eller et annet tredjeland (utenfor EU/EØS) uten skriftlig forhåndssamtykke fra Behandlingsansvarlig. Ved behov for slikt samtykke skal Databehandler henvende seg til Behandlingsansvarlig for å få innhentet forhåndssamtykke. Slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.

Databehandler forplikter seg til å gi skriftlig varsel til Behandlingsansvarlig minst 3 måneder før det gjøres endringer i forhold til behandling av Personopplysninger utenfor EU/EØS. Varselet skal skje via e-post eller post til Behandlingsansvarlig sin kontaktperson.

8. Behandlingsansvarliges rolle og ansvar

Behandlingsansvarlig er, foruten det som ellers fremgår av denne Databehandleravtalen, ansvarlig for at det foreligger et lovlig hjemmelsgrunnlag for Behandlingen av Personopplysninger, og at den aktuelle Behandling er i overensstemmelse med gjeldende personvernregelverk, herunder nasjonale lover og regelverk som Behandlingsansvarlig er underlagt. Behandlingsansvarlig er også ansvarlig for riktigheten av Personopplysningene og at den Registrerte er informert om Behandlingen i tråd med gjeldende personvernregelverk, herunder nasjonale lover og regelverk som Behandling ansvarlig er underlagt.

9. Databehandlers plikter

Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig.

Databehandler forplikter seg til å behandle Personopplysninger for Behandlingsansvarlig i samsvar med det til enhver tid gjeldende Personvernregelverk, denne Databehandleravtalen med vedlegg og eventuelle senere skriftlige avtaler mellom Partene.

Behandlingsansvarlig skal gi nødvendige og tilstrekkelige instrukser til Databehandler for å sikre at Behandlingen av Personopplysninger skjer i samsvar med formålet og med gjeldende personvernlovgivning. Databehandler skal følge de rutiner og instrukser for Behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde, herunder rutiner om sletting.

Databehandler forplikter seg til kun å behandle Personopplysninger innenfor rammene av Avtalen og i samsvar med de instrukser de mottar fra Behandlingsansvarlig. Databehandleren skal straks underrette Behandlingsansvarlig dersom Databehandleren mener at en instruks gitt av Behandlingsansvarlig er i strid med gjeldende Personvernregelverk.

Databehandler plikter å samarbeide med Behandlingsansvarlig og tilsynsmyndighetene ved kontroll. Ved et eventuelt stedlig tilsyn fra Datatilsynet er Databehandler pliktig til å samarbeide med/bistå Behandlingsansvarlig med å fremskaffe opplysninger som tilsynsmyndighetene mener er nødvendig og har hjemmel til å kreve fremlagt.

Databehandler skal ikke Behandle Personopplysninger eller øvrig data på eget initiativ eller for andre formål enn hva som frem går av Avtalen og denne Databehandleravtalen. Databehandler skal ikke ved noen handling eller unnlatelse sette Behandlingsansvarlig i en slik situasjon at Behandlingsansvarlig bryter noen bestemmelse i eller i medhold av personvernlovgivningen.

Databehandler garanterer å ha tilstrekkelig kunnskap, pålitelighet og ressurser for å gjennomføre databehandlingen på en sikker måte.

(i) Taushetsplikt

Databehandler, herunder Databehandlers ansatte, forplikter seg til å behandle alle Personopplysninger som Databehandler vil kunne få tilgang til i henhold til denne Databehandleravtalen. Databehandler, herunder Databehandlers ansatte, skal sørge for at materialet som kan inneholde Personopplysninger ikke deles eller på annen måte gjøres tilgjengelig for uvedkommende, med mindre det er påkrevd av lov eller krav av myndigheter eller nødvendig for å oppfylle Avtalen og ellers i tråd med Avtalen og denne Databehandleravtalen, for eksempel i tilknytning bruk av forhåndsgodkjente Underleverandører.

Denne bestemmelsen gjelder også etter Avtalens og Databehandleravtalens opphør. Nødvendige konfidensialitetsavtaler skal inngås hvis de ansatte ikke har lovpålagt taushetsplikt. Taushetsplikten omfatter også ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer som Databehandleren anvender for å levere tjenesten.

(ii) Oversikt over tilgangsrettigheter og behandlingsaktiviteten

Kun ansatte hos Databehandler og underdatabehandlere som har tjenstlig behov for utførelse av makulering eller destruksjonstjenester, kan gis slik tilgang til materiale i de plomberte beholdere. Databehandleren plikter å dokumentere sine rutiner og retningslinjer for tilgangsstyring, og gi Behandlingsansvarlig tilgang til slik dokumentasjon på forespørsel. Databehandler plikter å loggføre all autorisert og uautorisert bruk, samt forsøk på uautorisert bruk av egne hovedsystemer. Loggene skal oppbevares av Databehandleren i minimum 3 måneder. Behandlingsansvarlig skal på forespørsel gis tilgang til loggene.

