

DATABEHANDLERAVTALE

Standardavtalevilkår

i henhold til artikkel 28 nummer 3, i Europaparlamentets og Rådets forordning 2016/679 (personvernforordningen) med henblikk på databehandlerens behandling av personopplysninger

mellom

[NAVN]

Org.nr. [ORGANISASJONSNUMMER]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

heretter «den behandlingsansvarlige»

og

[NAVN]

Org.nr. [ORGANISASJONSNUMMER]

[ADRESSE]

[POSTNUMMER OG BY]

[LAND]

heretter «databehandleren»

som hver for seg er en «part» og sammen utgjør «partene»

HAR AVTALT følgende standardavtalevilkår (Vilkårene) med henblikk på å overholde personvernforordningen og sikre beskyttelse av fysiske personers grunnleggende rettigheter og friheter

1. Innhold	
2. Innledning	3
3. Den behandlingsansvarliges rettigheter og plikter	3
4. Databehandleren handler etter instruks	4
5. Konfidensialitet	4
6. Sikkerhet ved behandlingen	4
7. Bruk av underdatabehandlere	5
8. Overføring til tredjeland eller internasjonale organisasjoner	6
9. Bistand til den behandlingsansvarlige	7
10. Underretning om brudd på personopplysningssikkerheten	8
11. Sletting og returnering av opplysninger	9
12. Revisjon, herunder inspeksjon	9
13. Partenes avtale om andre forhold	9
14. Ikrafttredelse og opphør	10
15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren.....	10
Vedlegg A Opplysninger om behandlingen	12
Vedlegg B Underdatabehandlere	13
Vedlegg C Instruks for behandling av personopplysninger	14
Vedlegg D Partenes regulering av andre forhold.....	19

1. Disse Vilklårene fastsetter den behandlingsansvarlige og databehandlerens rettigheter og plikter når databehandleren utfører behandling av personopplysninger på vegne av den behandlingsansvarlige.
2. Disse Vilklårene er utformet med for å sikre partenes etterlevelse av artikkel 28 nummer 3 i Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen).
3. I forbindelse med leveringingen av tjenester som er utviklet i Offentlig Mobilitetssamarbeid (OMS) behandler databehandleren personopplysninger på vegne av den behandlingsansvarlige i overensstemmelse med disse Vilklårene.
4. Vilklårene har forrang i forhold til eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.
5. Det er fire vedlegg til disse Vilklårene, og vedleggene utgjør en integrert del av Vilklårene.
6. Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder om behandlingens formål og art, typen av personopplysninger, kategoriene av registrerte og behandlingens varighet.
7. Vedlegg B inneholder den behandlingsansvarliges betingelser for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som den behandlingsansvarlige har godkjent.
8. Vedlegg C inneholder den behandlingsansvarliges instruks når det gjelder databehandlerens behandling av personopplysninger, en beskrivelse av de sikkerhetstiltakene som databehandleren som minimum skal gjennomføre, og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal utføres.
9. Vedlegg D inneholder bestemmelser om andre aktiviteter som ikke er omfattet av Vilklårene.
10. Vilklårene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.
11. Disse Vilklårene fritar ikke databehandleren fra plikter som databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

3. Den behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernforordningen (se personvernfor-

ordningen artikkel 24), gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes¹ nasjonale rett og disse Vilklårene.

2. Den behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
3. Den behandlingsansvarlige er ansvarlig for, blant annet, å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om å gjøre.

4. Databehandleren handler etter instruks

1. Databehandleren skal bare behandle personopplysninger etter dokumenterte instruks fra den behandlingsansvarlige, med mindre noe annet kreves av unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Disse instruksene skal være spesifisert i vedlegg A og C. Etterfølgende instruks kan også gis av den behandlingsansvarlige mens det skjer behandling av personopplysninger, men instruksene skal alltid være dokumenterte og oppbevares skriftlig, herunder elektronisk, sammen med disse Vilklårene.
2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom en instruks fra den behandlingsansvarlige, etter databehandlerens mening, er i strid med personvernforordningen eller gjeldende personopplysningsvernbestemmelser i unionsretten eller medlemsstatenes nasjonale rett.

