# Databehandleravtale

## Standardkontraktsbestemmelser

i henhold til artikkel 28(3) i forordning 2016/679 (personvernforordningen) med sikte på databehandlerens behandling av personopplysninger

mellom

**Techems kunde**

Heretter "Kunden" eller "behandlingsansvarlig"

og

**Techem Norge AS**
Organisasjonsnummer: 992 327 669
Dicks vei 10B
1366 Lysaker
Norge

Heretter "databehandleren"

som hver er en "part" og til sammen utgjør "partene"

HAR GODTATT følgende standardkontraktsbestemmelser ("Bestemmelsene") for å overholde personvernforordningen og sikre beskyttelse av personvern og grunnleggende rettigheter og friheter for fysiske personer.

techem

## 1. Innholdsfortegnelse

## 2. Innledningen

1. Disse Bestemmelsene fastsetter databehandlerens rettigheter og plikter ved behandling av personopplysninger på vegne av behandlingsansvarlig.

2. Disse Bestemmelsene er utformet for å ivareta partenes overholdelse av artikkel 28 nr. 3 i europaparlaments- og rådsforordning (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, og oppheving av direktiv 95/46/EF (personvernforordning).

3. I forbindelse med levering av tjenester og leveranser til behandlingsansvarlig, herunder administrasjon og levering av forbruksregnskap og/eller forbruksdata inkludert data fra sensorer, behandler databehandleren personopplysninger på vegne av behandlingsansvarlig i samsvar med disse bestemmelsene.

4. Bestemmelsene skal ha forrang over eventuelle lignende bestemmelser i andre avtaler mellom partene.

5. Det er fire vedlegg til disse Bestemmelsene, og vedleggene utgjør en integrert del av Bestemmelsene.

6. Vedlegg A inneholder detaljer om behandlingen av personopplysninger, inkludert formålet med og arten av behandlingen, typen personopplysninger, kategoriene av registrerte og varigheten av behandlingen.

7. Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som behandlingsansvarlig har godkjent bruken for.

8. Vedlegg C inneholder den behandlingsansvarliges instrukser vedrørende databehandlerens behandling av personopplysninger, en beskrivelse av sikkerhetstiltakene som databehandleren minst må iverksette og hvordan databehandleren og eventuelle underdatabehandlere skal overvåkes.

9. Vedlegg D inneholder bestemmelser om annen virksomhet som ikke omfattes av bestemmelsene.

10. Bestemmelsene og vedleggene skal oppbevares skriftlig, herunder elektronisk, av begge parter.

11. Disse Bestemmelsene fritar ikke databehandleren fra forpliktelser som pålegges databehandleren i henhold til personvernforordningen eller annen lovgivning.

## 3. Databehandlerens rettigheter og plikter

1. Databehandleren er ansvarlig for at behandlingen av personopplysninger utføres i samsvar med personvernforordningen (se forordningens artikkel 24), databeskyttelsesbestemmelser i annen EU- eller medlemsstatslov[1] og disse Bestemmelsene.

2. Databehandleren har rett og plikt til å ta avgjørelser om formålet/midlene for behandling av personopplysninger.

3. Databehandleren er blant annet ansvarlig for at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger, som databehandleren er pålagt å utføre.

1 Henvisninger til «medlemsstat» i disse bestemmelsene skal tolkes som en henvisning til «EØS-medlemsstater».

## 4. Databehandleren handler i henhold til instruks

1. Databehandleren kan behandle personopplysninger bare etter dokumenterte instruksjoner fra den behandlingsansvarlig, med mindre det kreves av unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Denne instruksjonen skal spesifiseres i vedlegg A og C. Senere instruksjoner kan også gis av den behandlingsansvarlig mens personopplysninger behandles, men instruksjonen må alltid dokumenteres og lagres skriftlig, inkludert elektronisk, sammen med disse Bestemmelsene.

