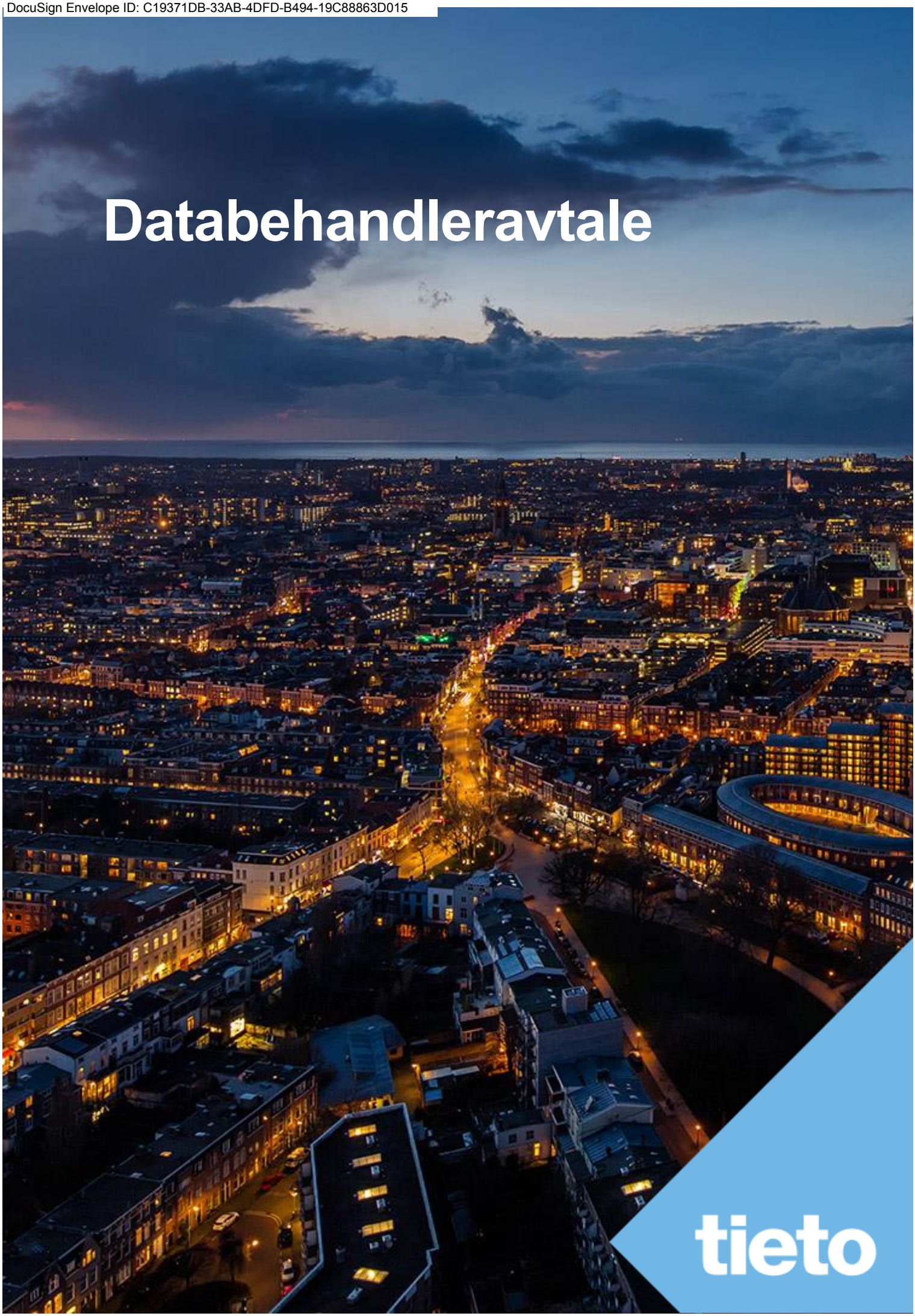
Databehandleravtale



tieto

Databehandleravtale

1 Parter

Rennebu kommune organisasjonsnummer 940 083 672 adresse Vassliveien 87 7391 Rennebu (på egne vegne og for dets Tilknyttede foretak) («**Kunde**» eller «**Behandlingsansvarlig**»)	**Tieto Norway AS** organisasjonsnummer 821 530 792 Karenslyst Allé 53 NO-0214 OSLO (på egne vegne og for dets Tilknyttede foretak) («**Leverandør**» eller «**Databehandler**»)

Kunden og Leverandøren kan også bli omtalt som en «Part» eller «Parter» etter hva som er relevant. En henvisning til «Kunde» eller «Leverandør» tolkes som henvisninger til en Part eller Parter som opptrer i disse funksjonene fra tid til annen.