5. Konfidensialitet

1. Databehandleren kan bare gi tilgang til personopplysninger som behandles på den behandlingsansvarliges vegne til personer underlagt databehandlerens instruksjonsmyndighet som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og bare i det nødvendige omfang. Listen av personer som har fått tilgang skal gjennomgås fortløpende. På bakgrunn av en slik gjennomgang kan tilgangen til personopplysninger stenges, dersom den ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelig for disse personene.
2. Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de aktuelle personene underlagt databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

6. Sikkerhet ved behandlingen

1. Personvernforordningen artikkel 32 fastslår at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

¹ Henvisninger til «medlemsstater» i disse Vilklårene skal forstås som en henvisning til stater som er del av det europeiske økonomiske samarbeidsområdet (EØS-stater).

Avtalen er en standard databehandleravtale vedtatt av det danske datatilsynet og lagt frem for personvermrådet (EDPB). Det norske datatilsynet har uoffisielt oversatt avtalen til norsk. Foreliggende avtale er utarbeidet av Entur AS for Offentlig Mobilitet Samarbeid i kollektivsektoren (OMtligS).

Den behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør og gjennomføre tiltak for å imøtegå disse risikoene. Avhengig av relevans kan tiltakene omfatte:

- a. pseudonymisering og kryptering av personopplysninger
 - b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene
 - c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse
 - d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.
2. Ifølge personvernforordningen artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å imøtegå risikoene. Med henblikk på denne vurderingen skal den behandlingsansvarlige stille den nødvendige informasjonen til rådighet for databehandleren som gjør vedkommende i stand til å identifisere og vurdere slike risikoer.
3. Databehandleren skal også bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges plikter etter personvernforordningen artikkel 32, ved blant annet å stille til den behandlingsansvarliges rådighet nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som databehandleren allerede har gjennomført i henhold til personvernforordningen artikkel 32, samt all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sine plikter etter personvernforordningen artikkel 32.

Hvis imøtegåelse av de identifiserte risikoene – etter den behandlingsansvarliges vurdering – krever at det gjennomføres ytterligere tiltak enn det databehandleren allerede har gjennomført, skal den behandlingsansvarlige angi disse tiltakene i vedlegg C.

7. Bruk av underdatabehandlere

1. Databehandleren skal oppfylle betingelsene som er fastsatt i personvernforordningen artikkel 28 nummer 2 og nummer 4 for å gjøre bruk av en annen databehandler (en underdatabehandler).
2. Databehandleren må således ikke bruke en underdatabehandler for å oppfylle Vilkårene uten på forhånd å ha innhentet en generell skriftlig godkjenning fra den behandlingsansvarlige.
3. Databehandleren har den behandlingsansvarliges generelle godkjenning til å benytte underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planlagte endringer som gjelder tilføyelse eller utskifting av underdatabehandlere med minst 1 måned varsel og dermed gi den behandlingsansvarlige mulighet til å motsette seg slike endringer før den eller de beskrevne

underdatabehandler(e) engasjeres. Lengre varslingsfrister for spesifikke underdatabehandlertjenester kan angis i vedlegg B. Listen over underdatabehandlere som den behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.

4. Når databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal underleverandøren pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilklårene, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning.

Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som minimum overholder databehandlerens forpliktelser etter disse Vilklårene og personvernforordningen.

5. En kopi av slik underdatabehandleravtale og eventuelle etterfølgende endringer skal – ved den behandlingsansvarliges anmodning – sendes til den behandlingsansvarlige, som på denne måten har mulighet for å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilklårene. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den behandlingsansvarlige.
6. Databehandleren skal i underdatabehandleravtalen inkludere den behandlingsansvarlige som begunstiget tredjepart i tilfelle databehandleren går konkurs, slik at den behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakeføre personopplysningene.
7. Hvis databehandleren ikke oppfyller sine personopplysningsvernforpliktelser blir databehandleren fullt ut ansvarlig overfor den behandlingsansvarlige når det gjelder oppfyllelse av underdatabehandlerens forpliktelser. Dette påvirker ikke de registrertes rettigheter etter personvernforordningen – særlig de nedfestet i personvernforordningen artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