2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom databehandleren mener at en instruks er i strid med denne forordning eller bestemmelser om vern av personopplysninger i annet unionsrett eller medlemsstatenes nasjonale rett.

## 5. Konfidensialitet

1. Databehandleren kan bare gi tilgang til personopplysninger behandlet på vegne av behandlingsansvarlig til personer som er underlagt databehandlerens instruksjonsmyndighet, som har forpliktet seg til taushetsplikt eller er underlagt en passende lovbestemt taushetsplikt, og bare i den grad det er nødvendig. Listen over personer som har fått innsyn må gjennomgås fortløpende. På bakgrunn av denne gjennomgangen kan tilgangen til personopplysninger bli stengt dersom tilgangen ikke lenger er nødvendig og personopplysningene ikke lenger skal være tilgjengelige for disse personene.

2. På forespørsel fra den behandlingsansvarlige må databehandleren kunne påvise at de berørte personene, som er underlagt databehandlerens instruksjonsmyndighet, er underlagt ovennevnte taushetsplikt.

## 6. Behandlingssikkerhet

1. Artikkel 32 i personvernforordningen fastslår at den behandlingsansvarlige og databehandleren, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og arten, omfanget, sammenhengen og formålet med den aktuelle behandlingen, samt risikoene med varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter, gjennomfører egnede tekniske og organisatoriske tiltak for å sikre et beskyttelsesnivå som er passende for disse risikoene.

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

   a. Pseudonymisering og kryptering av personopplysninger

   b. evne til å sikre pågående konfidensialitet, integritet, tilgjengelighet og robusthet av behandlingssystemer og tjenester

   c. evne til å gjenopprette tilgjengeligheten av og tilgangen til personopplysninger i tide i tilfelle en fysisk eller teknisk hendelse

   d. en framgangsmåte for regelmessig testing, vurdering og evaluering av effektiviteten av tekniske og organisatoriske tiltak for å ivareta behandlingens sikkerhet

2. I henhold til forordningens artikkel 32 må databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter som behandlingen utgjør, og iverksette tiltak for å håndtere disse risikoene. I denne vurderingen skal den behandlingsansvarlige gi databehandleren nødvendig informasjon slik at databehandleren kan identifisere og vurdere slike risikoer.

3. I tillegg skal databehandleren bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges forpliktelser i henhold til forordningens artikkel 32, blant annet ved å gjøre tilgjengelig for behandlingsansvarlig nødvendig informasjon om de tekniske og organisatoriske sikkerhetstiltakene som allerede er implementert av databehandleren i henhold til forordningens artikkel 32, og all annen informasjon som er nødvendig for at den behandlingsansvarlige skal overholde sine forpliktelser i henhold til forordningens artikkel 32 forordningen artikkel 32.

   Dersom det å redusere de identifiserte risikoene etter den behandlingsansvarliges oppfatning krever implementering av ytterligere tiltak enn de som allerede er implementert av databehandleren, skal behandlingsansvarlig spesifisere ytterligere tiltak som skal implementeres i vedlegg C.

## 7. Bruk av underdatabehandlere

1. Databehandleren må oppfylle vilkårene nevnt i personvernforordningens artikkel 28(2) og (4) for å kunne benytte seg av en annen databehandler (en underdatabehandler).

2. Databehandleren kan derfor ikke bruke en underdatabehandler til å overholde disse Bestemmelsene uten forutgående generell skriftlig godkjenning fra behandlingsansvarlig.

3. Databehandleren har den behandlingsansvarliges generelle godkjenning for bruk av underdatabehandlere. Databehandleren må varsle behandlingsansvarlig skriftlig om eventuelle planlagte endringer angående tillegg eller utskifting av underdatabehandlere med minst 1 måneds varsel, og dermed gi behandlingsansvarlig mulighet til å motsette seg slike endringer før bruk av de(n) aktuelle underdatabehandleren(e). Lengre varsel for varsling i forbindelse med spesifikke behandlingsaktiviteter kan spesifiseres i vedlegg B. Listen over underdatabehandlere som allerede er godkjent av behandlingsansvarlig, er angitt i vedlegg B.