I forbindelse med Behandlingen skal Kunden anses som Behandlingsansvarlig, og Leverandøren skal anses som Databehandler.

2 Avtalestruktur

2.1 Dokument-struktur og rangordning

Begrepet Hovedavtalen skal vise til individuelle avtaler som Skjema for spesifikasjon av behandlingen viser til, og/eller som får anvendelse på leveringen av Tjenester som definert i Hovedavtalen.

Databehandleravtalen skal utgjøre en integrert del av Hovedavtalen, som betyr at relevante deler av Hovedavtalen (inkludert dens bestemmelser om lovvalg og tvisteløsning) også skal gjelde for denne Databehandleravtalen, imidlertid forutsatt at i tilfelle motstrid skal bestemmelsene i denne Databehandleravtalen være de som gjelder.

DPAen inkluderer disse vedleggene, som gjelder i denne rekkefølgen:

1 Definerte begreper
2 Skjema for spesifikasjon av behandlingen
3 Sikkerhetstiltak

2.2 Definerte begreper

Når det er relevant, skal begrep med store bokstaver som brukes her, ha den betydningen som i Vedlegg 1. Med mindre og i den grad sammenhengen krever noe annet, skal all bruk av entall omfatte flertall og omvendt.

3 Formål

3.1 Omfang

Denne Databehandleravtalen skal regulere behandlingen av Personopplysninger fra Leverandøren på vegne av Kunden i henhold til alle avtaler som er inngått mellom Partene («Hovedavtalen»).

Formålet med denne Databehandleravtalen er å etablere en bindende avtale om behandling av personopplysninger mellom Partene som påkrevd i Lovene. Partene bekrefter og samtykker i at hvis Lovene eller retningslinjer fra tilsynsmyndighetene endres i vesentlig grad, skal vilkårene i denne Databehandleravtalen revideres slik at de så langt som mulig gjenspeiler Partenes opprinnelige prinsipper når de iverksetter denne Databehandleravtalen.

Partene skal angi Behandlingsaktivitetene som utføres i henhold til denne Databehandleravtalen i samsvar med skjemaet vedlagt som Vedlegg 2, Skjema for spesifikasjon av behandlingen, som – i utfylt form – skal være en integrert del av denne Databehandleravtalen, imidlertid forutsatt at i tilfelle motstrid, er det bestemmelsene i Skjema for spesifikasjon av behandlingen som skal gjelde.

4 Rettigheter og plikter

4.1 Generelt

Begge Parter skal være ansvarlig for å sikre at Behandlingen utføres i samsvar med Lovene som gjelder for hver Part samt god databehandlingspraksis.

4.2 Rettigheter og plikter for Behandlingsansvarlige

Den Behandlingsansvarlige skal

1 gi Databehandleren dokumenterte og omfattende instrukser om Behandlingen, og disse instruksene skal overholde Lovene,

2 ha rett og plikt til å angi formålet med og hjelpemidlene for å behandle Personopplysninger,

3 bekrefte at alle registrerte med Personopplysninger har fått alle relevante meldinger og opplysninger, og fastslå og opprettholde i den aktuelle gyldighetstiden de nødvendige rettslige grunnlagene for å overføre Personopplysninger til Databehandleren og tillate at Databehandleren utfører Behandlingen som er planlagt i denne avtalen,

4 bekrefte at dersom Behandlingsansvarlig representerer sine Tilknyttede foretak eller tredjeparter under denne Databehandleravtalen, har Behandlingsansvarlig juridisk grunnlag til å inngå denne Databehandleravtalen med Databehandleren, og tillate at Databehandleren behandler Personopplysningene ut fra vilkårene i denne Databehandleravtalen og Hovedavtalen,