8. Overføring til tredjeland eller internasjonale organisasjoner

1. Databehandleren kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den behandlingsansvarlige, og slik overføring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.
2. Hvis overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomføre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumentert instruks fra den behandlingsansvarlige kan databehandleren innenfor rammene av disse Vilklårene således ikke:
 - a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon
 - b. overlate behandling av personopplysninger til en underdatabehandler i et tredjeland
 - c. behandle personopplysningene i et tredjeland
4. Den behandlingsansvarliges instruks når det gjelder overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningen kapittel V som overføringen er basert på, skal angis i vedlegg C.6.
5. Disse Vilklårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 nummer 2 bokstav c og d, og disse Vilklårene kan ikke utgjøre et grunnlag for overføring av personopplysninger under personvernforordningen kapittel V.

9. Bistand til den behandlingsansvarlige

1. Databehandleren bistår, idet det tas hensyn til behandlingens art og i den grad det er mulig, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III.

Dette innebærer at databehandleren så langt det er mulig skal bistå den behandlingsansvarlige i den behandlingsansvarlige oppfyllelse av:

- a. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
 - b. opplysningsplikten dersom personopplysninger ikke er blitt samlet inn fra den registrerte
 - c. den registrertes rett til innsyn
 - d. retten til retting
 - e. retten til sletting («retten til å bli glemt»)
 - f. retten til begrensning av behandling
 - g. underrettingsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
 - h. retten til dataportabilitet
 - i. retten til å protestere
 - j. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisk behandling, herunder profilering
2. I tillegg til databehandlerens forpliktelse til å bistå den behandlingsansvarlige i henhold til Vilklårene 6.3., bistår databehandleren også, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, den behandlingsansvarlige med:

- a. den behandlingsansvarliges forpliktelse ved brudd på personopplysningsikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningsikkerheten til den kompetente tilsynsmyndigheten, Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter
 - b. den behandlingsansvarliges forpliktelse til uten ugrunnet opphold å underrette den registrerte om bruddet på personopplysningsikkerheten når det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter
 - c. den behandlingsansvarliges forpliktelse til før behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (vurdering av personvernkonsekvenser)
 - d. den behandlingsansvarliges forpliktelse til å rådføre seg med den kompetente tilsynsmyndigheten, Datatilsynet, før behandlingen dersom en vurdering av personvernkonsekvenser tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.
3. Partene skal i vedlegg C oppgi de egnede tekniske og organisatoriske tiltakene gjennom hvilke databehandleren skal bistå den behandlingsansvarlige, samt omfanget og utstrekningen av den påkrevde bistanden. Dette gjelder for forpliktelsene som følger av Vilkårene 9.1. og 9.2.

10. Underretning om brudd på personopplysningsikkerheten

1. Ved brudd på personopplysningsikkerheten skal databehandleren underrette den behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det.
2. Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje innen 24 timer etter at databehandleren har fått kjennskap til bruddet på personopplysningsikkerheten, slik at den behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.
3. I overensstemmelse med Vilkår 9 nummer 2 bokstav a skal databehandleren bistå den behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Det innebærer at databehandleren skal bistå med å fremskaffe informasjon listet opp nedenfor, som ifølge personvernforordningen artikkel 33 nummer 3 skal fremgå av den behandlingsansvarliges melding av bruddet til den kompetente tilsynsmyndigheten:
 - a. arten av bruddet på personopplysningsikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt
 - b. de sannsynlige konsekvenser av bruddet på personopplysningsikkerheten

- c. de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.
4. Partene skal i vedlegg C oppgi all informasjon som databehandleren skal fremskaffe når vedkommende bistår den behandlingsansvarlige med å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

11. Sletting og returnering av opplysninger

1. Ved opphør av databehandlertjenestene skal databehandleren slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet, med mindre unionsretten eller medlemsstatenes nasjonale rett krever oppbevaring av personopplysningene.
2. Følgende regler i unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt krever oppbevaring av personopplysningene etter at databehandlertjenestene har opphørt:
 - a. Bokføringsloven

Databehandleren forplikter seg til å utelukkende behandle personopplysningene til de(t) formål, med den varlighet og under de betingelsene som disse reglene fastsetter.