(iii) Innsyn, retting og sletting

Databehandler har ingen mulighet til å gi innsyn i eller retting av Personopplysninger på medier, dokumenter eller annet materiale overlevert til Databehandler under Avtalen. Ved skriftlig forespørsel fra Behandlingsansvarlig vil Databehandler tilbakelevere plomberte beholdere eller oppsamlingsenheter med medier eller dokumenter til Behandlingsansvarlig, forutsatt at destruksjons- eller makuleringsprosessen ikke allerede er påbegynt og materialet er fortsatt i en tilstand som muliggjør tilbakelevering.

(iv) Dataportabilitet

Databehandler utfører kun makulering og destruksjonstjenester og vil ikke behandle data på en måte som vil utløse krav eller mulighet for dataportabilitet.

Behandlingsansvarlig er ansvarlig for å behandle og eventuelt etterkomme krav om dataportabilitet fra Registrerte i samsvar med gjeldende personvernregelverk.

10. Bruk av Underdatabehandler

Databehandlerens bruk av Underdatabehandler til å Behandle Personopplysninger skal avtales skriftlig med Behandlingsansvarlig før Behandlingen starter hos Underdatabehandler.

Følgende Underdatabehandler(e) er forhåndsgodkjent:

- Norsk Gjenvinning AS
- Bozkurt Logistikk AS
- B&T Logistikk
- Holtet KMT AS
- Hovland Transport AS
- Nils Jr. Frey
- Notodden Renovasjon & Gjenvinning AS
- Retura Iris AS
- Stenshaug / OTTS AS
- MNS Transport AS

For region Nord-Norge:

- Østbø
- Vefas Retur AS
- Perpetuum Mobile AS
- HRS Miljø AS
- Senja Avfall Næring AS
- Reno-Vest AS

Databehandler er ansvarlig for Underdatabehandlers handlinger og unnlatelser på samme måte som om dette hadde vært Databehandlers egne handlinger og unnlatelser. Databehandler har ansvar for at Underdatabehandler er kjent med Databehandlerens avtalemessige og lovmessige forpliktelser, og for at Underdatabehandleren i henhold til egen databehandleravtale med Databehandler er forpliktet til å oppfylle disse på lik linje med Databehandleren.

Databehandler, og eventuelle Underdatabehandlere, kan ikke overføre Personopplysninger utenfor EU/EØS-område uten at dette på forhånd er avtalt skriftlig med Behandlingsansvarlig, jf. punkt 6.

11. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter gjeldende Personvernregelverk, og i henhold til Vedlegg 1 til denne Databehandleravtalen, herunder implementere og opprettholde tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen forbundet med Behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til Personopplysninger som er overført, lagret eller på annen måte behandlet.

Ved vurderingen av hvilke tekniske og organisatoriske tiltak som skal implementeres, skal Databehandler, i samråd med Behandlingsansvarlig, ta i betraktning;

- det aktuelle tekniske nivå
- karakteren og omfanget av Behandlingen
- konteksten og formålet med Behandlingen,
- alvorligheten av den risiko Behandlingen av personopplysninger medfører for den Registrertes rettigheter, og
- kostnaden ved implementering.

Sikkerhetstiltakene skal forhindre bevisste og ubevisste handlinger som kan gi uautorisert tilgang eller spredning av data så vel som enhver annen bruk av personopplysninger som ikke er i overenstemmelse med Behandlingsansvarliges instruksjoner. Medarbeidere som utfører makulering, skal ha nødvendig kompetanse for å utøve oppgaven.

Databehandleren må sørge for å ha forsvarlig sikring av digitale medier, beholdere, lokasjoner, tilganger og annet relevant utstyr, både ved tekniske og organisatoriske tiltak, slik at ingen uvedkommende kan få tilgang til personopplysninger. Det samme gjelder fysiske dokumenter som må skjermes mot uautorisert innsyn.

Tekniske tiltak skal foreligge slik at personer enten i eller utenfor Databehandlers virksomhet ikke skal kunne aksessere personopplysninger uten at dette blir loggført, slik at det fremgår hvem som har kunnet aksessere informasjonen.

Databehandleren skal ha et kvalitetssystem tilpasset det til enhver tid gjeldende Personvernregelverk. Systemet skal omfatte - men ikke avgrenses til rutiner for:

- Avviksbehandling som omfatter varsling ved sikkerhetsbrudd;
- Sikkerhetsrevisjon;
- Ledelsens gjennomgang av kvalitets og sikkerhetsarbeidet

Databehandleren plikter å dokumentere sine sikkerhetsrutiner. Dokumentasjonen skal på forespørsel gjøres tilgjengelig for Behandlingsansvarlig.