	5 bekrefte at • Behandlingen fastsatt i denne Databehandleravtalen oppfyller den Behandlingsansvarliges krav, inkludert, men ikke begrenset til, med hensyn til planlagte sikkerhetstiltak, og at • den Behandlingsansvarlige har gitt Databehandleren all nødvendig informasjon for at Databehandleren skal kunne gjennomføre Behandlingen i samsvar med Lovene.
4.3 Rettigheter og plikter for Data-behandleren	Databehandleren skal 1 utføre Behandlingen kun ut fra og i henhold til de dokumenterte, legitime og rimelige instruksene fra den Behandlingsansvarlige, med mindre det er påkrevd å gjøre det på annen måte gjennom Lovene, og i sistnevnte tilfelle skal Databehandleren informere den Behandlingsansvarlige om slike avvikende juridiske krav (forutsatt at Lovene ikke forbyr slik varsling). For å unngå tvil skal den Behandlingsansvarlige til enhver tid anses å ha instruert Databehandleren om å levere tjenestene som definert og avtalt i Hovedavtalen, 2 sikre at personer som har myndighet til å utføre Behandlingen angitt her, har forpliktet seg til konfidensiell behandling eller er underlagt en relevant lovfestet taushetsplikt som nærmere angitt i denne Databehandleravtalen, 3 treffe alle sikkerhetstiltak som er påkrevd av Databehandlere i henhold til Lovene som nærmere angitt i denne Databehandleravtalen, 4 overholde vilkårene som følger av Lovene for å engasjere Underdatabehandlere som nærmere angitt i denne Databehandleravtalen, 5 i den grad det er mulig og samtidig som det tas hensyn til Behandlingens art, bistå den Behandlingsansvarlige gjennom egnede tekniske og organisatoriske tiltak, for å oppfylle den Behandlingsansvarliges plikt til å svare på forespørsler om utøvelse av de registrertes rettigheter som fastsatt i Lovene, 6 bistå den Behandlingsansvarlige med å sikre overholdelse av dennes juridiske forpliktelser, som informasjonssikkerhet, melding om brudd på informasjonssikkerhet, vurdering av informasjonssikkerhet og plikt til forhåndsdrøfting, som påkrevd av Databehandleren gjennom Lovene, idet det tas hensyn til Behandlingens art og informasjonen som er tilgjengelig for Databehandleren, 7 etter instruks fra den Behandlingsansvarlige, slette eller returnere til den Behandlingsansvarlige alle Personopplysninger etter avsluttet levering av Tjenester knyttet til Behandlingen, og slette eksisterende kopier med

	mindre gjeldende lovgivning krever lagring av Personopplysninger. Sletting og returmetoder kan være nærmere avtalt mellom Partene, og 8 opprettholde nødvendige registre og stille til rådighet for den Behandlingsansvarlige all informasjon som er nødvendig for å overholde og dokumentere Databehandlerens plikter, som fastsatt i Lovene, og tillate og bidra til revisjoner, inkludert inspeksjoner, utført av den Behandlingsansvarlige eller en revisor med fullmakt fra den Behandlingsansvarlige som nærmere avtalt i denne Databehandleravtalen. Med mindre annet er avtalt, skal Databehandleren ha rett til å fakturere eventuelle kostnader som oppstår som følge av ovennevnte bistand i henhold til punkt 5-6 over, ut fra Databehandlerens gjeldende prisliste.

5 Informasjonssikkerhet

5.1 Sikkerhetst-iltak	Databehandleren skal iverksette og opprettholde passende tekniske og organisatoriske tiltak for å beskytte Personopplysningene, idet det tas hensyn til: 1 beste praksis, kostnader for gjennomføring samt art, omfang, sammenheng og formål med Behandlingen, samt risiko for varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter, og 2 de risikoene som følger av Behandlingen, særlig gjennom utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert utlevering av, eller tilgang til, Personopplysninger som er overført, lagret eller behandlet på annen måte.
5.2 Detaljer om Sikkerhetst-iltak	Prinsippene for Sikkerhetstiltakene som Databehandleren har iverksatt for relevant Behandling i henhold til denne Databehandleravtalen, er beskrevet i Vedlegg 3 og kan bli nærmere angitt og endret i den relevante Spesifikasjon for behandlingen og/eller Hovedavtalen. Slike tiltak omfatter blant annet, etter hva som er relevant: 1 pseudonymisering og kryptering av Personopplysninger, 2 evnen til å sikre løpende konfidensialitet, integritet, tilgjengelighet og robusthet for behandlingssystemer og -tjenester, 3 evnen til å gjenopprette tilgjengeligheten og tilgangen til Personopplysninger på en rettidig måte i tilfelle fysiske eller tekniske hendelser, og 4 en prosess for regelmessig testing, vurdering og evaluering av effektiviteten til tekniske og organisatoriske tiltak for å ivareta sikkerheten ved Behandlingen.