12. Revisjon, herunder inspeksjon

1. Databehandleren skal stille til den behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernforordningen artikkel 28 og disse Vilklårene. Videre skal databehandleren muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor som er bemyndiget av den behandlingsansvarlige.
2. Prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av databehandleren og underdatabehandlere er spesifisert i vedlegg C.7 og C.8.
3. Databehandleren forplikter seg til å gi tilsynsmyndighetene, som etter gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens lokaler, eller representanter som opptrer på slike tilsynsmyndigheters vegne, adgang til databehandlerens fysiske lokaler ved presentasjon av behørig legitimasjon.

13. Partenes avtale om andre forhold

1. Partene kan avtale andre bestemmelser som gjelder databehandlertjenestene, f.eks. erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot disse Vilklårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

1. Vilkårene trer i kraft på datoen for begge partenes underskrift.
2. Begge partene kan kreve Vilkårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilkårene gir grunn til dette.
3. Vilkårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilkårene ikke sies opp, med mindre partene avtaler andre vilkår som regulerer levering av databehandlertjenestene.
4. Hvis leveringen av databehandlertjenestene opphører, og personopplysningene er slettet eller returnert til den behandlingsansvarlige i overensstemmelse med Vilkårene 11.1 og vedlegg C.4, kan Vilkårene sies opp med skriftlig varsel av begge partene.
5. Underskrift

På vegne av den behandlingsansvarlige

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-postadresse	[E-POST]
Dato	[DATO]
Underskrift	[SIGNATUR]

På vegne av databehandleren

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-postadresse	[E-MAIL]
Dato	[DATO]
Underskrift	[SIGNATUR]

15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren

1. Partene kan kontakte hverandre via nedenstående kontaktpersoner.
2. Partene forplikter seg til å orientere hverandre løpende om endringer som gjelder kontaktpersoner.

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-postadresse	[E-MAIL]

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-postadresse	[E-MAIL]

Vedlegg A Opplysninger om behandlingen

[MERK: I TILFELLE AV FLERE BEHANDLINGSAKTIVITETER SKAL DISSE OPPLYSNINGENE FYLLES INN FOR HVER ENKELT BEHANDLINGSAKTIVITET]

A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:

[BESKRIV FORMÅLET MED BEHANDLINGEN]

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal primært dreie seg om (behandlingens art):

[BESKRIV BEHANDLINGENS ART]

A.3. Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

[BESKRIV TYPEN AV PERSONOPPLYSNINGER SOM BEHANDLES]

[FOR EKSEMPEL]

«Navn, e-postadresse, telefonnummer, adresse, fødselsnummer, betalingskortopplysninger, medlemsnummer, type av medlemskap, fremmøte på treningsstudio og påmelding til bestemte gruppetreningsøkter.»

[MERK: BESKRIVELSE BØR VÆRE SÅ DETALJERT SOM MULIG. UNDER ENHVER OMSTENDIGHET SKAL TYPEN AV PERSONOPPLYSNINGER PRESISERES YTTERLIGERE ENN BARE «PERSONOPPLYSNINGER SOM DEFINERT I PERSONVERNFORORDNINGEN ARTIKKEL 4 NUMMER 1» ELLER HVILKEN KATEGORI AV OPPLYSNINGER («PERSONVERNFORORDNINGEN ARTIKKEL 6, 9 ELLER 10») SOM BEHANDLES.]

A.4. Behandlingen omfatter følgende kategorier av registrerte:

[BESKRIV KATEGORIENE AV REGISTRERTE]

A.5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan begynne etter at Vilkårene har trådt i kraft. Behandlingen har følgende varighet:

[BESKRIV BEHANDLINGENS VARIGHET]

B.1. Godkjente underdatabehandlere

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN

Ved Vilkårenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende. Databehandleren kan ikke – uten den behandlingsansvarliges eksplisitte skriftlige godkjennelse – benytte en underdatabehandler til en annen behandlingsaktivitet enn den som er avtalt for vedkommende eller bruke en annen underdatabehandler til den beskrevne behandlingsaktiviteten.