4. Dersom databehandleren benytter en underdatabehandler i forbindelse med utføring av særlige behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal databehandleren ved hjelp av en avtale eller et annet rettslig tiltak i henhold til unionsretten eller medlemsstatenes nasjonale rett pålegge underbehandleren de samme personvernforpliktelsene som er fastsatt i disse Bestemmelsene, og særlig sørge for nødvendige garantier for at underdatabehandleren skal gjennomføre de tekniske og organisatoriske tiltakene på en slik måte at behandlingen er i samsvar med kravene i disse Bestemmelsene og personvernforordningen.

   Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som et minimum overholder databehandlerens forpliktelser i henhold til disse Bestemmelsene og personvernforordningen.

5. Underdatabehandleravtale(r) og eventuelle senere endringer av disse sendes – på den behandlingsansvarliges anmodning – på kopi til behandlingsansvarlig, som dermed har mulighet til å sikre at tilsvarende databeskyttelsesforpliktelser som følger av disse bestemmelsene, pålegges underdatabehandleren. Bestemmelser om kommersielle vilkår som ikke påvirker personverninnholdet i underdatabehandleravtalen, skal ikke sendes til behandlingsansvarlig.

6. I avtalen med underdatabehandleren må databehandleren inkludere behandlingsansvarlig som begunstiget tredjepart i tilfelle databehandlerens konkurs, slik at behandlingsansvarlig kan overta databehandlerens rettigheter og håndheve dem mot underdatabehandlere, som f.eks. gjør det mulig for behandlingsansvarlig å instruere underdatabehandleren om å slette eller returnere person-opplysningene.

7. Hvis underdatabehandleren ikke oppfyller sine databeskyttelsesforpliktelser, forblir databehandleren fullt ansvarlig overfor behandlingsansvarlig for oppfyllelsen av underdatabehandlerens forpliktelser. Dette berører ikke de registrertes rettigheter som følger av personvernforordningen, særlig artikkel 79 og 82 i nevnte forordning, overfor behandlingsansvarlig og databehandler, herunder underdatabehandleren.

## 8. Overførsel til tredjeland eller internasjonale organisasjoner

1. Enhver overføring av personopplysninger til tredjeland eller internasjonale organisasjoner kan bare utføres av databehandleren på grunnlag av dokumenterte instruksjoner fra behandlingsansvarlig og skal alltid skje i samsvar med kapittel V i personvernforordningen.

2. Dersom overføring av personopplysninger til tredjeland eller internasjonale organisasjoner som databehandleren ikke er instruert om å utføre av den behandlingsansvarlige, kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om dette rettslige kravet før behandlingen, med mindre nevnte lov forbyr slik underretning av hensyn til viktige allmenne interesser.

3. Således, uten dokumenterte instruksjoner fra behandlingsansvarlig, kan databehandleren ikke, innenfor rammen av disse Bestemmelsene:

    a. overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon;
    b. overlate behandlingen av personopplysninger til en underbehandler i et tredjeland
    c. behandle personopplysningene i et tredjeland

4. Den behandlingsansvarliges instruksjoner om overføring av personopplysninger til et tredjeland, herunder det mulige overføringsgrunnlaget i kapittel V i personvernforordningen som overføringen er basert på, skal spesifiseres i vedlegg C.6.

5. Disse Bestemmelsene må ikke forveksles med standardkontraktsbestemmelser i som er omtalt i personvernforordningen artikkel 46 avsnitt 2, bokstav c og d. Disse Bestemmelsene kan heller ikke danne grunnlag for overføring av personopplysninger som omhandlet i personvernforordningen kapittel V.