5.3 Informasjon om Sikkerhets-tiltak	Den Behandlingsansvarlige har ansvar for å sikre at Databehandleren blir informert om alle forhold (inkludert men ikke begrenset til risikovurdering og inkludering av særlige kategorier av Personopplysninger) knyttet til Personopplysninger som den Behandlingsansvarlige har levert, og som påvirker tekniske og organisatoriske tiltak som benyttes i henhold til denne Databehandleravtalen.
5.4 Endring av Sikkerhets-tiltak	Endringer skal behandles i samsvar med endringsstyringsprosessen i Hovedavtalen.

6 Underdatabehandler

6.1 Bruk av Underdata-behandlere	Databehandleren kan fra tid til annen bruke Underdatabehandlere for å behandle Personopplysningene angitt her. Underdatabehandlere som brukes for å levere Tjenestene er oppført i Spesifikasjon for behandlingen og/eller i Hovedavtalen Slik bruk vil være i henhold til skriftlig avtale, og Databehandleren vil kreve at Underdatabehandleren overholder personvernforpliktelsene som gjelder for Databehandleren i henhold til denne Databehandleravtalen eller forpliktelser som gir samme nivå av personvern og informasjonssikkerhet. Databehandleren skal være like ansvarlig for sine Underdatabehandleres handlinger som sine egne.
6.2 Samtykke	Den Behandlingsansvarlige samtykker i at Databehandleren har generelt samtykke til å bruke Databehandlerens Tilknyttede foretak som Underdatabehandlere ved Behandling av Personopplysninger.
6.3 Endring av Underdata-behandlere	Databehandleren skal informere den Behandlingsansvarlige på forhånd om eventuelle planlagte endringer som gjelder tillegg av Underdatabehandlere eller utskiftning av dem. Dersom den Behandlingsansvarlige ikke aksepterer en planlagt endring, kan den Behandlingsansvarlige skriftlig si opp den delen av Hovedavtalen som underdatabehandlingen er knyttet til, med tretti (30) dagers varsel.

7 Overføring av Personopplysninger

7.1 Kundesam-tykke til overføring av Personopplys ninger utenfor	Databehandleren skal bare overføre Personopplysninger fra territoriet til medlemsstatene i EU, EØS eller andre stater som Europakommisjonen har besluttet at garanterer et tilfredsstillende nivå for personvern og informasjonssikkerhet (samlet kalt «Godkjente Jurisdiksjoner» med skriftlig samtykke fra den Behandlingsansvarlige på forhånd.

Godkjente Jurisdiksjoner	
7.2 Databeskyttelse ved Dataover-føring	Dersom det kreves i henhold til gjeldende lovgivning, skal Databehandleren inngå relevante kontraktsmessige ordninger med påkrevde parter (herunder med den Behandlingsansvarlige selv eller noen av den Behandlingsansvarliges Tilknyttede foretak) for lovlig overføring av Personopplysninger fra Godkjente Jurisdiksjoner til tredjestater. Slike kontraktsmessige ordninger skal utføres i samsvar med de standardvilkår for datasikkerhet vedtatt eller godkjent av Europakommisjonen («Standard kontraktsvilkår»/«Standard Contractual Clauses»). Som et alternativ til å inngå Standard kontraktsvilkår, kan Databehandleren basere seg på en alternativ beskyttelse av overføringen, som tillater og sørger for lovlig overføring av Personopplysninger utenfor de Godkjente Jurisdiksjonene, forutsatt at slik beskyttelse er i samsvar med gjeldende lovgivning.
7.3 Rangordning	Standard kontraktsvilkår som er relevante for denne Databehandleravtalen, finnes som vedlegg til denne Databehandleravtalen, og skal gjelde for alle Spesifikasjoner for behandlingen der en relevant overføring er blitt angitt. Ved motstrid mellom Standard kontraktsvilkår eller annen alternativ beskyttelse av overføringen som tillater lovlig overføring av Personopplysninger utenfor de Godkjente Jurisdiksjonene, og Databehandleravtalen, skal Standard kontraktsvilkår eller slike alternative rammevilkår alltid gå foran Hovedavtalen og denne Databehandleravtalen.