C.1. Behandlingens gjenstand/instruks for behandlingen

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

Behandlingen(e) som er beskrevet i vedlegg A.

C.2. Informasjonssikkerhet

Sikkerhetsnivået skal gjenspeile:

[IDET DET TAS HENSYN TIL BEHANDLINGENS ART, OMFANG, FORMÅL OG SAMMENHENGEN DEN UTFØRES I, SAMT RISIKOENE AV VARIERENDE SANNSYNLIGHETS- OG ALVORLIGHETSGRAD FOR FYSISKE PERSONERS RETTIGHETER OG FRIHETER, BESKRIV ELEMENTENE SOM ER AVGJØRENDE FOR SIKKERHETSNIVÅET]

[FOR EKSEMPEL]

«Behandlingen omfatter en stor mengde personopplysninger omfattet av personvernforordningen artikkel 9 om 'særlige kategorier av personopplysninger'. Derfor skal det 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:

[BESKRIV KRAVENE SOM GJELDER PSEUDONYMISERING OG KRYPTERING AV PERSONOPPLYSNINGER]

[BESKRIV KRAVENE SOM GJELDER Å SIKRE VEDVARENDE KONFIDENSIALITET, INTEGRITET, TILGJENGELIGHET OG ROBUSTHET I BEHANDLINGSSYSTEMER OG -TJENESTER]

[BESKRIV KRAVENE SOM GJELDER EVNEN TIL Å GJENOPPRETTE TILGJENGELIGHETEN OG TILGANGEN TIL PERSONOPPLYSNINGER I RETT TID DERSOM DET OPPSTÅR EN FYSISK ELLER TEKNISK HENDELSE]

[BESKRIV KRAVENE SOM GJELDER PROSESSER FOR REGELMESSIG TESTING, VURDERING OG EVALUERING AV DE TEKNISKE OG ORGANISATORISKE TILTAKENES EFFEKTIVITET NÅR DET GJELDER Å SIKRE PERSONOPPLYSNINGSIKKERHETEN]

[BESKRIV KRAVENE SOM GJELDER TILGANG TIL OPPLYSNINGENE VIA INTERNETT]

[BESKRIV KRAVENE SOM GJELDER BESKYTTELSE AV OPPLYSNINGER UNDER OVERFØRING]

[BESKRIV KRAVENE SOM GJELDER BESKYTTELSE AV OPPLYSNINGER UNDER OPPBEVARING]

Avtalen er en standard databehandleravtale vedtatt av det danske datatilsynet og lagt frem for personvernrådet (EDPB). Det norske datatilsynet har uoffisielt oversatt avtalen til norsk. Foreliggende avtale er utarbeidet av Entur AS for Offentlig Mobilitet Samarbeid i kollektivsektoren (OMtligS).

[BESKRIV KRAVENE SOM GJELDER FYSISK SIKRING AV LOKASJONER HVOR PERSONOPPLYSNINGER BLIR BEHANDLET]

[BESKRIV KRAVENE SOM GJELDER BRUK AV HJEMME-/FJERNARBEIDSPASSER]

[BESKRIV KRAVENE SOM GJELDER LOGGING]

C.3 Bistand til den behandlingsansvarlige

Databehandleren skal i den grad det er mulig – i det nedenfor beskrevne omfang og utstrekning – bistå den behandlingsansvarlige i samsvar med Vilkårene 9.1 og 9.2 ved å gjennomføre følgende tekniske og organisatoriske tiltak:

[BESKRIV OMFANGET OG UTSTREKNINGEN AV BISTANDEN SOM SKAL YTES AV DATABEHANDLEREN]

[BESKRIV DE SPESIFIKKE TEKNISKE OG ORGANISATORISKE TILTAKENE SOM DATABEHANDLEREN SKAL GJENNOMFØRE FOR Å YTE BISTAND DEN BEHANDLINGSANSVARLIGE]

C.4 Oppbevaringsperiode/sletteprosedyrer

[BESKRIV EVENTUELL OPPBEVARINGSPERIODE/SLETTEPROSEDYRE FOR DATABEHANDLEREN]

[FOR EKSEMPEL]

«Personopplysninger oppbevares i [OPPGI TIDSPERIODE ELLER HENDELSE], hvorefter de slettes automatisk av databehandleren.