## 9. Bistand til databehandleren

1. Databehandleren bistår, med hensyn til behandlingens art, så langt det er mulig, den behandlingsansvarlige ved å ta i bruk passende tekniske og organisatoriske tiltak for å oppfylle den behandlingsansvarliges forpliktelse til å svare på forespørsler om utøvelse av registrertes rettigheter, som fastsatt i personvernforordningens kapittel III.

Dette innebærer at databehandleren skal, så langt det er mulig, bistå behandlingsansvarlig i forbindelse med at behandlingsansvarlig sikrer etterlevelse av:

a. plikten til å gi informasjon når personopplysninger samles inn fra den registrerte
b. plikten til å gi informasjon dersom personopplysninger ikke er samlet inn fra den registrerte
c. retten til innsyn
d. retten til korrigering
e. retten til sletting ("retten til å bli glemt")
f. retten til begrensning av behandling
g. meldeplikt 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 underlagt en beslutning basert utelukkende på automatisert behandling, inkludert profilering

2. I tillegg til databehandlerens forpliktelse til å bistå behandlingsansvarlig i samsvar med Bestemmelse 6.3., skal databehandleren også, under hensyntagen til behandlingens art og informasjonen som er tilgjengelig for databehandleren, bistå behandlingsansvarlig med:

   a. den behandlingsansvarliges plikt til å varsle bruddet på personopplysninger til den kompetente tilsynsmyndigheten, Datatilsynet, uten unødig forsinkelse og, om mulig, senest 72 timer etter å ha blitt klar over det, med mindre det er usannsynlig at bruddet på personopplysninger medfører en risiko for fysiske personers rettigheter eller friheter

   b. den behandlingsansvarliges plikt til uten unødig forsinkelse å underrette den registrerte om brudd på personopplysningssikkerheten dersom bruddet sannsynligvis vil medføre en høy risiko for fysiske personers rettigheter og friheter

   c. den behandlingsansvarliges plikt til før behandlingen å foreta en analyse av virkningen av de tiltenkte behandlingsaktivitetene på vernet av personopplysninger (en konsekvensanalyse)

   d. den behandlingsansvarliges plikt til å konsultere den kompetente tilsynsmyndigheten, Datatilsynet, før behandling, dersom en vurdering av personvernkonsekvenser viser at behandlingen vil føre til høy risiko i fravær av tiltak fra den behandlingsansvarlige for å begrense risikoen.

3. Partene skal i vedlegg C angi de nødvendige tekniske og organisatoriske tiltakene der databehandleren skal bistå den behandlingsansvarlige, samt i hvilken grad og omfang dette gjelder for forpliktelsene i henhold til Bestemmelse 9.1 og 9.2.

## 10. Varsling om brudd på personopplysningssikkerheten

1. Databehandleren informerer behandlingsansvarlig uten ugrunnet opphold etter å ha blitt kjent med at det har skjedd et brudd på personopplysningssikkerheten.

2. Databehandlerens varsling til behandlingsansvarlig skal om mulig skje senest 48 timer etter at behandlingsansvarlig har fått kjennskap til bruddet, slik at behandlingsansvarlig kan overholde sin plikt til å rapportere bruddet til kompetent tilsynsmyndighet, jf. personvernforordningen artikkel 33.

3. I samsvar med Bestemmelse 9.2.a skal databehandleren bistå behandlingsansvarlig med å varsle om bruddet til kompetent tilsynsmyndighet. Dette betyr at databehandleren skal bistå med å gi følgende informasjon, som i henhold til artikkel 33, avsnitt 3 skal fremgå av den behandlingsansvarliges melding om bruddet til den kompetente tilsynsmyndigheten:

    a. arten av bruddet på personopplysningssikkerheten, herunder, der det er mulig, kategoriene og omtrentlig antall berørte registrerte samt kategoriene og omtrentlig antall berørte personopplysninger

    b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten

    c. de tiltak som er truffet eller foreslått truffet av den behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten, herunder, der det er hensiktsmessig, tiltak for å begrense de mulige skadevirkningene.