8 Melding om Personvernbrudd

8.1 Prosess for varsel om Personvernbrudd	Databehandleren skal uten ugrunnet opphold varsle den Behandlingsansvarlige dersom den, eller en av dens Underbehandlere, blir kjent med Personvernbrudd. Det skal gis informasjon til kontaktpersonen som er utpekt av den Behandlingsansvarlige, dersom ikke annet er avtalt mellom Partene.
8.2 Innhold i varsel om Person-vernbrudd	Databehandleren skal uten ugrunnet opphold informere den Behandlingsansvarlige om omstendighetene som har ført til Personvernbruddet, og om annen tilknyttet informasjon som den Behandlingsansvarlige med rimelighet ber om og som er tilgjengelig for Databehandleren. I tillegg skal informasjon som gis til den Behandlingsansvarlige, i den grad slik informasjon er tilgjengelig for Databehandleren, omfatte: 1 en beskrivelse av arten av Personvernbrudd, herunder når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og

	kategoriene av og omtrentlig antall Personopplysningsposter som er berørt, 2 en beskrivelse av de sannsynlige konsekvensene Personvernbruddet, og 3 en beskrivelse av tiltak som Databehandleren har truffet eller foreslår å treffe for å håndtere Personvernbruddet, herunder dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet. Partene kan bli enige om en mer detaljert prosess for melding om brudd atskilt fra dette.

9 Revisjon

9.1 Generelt	Den Behandlingsansvarlige skal ha rett til å revidere Databehandlerens utførelse av sine Behandlingsforpliktelser i henhold til denne Databehandleravtalen («Revisjon»).
9.2 Gjennom-føring av revisjon	Den Behandlingsansvarlige har plikt til å bruke eksterne revisorer som ikke er konkurrenter til Databehandleren, til å utføre en slik revisjon. Partene skal bli enige i god tid i forveien om tidspunkt og andre detaljer knyttet til gjennomføring av slike Revisjoner. Revisjonen skal gjennomføres på en slik måte at Databehandlerens forpliktelser overfor tredjeparter (inkludert, men ikke begrenset til Databehandlerens kunder, partnere og leverandører) på ingen måte settes i fare. Alle Behandlingsansvarliges representanter eller eksterne revisorer som deltar i Revisjonen, skal underlegges vanlig taushetsplikt overfor Databehandleren.
9.3 Myndigheters revisjonsad-gang	Databehandleren skal alltid tillate at enhver relevant tilsynsmyndighet som fører tilsyn med den Behandlingsansvarliges virksomhet, skal få utført Revisjoner av Databehandlerens virksomhet, og i så fall får relevante deler av Partenes avtale som er angitt her, anvendelse.
9.4 Revisjonskost nader	Den Behandlingsansvarlige skal stå for alle kostnader til Revisjonen, og skal godtgjøre Databehandleren for alle kostnader som påløper som følge av Revisjonen; imidlertid forutsatt at dersom Revisjonen avdekker vesentlige avvik i Databehandlerens arbeid, skal Databehandleren selv stå for egne kostnader til Revisjonen.

10 Taushetsplikt

10.1 Databehandlerens plikter	Databehandleren skal 1 holde alle Personopplysninger som er mottatt fra den Behandlingsansvarlige, konfidensielt, 2 sikre at personer som er autorisert til å behandle Personopplysninger, har forpliktet seg til å overholde taushetsplikten, og 3 sikre at Personopplysninger ikke avsløres til tredjeparter uten skriftlig forhåndssamtykke fra den Behandlingsansvarlige, med mindre Databehandleren er forpliktet gjennom ufravikelig lov eller forordning til å fremlegge slik informasjon.
10.2 Innsyn	I tilfelle registrerte eller offentlige myndigheter kommer med en forespørsel om Personopplysninger, skal Databehandleren så snart som praktisk mulig, informere den Behandlingsansvarlige om slike forespørsler før det gis noe svar eller treffes andre tiltak om Personopplysningene, eller i tilfelle noen relevant myndighet krever omgående svar, så snart som praktisk mulig etter dette med mindre Leverandøren er forhindret gjennom ufravikelig lov eller pålegg fra myndighetene til å fremlegge slik informasjon.