Ved opphør av databehandlertjenestene skal databehandleren enten slette eller levere tilbake personopplysningene i overensstemmelse med Vilkårene 11.1, med mindre den behandlingsansvarlige – etter at Vilkårene ble underskrevet – har endret den behandlingsansvarliges opprinnelige valg. Slike endringer skal være dokumentert og oppbevares skriftlig, herunder elektronisk, sammen med Vilkårene.»

C.5 Lokasjon for behandling

Behandling av personopplysninger som omfattes av Vilkårene kan ikke, uten den behandlingsansvarliges skriftlige forhåndsgodkjennelse, finne sted på andre lokasjoner enn følgende:

[OPPGI HVOR BEHANDLINGEN FINNER STED] [OPPGI HVILKEN DATABEHANDLER ELLER UNDERDATABEHANDLER SOM BENYTTET ADRESSEN]

C.6 Instruks for overføring av personopplysninger til tredjeland

[BESKRIV INSTRUKSEN SOM GJELDER OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJELAND ELLER INTERNASJONALE ORGANISASJONER]

[OPPGI GRUNNLAGET FOR OVERFØRINGEN ETTER PERSONVERNFORORDNINGEN KAPITEL V]

Hvis ikke den behandlingsansvarlige i Vilklårene eller etterfølgende gir en dokumentert instruks som gjelder overføring av personopplysninger til et tredjeland eller internasjonal organisasjon, kan ikke databehandleren, innen rammene av Vilklårene, gjennomføre slike overføringer.

C.7 Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

[BESKRIV PROSEDYRENE FOR DEN BEHANDLINGSANSVARLIGES REVISJONER, HERUNDER INSPEKSJONER, AV BEHANDLINGEN AV PERSONOPPLYSNINGER SOM ER OVERLATT TIL DATABEHANDLEREN]

[FOR EKSEMPEL]

«Databehandleren skal **[OPPGI TIDSPERIODE]** for **[EGEN/DEN BEHANDLINGSANSVARLIGES]** regning innhente en **[REVISJONSRAPPORT/INSPEKSJONSRAPPORT]** fra en uavhengig tredjepart som gjelder databehandlerens overholdelse av personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene.

Partene er enig om at følgende typer av **[REVISJONSRAPPORT/INSPEKSJONSRAPPORT]** kan benyttes i samsvar med Vilklårene:

[BESKRIV «GODKJENTE» REVISJONSRAPPORTER/INSPEKSJONSRAPPORTER]

[REVISJONSRAPPORT/INSPEKSJONSRAPPORT] oversendes uten ugrunnet opphold til den behandlingsansvarlige til orientering. Den behandlingsansvarlige kan bestride omfanget av og/eller metoden i rapporten og kan i slike tilfeller kreve en ny **[REVISJON/INSPEKSJON]** med annet omfang og/eller med en annen metode.

Basert på resultatene av **[REVISJONEN/INSPEKSJONEN]** kan den behandlingsansvarlige kreve at det gjennomføres ytterligere tiltak for å sikre at personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene blir overholdt.

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.»

[ELLER]

«Den behandlingsansvarlige eller den behandlingsansvarliges representant skal **[OPPGI TIDSPERIODE]** utføre en fysisk inspeksjon av stedene hvor databehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen, for å fastslå at databehandleren overholder personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene.

I tillegg til planlagt inspeksjon kan den behandlingsansvarlige gjennomføre en inspeksjon av databehandleren når den behandlingsansvarlige finner det nødvendig.»

«Den behandlingsansvarliges eventuelle utgifter i forbindelse med fysisk inspeksjon dekkes av den behandlingsansvarlige selv. Databehandleren skal likevel avsette de ressurser (hovedsakelig den tid) som er nødvendig for at den behandlingsansvarlige skal kunne gjennomføre sin inspeksjon.»