12. Avvik

Ved avdekking av brudd på kravene til informasjonssikkerhet, plikter Databehandler uten ugrunnet opphold, og senest innen 24 timer å meddele dette til Behandlingsansvarliges kontaktpunkt for avtalen.

Dette gjelder ikke feil som åpenbart ikke har hatt betydning for sikkerheten rundt og opplysninger om de Registrerte. Dersom Databehandler er i tvil om avvikets konsekvenser, skal Behandlingsansvarlig likevel varsles.

Meldingen skal inneholde:

- en beskrivelse av avviket og, hvis mulig, omfang av avviket
- navn og kontaktdetaljer til eventuelt personvernombud eller annen kontaktperson hos Databehandler,
- en beskrivelse av de sannsynlige konsekvensene av hendelsen,
- en beskrivelse av tiltakene som er, eller vil bli tatt, for å adressere avviket og, når relevant, tiltak som motvirker negative konsekvenser av avviket.

Databehandler er ansvarlig for at avviksmeldingen sendes til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding eventuelt sendes Datatilsynet og eventuelt til Registrerte som er berørt.

13. Krav til sikkerhetsrevisjon

Databehandleren skal jevnlig og etter vesentlige endringer eller avvik, gjennomføre sikkerhetsrevisjoner av systemer og annet som er relevante for Behandlingen av Personopplysninger i henhold til denne Databehandleravtalen. Sikkerhetsrevisjonen skal verifisere at de tekniske, fysiske og organisatoriske sikkerhetstiltak som er besluttet etablert, faktisk blir etterlevd og fungerer etter sin hensikt, samt identifisere mulige forbedringer. Resultatet fra sikkerhetsrevisjon skal dokumenteres og være tilgjengelig for Behandlingsansvarlig, bl.a. for bruk i Behandlingsansvarlig sikkerhetsrevisjon.

Databehandler skal tillate og bistå dersom Behandlingsansvarlig gjennomfører sikkerhetsrevisjoner hos Databehandler, eventuelt ved bruk av en tredjepart/revisor engasjert av Behandlingsansvarlig. Behandlingsansvarlig må selv dekke egne kostnader relatert til inspeksjoner og sikkerhetsrevisjoner initiert av Behandlingsansvarlig. Behandlingsansvarlig må minimum varsle Databehandler 3 måneder før ønsket oppstart av inspeksjon/revisjon.

Databehandler har oppfølgingsansvar overfor eventuelle Underdatabehandlere for at disse faktisk etterlever sikkerhetskravene. Behandlingsansvarlig kan kreve bekreftelser fra tredjepart på at slik revisjon har blitt gjennomført og at resultatet av revisjonen fremlegges uten ugrunnet opphold.

14. Opplæring og kompetanse

Databehandler skal påse at alle som gis tilgang til systemer og/eller håndterer Personopplysninger, til enhver tid, har den nødvendige og tilstrekkelige kunnskap til å bruke systemene for sin rolle, utføre sine oppgaver og til å ivareta informasjonssikkerheten.

15. Avtalens varighet og opphør av Databehandleravtalen

Denne Databehandleravtalen gjelder fra inngåelse av oppdrag og opphører på samme tidspunkt som Avtalen opphører eller på det tidspunkt Databehandler ikke lenger behandler Personopplysninger for Behandlingsansvarlig.

Ved opphør av Databehandleravtalen gjelder følgende for dokumenter, lagringsmedier og annet som kan inneholde Personopplysninger som omfattes av Avtalen:

Materiale som er overlevert til Databehandler for makulering eller destruksjon i henhold til Avtalen, skal behandles i samsvar med Avtalen.

Ved skriftlig forespørsel fra Behandlingsansvarlig vil Databehandler kunne tilbakelevere plomberte beholdere eller oppsamlingsenheter med medier eller dokumenter til Behandlingsansvarlig, forutsatt at destruksjons- eller makuleringsprosessen ikke allerede er påbegynt og materialet er fortsatt i en tilstand som muliggjør tilbakelevering.

Ved brudd på denne Databehandleravtale eller gjeldende personvernregelverk, kan Behandlingsansvarlig pålegge Databehandleren å stoppe den videre Behandlingen av opplysningene med øyeblikkelig virkning og terminere denne Databehandleravtalen.

16. Lovvalg og verneting

Partenes rettigheter og plikter etter Databehandleravtalen reguleres av norsk rett. Enhver tvist i forbindelse med Databehandleravtalen skal i alle tilfeller forsøkes løst ved dialog og forhandling mellom Partene.