4. Partene skal spesifisere i vedlegg C informasjonen som databehandleren må gi i forbindelse med sin bistand til behandlingsansvarlig i sin forpliktelse til å varsle brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

## 11. Sletting og tilbakelevering av informasjon

1. Ved opphør av tjenestene vedrørende behandling av personopplysninger er databehandleren forpliktet til å slette eller anonymisere alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige, og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet eller anonymisert, med mindre unionsretten eller medlemsstatenes nasjonale rett tillater lagring av personopplysningene.

## 12. Revisjon, herunder inspeksjon

1. Databehandleren stiller til rådighet for behandlingsansvarlig all informasjon som er nødvendig for å påvise overholdelse av artikkel 28 i personvernforordningen og disse Bestemmelsene, og tillater og bidrar til revisjoner, herunder inspeksjoner, som utføres av behandlingsansvarlig eller annen revisor som er autorisert av behandlingsansvarlig.

2. Prosedyrene for revisjoner, inkludert inspeksjoner, av behandlingsansvarlig med databehandleren og underdatabehandlere er spesifisert i vedlegg C.7. og C.8.

3. Databehandleren er forpliktet til å gi tilsynsmyndigheter som i henhold til gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens fasiliteter, eller representanter som opptrer på vegne av tilsynsmyndigheten, tilgang til databehandlerens fysiske fasiliteter mot korrekt identifisering.

## 13. Partenes avtale om andre forhold

1. Partene kan avtale andre bestemmelser knyttet til tjenesten om behandling av personopplysninger, for eksempel ansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte er i strid med Bestemmelsene eller svekker den registrertes grunnleggende rettigheter og friheter som følge av personvernforordningen.

## 14. Ikrafttredelse og oppsigelse

1. Bestemmelsene trer i kraft på datoen da begge parter signerer tjenesteavtalen.

2. Hver av partene kan kreve at Bestemmelsene reforhandles dersom lovendringer eller hensiktsmessighet av Bestemmelsene fører til dette.

3. Bestemmelsene gjelder så lenge tjenesten knyttet til behandling av personopplysninger pågår. I denne perioden kan Bestemmelsene ikke sies opp, med mindre andre bestemmelser som regulerer levering av tjenesten knyttet til behandling av personopplysninger, avtales mellom partene.

4. Hvis leveransen av tjenestene knyttet til behandling av personopplysninger avsluttes, og personopplysningene er slettet eller returnert til den behandlingsansvarlige i samsvar med Bestemmelse 11.1 og Vedlegg C.4, kan Bestemmelsene sies opp med skriftlig varsel fra begge parter.

## 15. Kontaktpersoner hos behandlingsansvarlig og databehandler

1. Partene kan kontakte hverandre via kontaktpersoner som er nærmere avtalt mellom dem.

Versjon: Januar 2024

## Vedlegg A Informasjon om behandlingen

### A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig

Levering av tjenester og leveranser, som nærmere definert ved avtale mellom partene, inkluderer administrasjon og levering av forbruksregnskaper og/eller forbruksdata, inkludert data fra ulike sensorer i spesifikke eiendommer. Dette omfatter også kontinuerlig service, vedlikehold og utvikling av våre systemer, inkludert bruk av data som testdata.

Administrasjonen inkluderer blant annet avlesning av forbruk, inngåelse av avtaleperioder i forbindelse med service og avlesning, flytteavlesninger, utarbeidelse av forbruksregnskaper og håndtering av innsigelser.

### A.2. Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig gjelder først og fremst (behandlingens art)

Behandlingen av personopplysninger vil utgjøre innsamling, registrering, organisering, organisering, systematisering, bruk, lagring, oppdatering, justering eller kombinering, begrensning, sletting eller ødeleggelse, utveksling av data (på vegne av og etter instruks fra den behandlingsansvarlige).

