

Standardavtalevilkår for databehandling

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

mellom

Ferde AS
Org.nr. 918 012 745
Fjøsangerveien 68
5068 Bergen
Norge

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	9
15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren.....	10
Vedlegg A Opplysninger om behandlingen.....	11
Vedlegg B Underdatabehandlere.....	12
Vedlegg C Instruks for behandling av personopplysninger	13
Vedlegg D Partenes regulering av andre forhold.....	16

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 leveringen av saks-og arkivløsning 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.

Side 4 av 16

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. *Databehandleren skal ikke følge instruks fra den behandlingsansvarlige som er i strid med gjeldende norsk rett om vern av personopplysninger.*

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 alvor-

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

lighetsgrad 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.

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 spesifikk skriftlig godkjenning fra den behandlingsansvarlige.
3. Databehandleren kan bare bruke underdatabehandlere som den behandlingsansvarlige på forhånd har godkjent skriftlig. Databehandleren skal be om slik godkjenning minst tre måneder før den aktuelle underdatabehandleren engasjeres. Listen over

underdatabehandlere, som den behandlingsansvarlige allerede har godkjent, fremgår av vedlegg B.

Side 6 av 16

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 Vilåårene, 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 gjennomfrt 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 Vilåårene og personvernforordningen.

5. En kopi av slik underdatabehandleravtale og eventuelle etterflgende endringer skal – ved den behandlingsansvarliges anmodning – sendes til den behandlingsansvarlige, som på denne måten har mulighet for å srge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i disse Vilåårene. 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 gjre dem gjeldende overfor underdatabehandler, hvilket for eksempel setter den behandlingsansvarlige i stand til å instruere underdatabehandleren om å slette eller tilbakefre 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. Overfring til tredjeland eller internasjonale organisasjoner

1. Databehandleren kan kun overfre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumentert instruks fra den behandlingsansvarlige, og slik overfring skal alltid skje i overensstemmelse med personvernforordningen kapittel V.
2. Hvis overfring av personopplysninger til tredjeland eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert av den behandlingsansvarlige om å gjennomfre, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav fr 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 Vilåårene 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 Vilåårene skal ikke forveksles med standard personvernbestemmelser som omhandlet i personvernforordningen artikkel 46 nummer 2 bokstav c og d, og disse Vilåårene 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 behandlingsansvarliges 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. underretningsplikten 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 Vilåårene 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 personopplysningssikkerheten til uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet på personopplysningssikkerheten

til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter

Side 8 av 16

- b. den behandlingsansvarliges forpliktelse til uten ugrunnet opphold å underrette den registrerte om bruddet på personopplysningssikkerheten 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 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 Vilåårene 9.1. og 9.2.

10. Underretning om brudd på personopplysningssikkerheten

1. Ved brudd på personopplysningssikkerheten 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 48 timer etter at databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten, slik at den behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten, jf. personvernforordningen artikkel 33.
3. I overensstemmelse med Vilår 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 personopplysningssikkerheten, 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 personopplysningssikkerheten
 - 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 personopplysningsikkerheten til den kompetente tilsynsmyndigheten.

11. Sletting og returnering av opplysninger

1. Databehandleren forplikter seg til å utelukkende behandle personopplysningene til de(t) formål, med den varlighet og under de betingelsene som disse reglene fastsetter.
2. Når avtalen skal avsluttes, Ved opphør av databehandlertjenestene skal databehandleren levere tilbake alle personopplysningene og slette eksisterende kopier. *Gjennomføringen av tilbakeføringen og slettingen skal avtales mellom partene. Databehandleren skal gjøre alle nødvendige tiltak for å hindre at den behandlingsansvarliges data går tapt, men særlig hensyn til regler i lov eller forskrift som krever oppbevaring av personopplysningene. Data skal ikke slettes hvis det er i strid med gjeldende regler om lagring av data som den behandlingsansvarlige er omfattet av.*

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 Vilåårene. 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 Vilåårene eller er til skade for den registrertes grunnleggende rettigheter og friheter og beskyttelsen som følger av personvernforordningen.

14. Ikrafttredelse og opphør

1. Vilåårene trer i kraft på datoen for begge partenes underskrift.
2. Begge partene kan kreve Vilåårene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Vilåårene gir grunn til dette.
3. Vilåårene gjelder så lenge databehandlertjenestene varer. I denne perioden kan Vilåårene 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	Svein Jarle Fagerheim
Stilling	viseadministrerende direktør
Telefonnummer	938 06 840
E-postadresse	svein.jarle.fagerheim@ferde.no

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

[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:

[Databehandleren] bistår den behandlingsansvarlige med produkter og tjenester tilknyttet informasjonsteknologi, forvaltning og drift av IT-systemer og andre tjenester tilknyttet informasjonsteknologi.

Databehandlingen utføres for å gjøre det mulig for den behandlingsansvarlige å drive saksbehandling og arkivering ved hjelp av databehandlerens saks- og arkivløsning. Arbeidet omfatter også innkalling til, gjennomføring av og etterarbeid etter styremøter.

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

Databehandlingen skjer når kunden laster opp data til leverandørens løsning for å arkivering eller saksbehandling.