C.8 [HVIS RELEVANT] Prosedyrer for revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til underdatabehandleren

[HVIS RELEVANT, BESKRIV PROSEDYRENE FOR DATABEHANDLERENS REVISJONER, HERUNDER INSPEKSJONER, AV BEHANDLINGEN AV PERSONOPPLYSNINGER SOM ER OVERLATT TIL UNDERDATABEHANDLEREN]

[FOR EKSEMPEL]

«Databehandleren skal [OPPGI TIDSPERIODE] for [EGEN/DEN BEHANDLINGSANSVARLIGES] regning innhente en [REVISJONSRAPPORT/INSPEKSJONSRAPPORT] fra en uavhengig tredjepart som gjelder underdatabehandlerens overholdelse av personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilkårene.

Partene er enig om at følgende typer av [REVISJONSRAPPORT/INSPEKSJONSRAPPORT] kan benyttes i samsvar med Vilkårene:

[BESKRIV «GODKJENTE» REVISJONSRAPPORTER/INSPEKSJONSRAPPORTER]

[REVISJONSRAPPORT/INSPEKSJONSRAPPORT] oversendes uten ugrunnet opphold til den behandlingsansvarlige til orientering. Den behandlingsansvarlige kan bestride omfanget av og/eller metoden i rapporten og kan i slike tilfeller kreve en ny [REVISJON/INSPEKSJON] med annet omfang og/eller med en annen metode.

Basert på resultatene av [REVISJONEN/INSPEKSJONEN] kan den behandlingsansvarlige kreve at det gjennomføres ytterligere tiltak for å sikre at personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilkårene blir overholdt.

Databehandleren eller databehandlerens representant skal dessuten ha adgang til å inspisere, herunder inspisere fysisk, stedene hvor underdatabehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen. Slike inspeksjoner kan gjennomføres når databehandleren (eller den behandlingsansvarlige) finner det nødvendig.

Dokumentasjon for slike inspeksjoner oversendes uten ugrunnet opphold til den behandlingsansvarlige til orientering. Den behandlingsansvarlige kan bestride omfanget av og/eller metoden i rapporten og kan i slike tilfeller kreve en ny inspeksjon med annet omfang og/eller med en annen metode»

[ELLER]

«Databehandleren eller databehandlerens representant skal [OPPGI TIDSPERIODE] utføre en fysisk inspeksjon av stedene hvor underdatabehandleren foretar behandling av personopplysninger, herunder fysiske lokaler samt systemer som benyttes til og relatert til behandlingen, for å fastslå at underdatabehandleren overholder personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene.

I tillegg til planlagt inspeksjon kan databehandleren gjennomfre en inspeksjon av underdatabehandleren nr databehandleren (eller den behandlingsansvarlige) finner det ndvendig.

Dokumentasjon for slike inspeksjoner oversendes uten ugrunnet opphold til den behandlingsansvarlige til orientering. Den behandlingsansvarlige kan bestride omfanget av og/eller metoden i rapporten og kan i slike tilfeller kreve en ny inspeksjon med annet omfang og/eller med en annen metode.

Basert p resultatene av inspeksjonen kan den behandlingsansvarlige kreve at det gjennomfres ytterligere tiltak for å sikre at personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene blir overholdt.»

[OG, HVIS RELEVANT]

«Den behandlingsansvarlige kan – hvis ndvendig – velge å initiere og delta p en fysisk inspeksjon av underdatabehandleren. Dette kan bli aktuelt dersom den behandlingsansvarlige anser at databehandlerens tilsyn med underdatabehandleren ikke har gitt den behandlingsansvarlige tilstrekkelig sikkerhet for at underdatabehandlerens behandling skjr i overensstemmelse med personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene.

Den behandlingsansvarliges eventuelle deltakelse i en inspeksjon av underdatabehandleren endrer ikke det faktum at databehandleren fortsetter å bre det fulle ansvaret for at underdatabehandleren etterlever personvernforordningen, gjeldende bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og Vilklårene.»

[OG, HVIS RELEVANT]

«Databehandlerens og underdatabehandlerens eventuelle utgifter i forbindelse med fysisk inspeksjon av underdatabehandlerens lokaler er den behandlingsansvarlige uvedkommende – uansett om den behandlingsansvarlige har initiert og deltatt i slik inspeksjon.»