### A.3. Behandlingen inkluderer følgende typer personopplysninger om de registrerte

Behandlingen omfatter generelle personopplysninger, som beboerens navn, adresse, telefonnummer, beboerens identifikasjonsnummer, botid og informasjon om utflytting, herunder innflyttingsadresse, inneklimaparametere, data fra ulike sensorer, beboerens energi- og vannforbruk inkludert forbruksmønster, e-postadresse, registrering av personlig tilstedeværelse eller manglende tilstedeværelse i eiendommen i forbindelse med avlesning.

### A.4. Behandlingen omfatter følgende kategorier av registrerte

Behandlingen omfatter nåværende og fraflyttede beboere i eiendommene som omfattes av avtalen mellom databehandleren og behandlingsansvarlig.

### A.5. Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig kan påbegynnes etter ikrafttredelsen av disse Bestemmelsene. Behandlingen har følgende varighet:

Behandlingen av personopplysninger på vegne av behandlingsansvarlig opphører når behandlingsansvarlig har trukket seg fra samarbeidet i samsvar med avtalen mellom databehandleren og behandlingsansvarlig, og når databehandleren har fått en klar instruks om å utføre sletting eller anonymisering.

## Vedlegg B Underdatabehandlere

### B.1. Godkjente underdatabehandlere

Ved Bestemmelsens ikrafttredelse har behandlingsansvarlig godkjent bruk av følgende underdatabehandlere

| NAVN | CVR | ADRESSE | BESKRIVELSE AV BEHANDLING |
|---|---|---|---|
| Techem Energy Service GmbH | | Haupstrasse 89, 65760 Eschborn, Tyskland | Behandling av alle data i forbindelse med utarbeidelse av forbruksregnskap. |
| Techem Danmark A/S | 29 41 69 82 | Trindsøvej 7 A-B, 8000 Aarhus C Danmark | Delt servicesenter. |
| Hetzner Online GmbH | | Bransjertr. 25, 91710 Gunzenhausen | Behandling av generelle personopplysninger i forbindelse med levering av web- og database-servertjenester, inkludert nettsted, APIer og GraphQL. |
| Stoked ApS | 36068469 | Mejlgade 80, 5 DK-8000 Aarhus C | Behandling av generelle personopplysninger i forbindelse med ytelse av utviklingstjenester, herunder portalutvikling. |
| Mailjet | | 4, rue Jules Lefebre 75009 Paris | Håndtere e-post fra portal til administrator og/eller beboer. |
| Techem France Siège Social Techem Paris | | Batiment Mikadoz 378/380 Avenue de la Division Leclerc 92290 Chateney-Malabry (Paris) | Behandling av data fra fjernavleste målere, samt bygningsstamdata |
| Podio | | Kalkbrænderiløbskaj 4, 2100 København Danmark | Planlegging av installasjonsoppgaver Behandling og innsamling av generelle personopplysninger i forbindelse med tjenesteytelser. |

Ved ikrafttreden av Bestemmelsene har den behandlingsansvarlige godkjent bruken av de nevnte underdatabehandlerne for den beskrevne behandlingsaktiviteten. Databehandleren kan ikke, uten skriftlig varsel til den behandlingsansvarlige med minst 1 måneds varsel, benytte en underdatabehandler for en annen behandlingsaktivitet enn den som er beskrevet og avtalt, eller benytte en annen underdatabehandler for denne behandlingsaktiviteten.

**B.2. Varsel for godkjenning av underdatabehandlere**

Se punkt 7.3.

## Vedlegg C Instruks vedrørende behandling av personopplysninger

### C.1. Gjenstand/instruksjoner for behandlingen

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig skjer ved at databehandleren foretar avlesninger og utarbeider fordelingsregnskap og/eller forbruksdata etter nærmere avtale med behandlingsansvarlig.