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

Databehandlingen omfatter, men er ikke begrenset til, følgende personopplysninger:

- navn
- e-postadresse
- telefonnummer
- adresse
- fødselsnummer
- betalingsinformasjon
- opplysninger om passeringer gjennom bomstasjoner
- personlige opplysninger som gir grunnlag for bortfall av plikt til å betale bompenger, f.eks. helseopplysninger eller økonomiske forhold
- informasjon i personalsaker

A.4. Behandlingen omfatter følgende kategorier av registrerte:

- personale
- styremedlemmer
- kunder/trafikanter

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

Behandlingen skal vare så lenge Databehandleren yter tjenestene etter Hovedavtalen til Behandlingsansvarlig.

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.

B.2. Varsel for godkjennelse av underdatabehandlere

Dersom databehandleren vil bruke nye underdatabehandlere i tillegg til eller i stedet for eksisterende underdatabehandlere, skal den behandlingsansvarlige varsles senest tre måneder før databehandleren ønsker at endringen skal tre i kraft.

C.1. Behandlingens gjenstand/instruks for behandlingen

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren behandler data som den behandlingsansvarlige skal arkivere.

C.2. Informasjonssikkerhet

Sikkerhetsnivået skal gjenspeile:

Personopplysninger som er omfattet av personvernforordningen artikkel 9 utgjør en liten del av den samlede datamengden som Databehandleren skal behandle som del av oppdraget. De personopplysningene som skal behandles, vil ofte være av svært sensitiv art. Informasjonen vil blant annet inneholde intim informasjon om enkeltpersoner og informasjon om enkeltpersoners bevegelsesmønster.

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:

All data i transport skal beskyttes med kryptert nettverkskommunikasjon. Det skal ikke benyttes cipher-suites som har kjente svakheter.

All lagret data skal beskyttes av kryptering. Krypteringen skal minimum tilsvare AES-128.

Systemet skal omfatte, men skal ikke avgrenses til, rutiner for:

- Avviksbehandling som omfatter varsling ved feil bruk av informasjonssystemet, herunder sikkerhetsbrudd.
- Sikkerhetsrevisjon, herunder jevnlig oversendelse av rapporter fra sikkerhetsrevisjoner.
- Ledelsens gjennomgang av sikkerhetsarbeidet.
- Gjennomføring av årlige revisjoner av virksomheten

Databehandleren skal ha en gjenopprettingsplan for tjenesten.

Databehandleren skal dokumentere at sikkerheten i tjenesten testes jevnlig.

Kommunikasjon med tjenesten over internett skal være kryptert.

Tilgang til datahall der personopplysninger lager skal sikres mot at uautoriserte for fysisk tilgang til lokalet, utstyr og informasjon.

Den fysiske sikringen gjelder både for utstyr benyttet for å behandle personopplysninger og annet utstyr med betydning for informasjonssikkerheten .

Tilgang til administrasjon av tjenesten og til personopplysninger skal måtte autentiseres med multifaktorautentisering. Systemet skal ikke lagre detaljerte brukslogger. Logger skal ikke inneholde sensitive personopplysninger.

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 Vilklårene 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]

Denne teksten vil bli fylt inn før kontraktssignering, basert på tilbudet fra leverandøren.

C.4 Oppbevaringsperiode/sletteprosedyrer

Databehandleren skal etablere rutiner for å slette informasjon når lagring av den ikke lenger er nødvendig ut fra formålet med behandlingen.

C.5 Lokasjon for behandling

Behandling av personopplysninger som omfattes av Vilklårene 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 BENYTTER ADRESSEN]

Denne teksten vil bli fylt inn før kontraktssignering, basert på tilbudet fra leverandøren.

C.6 Instruks for overføring av personopplysninger til tredjeland

Eventuell overføring av personopplysninger til tredjeland skal skje i samsvar med SSA-L punkt 6.2.

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

Behandlingsansvarlig kan til enhver tid kreve innsyn i Databehandlers behandling av personopplysninger som tilhører Behandlingsansvarlig, herunder i dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Databehandlers system for internkontroll. Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen av opplysningene som utføres av Databehandler på vegne av Behandlingsansvarlig, og øvrige innsynsrettigheter nedfelt i lov.

Behandlingsansvarlig skal så vidt mulig gi Databehandler varsel i rimelig tid før krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Behandlingsansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere behandlingsansvarlige som får levert tjenester fra databehandler. Innsyn og kontroll kan gjennomføres av Behandlingsansvarlig eller den tredjepart

behandlingsansvarlige måtte velge til gjennomføring. Databehandler kan kreve dekket dokumenterte merknader som påløper ved slike revisjoner.

Side 15 av 16

Databehandler plikter å gi Datatilsynet og annen relevant tilsynsmyndighet slik tilgang og innsyn i behandlingen av personopplysninger som følger av personopplysningsloven. Databehandleren skal legge til rette for slik informasjonsdeling.

Databehandler skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Databehandler eller dennes underleverandører skal korrigeres uten kostnad for Behandlingsansvarlig. Databehandler skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

Den behandlingsansvarlige kan når som helst, likevel ikke oftere enn én gang per år, innhente en revisjonsrapport om databehandlerens overholdelse av vilkårene i SSA-L med vedlegg, inkludert denne databehandleravtalen. Kostnadene til en slik rapportinnhenting bæres av den behandlingsansvarlige. Databehandleren bærer sine interne kostnader.

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.

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

Reglene i C.7 skal gjelde tilsvarende for eventuelle underdatabehandlere. Databehandleren er ansvarlig for å sikre at alle underdatabehandlere aksepterer vilkårene.