11 Ansvarsbegrensning

11.1 Generelt	Ansvarsbegrensningen som er fastsatt i Hovedavtalen, skal gjelde også for denne Databehandleravtalen.
11.2 Ansvar	Partene er enige om at det generelle prinsippet om ansvarsfordeling mellom Partene i forbindelse med administrativ overtredelsesgebyr eller tvangsmulkt pålagt av relevante tilsynsmyndigheter eller krav reist av de registrerte under denne Databehandleravtalen, er basert på at hver enkelt Part må oppfylle sine egne forpliktelser i henhold til Lovene. Dermed skal pålagte overtredelsesgebyr/tvangsmulkt eller tilkjent erstatning betales av Parten som har unnlatt å oppfylle sine juridiske forpliktelser i henhold til Lovene, som besluttet av relevant tilsynsmyndighet eller kompetent domstol med myndighet til å pålegge slike gebyrer, tvangsmulkt eller erstatninger.

12 Gyldighetstid

12.1 Generelt	Denne Databehandleravtalen skal gjelde så lenge 1 Partene har gjeldende avtaler seg imellom, eller 2 det gjenstår forpliktelser i henhold til ethvert separat Skjema for spesifikasjon av behandlingen som er utfylt under denne avtalen, etter hva som inntreffer sist, eller 3 dersom en av Partene sier opp denne Databehandleravtalen ved å gi seks (6) måneders skriftlig varsel.

12.2 Gjenlevende klausuler	Alle bestemmelser som ut fra sin art er ment å overleve opphøret av denne Databehandleravtalen, skal fortsatt gjelde uavhengig av om denne Databehandleravtalen opphører.

13 Kopier og underskrifter

Denne Databehandleravtalen er blitt utferdiget i to (2) eksemplarer, ett til hver av Partene. Enhver undertegnet og elektronisk utvekslet kopi skal gjelde i samme grad som det undertegnede originaldokumentet.

Sted og dato 2021 april 22 | 11:48 EEDT Sted Rennebu kommune DocuSigned by: Ingrid Fagerli 0D07728EE51F411... Ingrid Fagerli	Sted og dato 2021 April 21 | 14:50 EEDT Ski **Tieto Norway AS** DocuSigned by: Andreas Slette A4CDDB5B79C64BF... Andreas Slette
<navn>r	<navn>
<navn>	<navn>

Vedlegg 1 - Definerte Begreper

Med **Tilknyttet foretak** menes et rettssubjekt som er direkte eller indirekte eid eller kontrollert av en Part, eller som direkte eller indirekte eier eller kontrollerer en Part, eller er under samme direkte eller indirekte eierskap eller kontroll som en Part, så lenge slikt eierskap eller kontroll vedvarer. Eierskap eller kontroll skal foreligge når det er direkte eller indirekte eierskap av mer enn femti (50 %) prosent av den nominelle verdien av den utstedte eierandelskapitalen, eller mer enn femti (50 %) prosent av stemmerettene som gir rett til å stemme ved valg av styremedlemmer eller personer som utøver tilsvarende funksjoner eller rettigheter gjennom andre metoder for å velge eller utnevne styremedlemmer eller personer som i fellesskap kan utøve slik kontroll.

Med **Behandlingsansvarlig** menes Kunden, som bestemmer formålet med og hjelpemidlene for Behandlingen.

Med **Databehandler** menes Leverandøren, som behandler Personopplysninger på vegne av den Behandlingsansvarlige.

Med **Lover** menes EUs personvernforordning (2016/679) og personvernlovgivningen under gjeldende lov for Hovedavtalen, som gjelder for Behandlingen angitt her, til enhver tid. Partene bekrefter og samtykker i at tidsrommet før EUs personvernforordning (2016/679) trer i kraft (forventet 25. mai 2018), skal tolkningen av denne Databehandleravtalen bygge på gjeldende personvernlovgivning under gjeldende lov for Hovedavtalen.

Med **Personopplysning** menes enhver opplysning knyttet til en identifisert eller identifiserbar fysisk person; en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, for eksempel et navn, et ID-nummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere faktorer som er spesifikke for den fysiske personens fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identitet.