Hvis slike forhandlinger ikke fører frem, skal tvisten avgjøres ved ordinær rettergang, med mindre annet fremgår av avtale mellom Partene. Partene vedtar NG Secures forretningsadresse skal være rett verneting.

Vedlegg 1 Instruks for Behandling av Personopplysninger

1. Behandlingens gjenstand/instruks for behandlingen

Databehandlerens Behandling av Personopplysninger på vegne av den Behandlingsansvarlige skjer ved at Databehandleren utfører følgende:

Databehandler vil utføre makulerings og/eller destruksjonstjenester av dokumenter, digitale lagringsmedier eller varer og produkter i henhold til Avtalen.

2. Informasjonssikkerhet

Behandlingen vil kunne omfatte sletting/destruksjon av større mengder personopplysninger omfattet av personvernforordningen artikkel 9 om 'særlige kategorier av personopplysninger'. Derfor skal det som utgangspunkt etableres et 'høyt' sikkerhetsnivå.

Databehandleren har heretter rett og plikt til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige (og avtalte) sikkerhetsnivået.

Databehandleren skal likevel – under enhver omstendighet og som minimum – gjennomføre følgende tiltak, som er avtalt med den Behandlingsansvarlige:

Risikovurdering

Databehandleren utfører stedlige risikovurderinger ihht. NS5014 og NS5830-serien.

Kvalitetsledelse

Databehandleren har implementert og vedlikeholder kvalitetsstyringssystem i henhold til ISO 9001 standarden.

Sikre beholdere

Dokumenter og digitale media oppbevares i plomberte beholdere, sikkerhetsposer, eller låsbare beholdere, helt frem til makulering finner sted.

Sikkerhetsgodkjent og uniformert personell

Alt personell som har tilgang til sensitivt materiale er sikkerhetsgodkjent ved at det er utført bakgrunnssjekk, innhentet politiattest der dette er hjemlet i lov, signert taushetserklæring og signert og gjennomført relevant sikkerhetsopplæring. Sjåfører er uniformert og bærer synlige ID-kort.

Sikre lokaler

Innholdet i makuleringsbeholderen makuleres på godkjent anlegg med streng adgangskontroll og kvalitetssikrede rutiner. Alle lokaler har godkjent innbruddsalarm og videoovervåking tilknyttet en vaktsentral med uttrykning.

Makulering/destruksjon

Dokumenter makuleres i kvern, Untha RE 100-4s, som krysskutter papiret i så små biter at det ikke er mulig å gjenskape det opprinnelige innholdet. Størrelse på bitene vil være mindre enn 320 mm^2 etter makulering. De blandes med biter fra andre kvernede dokumenter. Papiret går deretter til materialgjenvinning for produksjon av nye papirprodukter.

Digitale lagringsmedier makuleres i kvern, Untha RS30, hvor fragmentene ikke er større enn 15 mm2 etter kverning. De blandes med fragmenter fra andre kvernede lagringsmedier og innholdet kan ikke gjenskapes. Fragmentene går deretter til metallgjenvinning. Ved særlige krav kan det kvernede materialet gå til forbrenning. Materialer som ikke kan gjenvinnes behandles som EE-avfall.

3. Lokasjon for behandling

Behandling av personopplysninger som omfattes av Databehandleravtalen kan ikke, uten den Behandlingsansvarliges skriftlige forhåndsgodkjennelse, finne sted på andre lokasjoner enn NG Secure sine egne lokasjoner, eller underleverandører oppgitt i Databehandleravtalens punkt 10.

4. Prosedyrer for den Behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til Databehandleren

Databehandleren skal jevnlig og minst årlig for egen regning innhente en revisjonsrapport fra en uavhengig tredjepart som gjelder databehandlerens overholdelse av kvalitets og sikkerhetstiltak beskrevet i Vedlegg 1, punkt 2.

Partene er enig i at følgende typer av bevis for utført revisjon benyttes, i samsvar med Vilkårene:

- ISO 9001 sertifikat
- Semac Sikringssertifikat

Behandlingsansvarlig har rett til å få oversendt sertifikat, ved forespørsel.

Den Behandlingsansvarlige eller den Behandlingsansvarliges representant skal dessuten ha adgang til å inspisere, herunder inspisere fysisk, stedene hvor Databehandleren foretar Behandling av Personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til Behandlingen. Slike inspeksjoner kan gjennomføres når den Behandlingsansvarlige finner det nødvendig, i henhold til databehandleravtalens punkt 13, 2.avsnitt.

Databehandler er selv ansvarlig for å utføre tilstrekkelig kontroll med eventuelle underdatabehandlere.