Med **Personvernbrudd** menes et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, uautorisert utlevering av eller tilgang til, Personopplysninger som er overført, lagret eller på annen måte behandlet som angitt her.

Med **Behandling** menes enhver operasjon eller sett av operasjoner som utføres på Personopplysninger eller på sett av Personopplysninger, enten automatisert eller ikke, for eksempel innhenting, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller kombinering, begrensning, sletting eller tilintetgjøring av Personopplysninger.

Med **Skjema for spesifikasjon av behandlingen** menes vedlegget til Databehandleravtalen som angir behandlingsaktiviteter i henhold til Databehandleravtalen.

Med **Tjenester** menes alle tjenester som ytes i henhold til eller i forbindelse med Hovedavtalen.

Med **Underdatabehandler** menes en behandler som ifølge kontrakt med Databehandleren skal utføre Behandling som angitt her, helt eller delvis, på vegne av Databehandleren.

Vedlegg 3 - Tekniske og Organisatoriske Sikkerhetstiltak

Formålet med dette dokumentet er å beskrive prinsippene for tekniske og organisatoriske tiltak i Tietos konsernselskaper («Tieto»), som Tieto leverer til alle Kunder som standard i Tietos produkter og tjenester, som påkrevd ved forordning (EU 2016/679), personvernforordningen (General Data Protection Regulation – «GDPR»).

- Tieto iverksetter egnede tekniske og organisatoriske datasikkerhetstiltak som er utformet for å oppfylle personvernprinsippene på en effektiv måte, og sikrer at egnet beskyttelse er integrert i behandlingen av personopplysninger for å oppfylle kravene i GDPR, og beskytte de registrertes rettigheter som beskrevet nedenfor.

- Sikkerhetsbeskrivelser på produktnivå er tilgjengelig på forespørsel dersom det ikke er avtalt at de skal være en del av avtalen som styrer behandling av personopplysninger. Kundespesifikke sikkerhetstiltak avtales separat.

1 Risikovurdering av personvern

Tieto foretar og dokumenter risikovurdering for hvert Tieto-produkt eller -tjeneste. Personvern og sikkerhetsrisikoer er registrert og overvåkes i Tietos risikodatabaser.

Tieto foretar risikovurdering av personvern for å beslutte hvilke datasikkerhetstiltak som skal iverksettes. Målet er å definere et passende nivå av datasikkerhetstiltak for hvert produkt eller tjeneste. Tieto har i hvert fall minst iverksatt sikkerhetstiltakene som er beskrevet i kapittel 2 nedenfor.

2 Sikkerhetstiltak

Som del av Informasjonssikkerhetssystemet (Information Security Management System – ISMS) har Tieto retningslinjer for offentlig sikkerhet og personvern, som kundene kan få tilgang til på forespørsel. Retningslinjene støttes av et bredt utvalg av obligatoriske regler for ulike aspekter av personvern og informasjonssikkerhet. Dokumentene er underlagt en regelmessig intern gjennomgangsprosess samt en ekstern tredjepartsverifisering av deres egnethet i tillegg til gjennomgangsprosessen.

Tieto har sertifisert relevante operasjoner som benytter følgende intenasjonale standarder, ISO 27001, ISO 9001 og ISO 14001.

	Med hensyn til fysiske og miljømessige kontroller i databehandlingsanlegg og sikkerhetsledelse, utføres det hvert år en ekstern tredjepartsrevisjon som benytter ISAE 3402 Type 2-standard. Den årlige revisjonsrapporten kan leveres til Tieto-kunden på forespørsel. Dersom det er avtalt, kan Tieto også levere en kundespesifikk infrastrukturrapport, ISAE 3402 Type 2.
2.1 Sikkerhet for person-opplysninger	Tieto gjennomfører følgende tiltak basert på krav fastsatt i «Databehandlingssikkerhet» (artikkel 32 i GDPR):
	pseudonymisering og kryptering av personopplysninger Tieto benytter kryptering og/eller pseudonymisering i sin virksomhet for å redusere personvernrisikoen når det er relevant. Krypterings- og pseudonymiseringsteknikker kan variere ut fra krav til tjenester og risikovurdering av personvern. Nærmere opplysninger og de benyttede tiltakene fås på forespørsel.
	(b) evnen til å sikre løpende konfidensialitet, integritet, tilgjengelighet og robusthet for behandlingssystemer og –tjenester Vern av personopplysninger krever at det iverksettes mange sikkerhetskontroller. Standard driftsprosesser følger ITILs ramme for god bransjepraksis. Standardiserte prosesser bidrar til å sikre kvaliteten på tjenesten og beskytter behandlingen av personopplysninger. Tieto har et sentralisert system for å styre administrativ tilgang til kundenes miljøer. For å få tilgang til et kundesystem må medarbeideren ha en gyldig grunn, og tilgangen godkjennes bare ved at det benyttes en prosess som er avtalt i fellesskap med kunden. Som minimum krever all tilgang til kundens miljø en kryptert tunnel innenfor Tietos nettverk. Tilkoblinger til kundenes miljøer loggføres for å gi et fullstendig revisjonsspor for administrative operasjoner i kundemiljøer. All fjerntilkobling til Tietos tjenester krever en kryptert tilkobling og andre mulige tiltak (f.eks. sterk autentisering) som påkrevd gjennom risikovurderingen av personvern. Uautoriserte personer er forhindret fra å få fysisk tilgang til databehandlingsanlegg. Personopplysninger er beskyttet mot utilsiktet og ulovlig ødeleggelse ved hjelp av fysiske og miljømessige kontroller. Fysiske og miljømessige sikkerhetskontroller i databehandlingsanlegg er underlagt en årlig revisjon av en uavhengig tredjepart, ISAE 3402 Type 2. Tieto kontrollerer, overvåker og reviderer alle administrative tilkoblinger, tredjepartstilgang og filoverføringer som benyttes i Tietos infrastruktur.

Tieto oppretter en ramme for planlegging, iverksettelse og kontroll av kundens forretningsoperasjoner. Organisasjonsstrukturen tildeler roller og ansvar for å sikre tilstrekkelig bemanning og effektiv operativ kompetanse. Tieto-ledelsen har etablert myndighet og egnede rapporteringslinjer for nøkkelpersonell. Som del av ansettelsesprosessene utføres det verifisering av utdanning og bakgrunnssjekker basert på den ansattes stilling og tilgangsnivå til Tietos behandlingsanlegg og systemer.

Tieto opprettholder og kontrollerer gjennomføringen av Tietos sikkerhetspolitikk, gir sikkerhetsopplæring til de ansatte, og utfører gjennomganger av programsikkerhet. Disse gjennomgangene vurderer konfidensialiteten, integriteten og tilgjengeligheten for data, samt samsvar med Tietos policy for informasjonssikkerhet.

(c) evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid i tilfelle fysiske eller tekniske hendelser

For å gjenopprette tilgjengelighet og tilgangen til personopplysninger i rett tid i tilfelle fysiske eller tekniske hendelser, har Tieto backup og forretningskontinuitetsprosesser og -strategier som sikrer rask gjenoppretting av forretningskritiske systemer ved behov.

Tieto har definert planer for kontinuitet og nødgjenoppretting for Tietos infrastrustruktur, for å støtte Tietos tjenesteleveranser til Kunder. Disse planene oppdateres og testes regelmessig, og er underlagt tredjepartsrevisjoner. Kundespesifikke kontinuitetsplaner og -prosedyrer avtales separat mellom Tieto og Kunden.

(d) en prosess for regelmessig testing, vurdering og evaluering av tekniske og organisatoriske tiltaks effektivitet for å ivareta sikkerheten ved behandlingen

Tietos prosesser, planer og systemer for beredskap testes regelmessig for å vurdere og evaluere tekniske og organisatoriske tiltaks effektivitet for å ivareta sikkerheten ved behandling av personopplysninger. Kundespesifikk testing av nødgjenoppretting avtales separat.

Tieto-operasjoner følger definerte prosesser og er underlagt interne og uavhengige tredjepartsrevisjoner som del av sertifiseringen for kvalitets- og sikkerhetshåndtering (ISO 9001 og 27001).

Tieto foretar intern sikkerhetstesting og sårbarhetsskanning. For miljøer med høy risiko benytter Tieto sikkerhetstestingstjenester fra tredjeparter, inkludert penetrasjonstester.