### C.2. Sikkerhet ved behandling

Sikkerhetsnivået skal gjenspeile at behandlingen involverer vanlige personopplysninger for et stort antall registrerte.

Databehandleren må imidlertid - i alle fall og som et minimum - gjennomføre følgende tiltak som er avtalt med behandlingsansvarlig:

*Operativ sikkerhet*

Databehandleren skal sikre:

i) at det nødvendige og tilstrekkelige sikkerhetsnivået vedlikeholdes og opprettholdes, og at eventuelle endringer i databehandlerens sikkerhetstiltak som er relevante for personopplysningene, loggføres og dokumenteres,
ii) at endringer og vedlikehold av databehandlerens sikkerhetstiltak så langt det er mulig ikke påvirker den behandlingsansvarliges virksomhet, herunder - men ikke begrenset til - IT-systemer, nettverk, tilkoblinger og responstider,
iii) at databehandlerens eventuelle testmiljøer er tilstrekkelig avgrenset og på annen måte sikret mot uautorisert tilgang,
iv) at databehandlerens IT-systemer og nettverk er tilstrekkelig sikret mot hacking og annen uautorisert tilgang,
v) at databehandleren utfører kontroller for å avdekke og forhindre uautorisert tilgang, skadevare mv., og
vi) at de interne operasjonelle sikkerhetsprosedyrene og håndbøkene følges.

*Konfidensialitet*

Databehandleren skal gjennomføre tiltakene og prosessene som er oppført nedenfor:

i) Sikre bruk av rollebasert tilgangskontroll og pålogging til deler av personopplysninger (inkludert mulighet for oppfølging/justering av rollebasert tilgangskontroll) og at kun autoriserte enheter og relevante ansatte med arbeidsrelaterte databehandlingsbehov har tilgang til personopplysninger.
ii) Sørg for at ansatte, når de bytter jobb, ikke beholder tilgang til midlene de trengte i sine tidligere jobber. Når ansatte sier opp, må man passe på at de ikke tar med seg forretningskritisk informasjon. Det må sikres at ingen tidligere ansatte eller eksterne konsulenter har tilgangsrettigheter til systemene som inneholder personopplysninger. Tilgangsrettigheter for eiere av systemer eller tjenester må også vurderes fortløpende.
iii) Sikre bruk av pseudonymisering og kryptering av personopplysninger der det er mulig og lovpålagt.
iv) Bruke sikre/krypterte overføringer av personopplysninger på det åpne internett når personopplysningene som overføres ikke er ment for offentligheten.
v) Databehandleren skal sikre at enhver person som utfører arbeid for databehandleren og får tilgang til personopplysningene, bare skal behandle slike opplysninger etter instruks fra den behandlingsansvarlige, med mindre behandlingen kreves av unionsretten eller nasjonal lovgivning i EØS-statene.
vi) Databehandling kan bare gjøres på PC-er med en nødvendig VPN-tilkobling med sterk autentisert kryptering (AES 256 bit), inkludert å sikre at brannmur og bruker er beskyttet av tofaktorautentisering. Hvis mobile medier brukes, må disse beskyttes av MDM (Mobile Device Management).

I tillegg skal databehandleren sikre sine fysiske lokaler, servere mv. mot uautorisert tilgang ved å:

i) ha interne sikkerhetsprosedyrer for å sikre, ved fjerning, avhending eller gjenbruk av maskinvare, at personopplysningene til den behandlingsansvarlige ikke kompromitteres
ii) installere passende låser eller andre fysiske kontroller på dører og vinduer i rom der datamaskiner er lagret
iii) fysisk sikre bærbare datamaskiner uten tilsyn (f.eks. ved å låse dem i en sikker skuff eller et skap)
iv) sikre kontroll og beskyttelse av alle mobile medier, for eksempel flyttbare harddisker, CD-er og USB-pinner som inneholder personopplysninger
v) ødelegge eller fjerne alle personopplysninger fra medier, for eksempel USB-minnepinner, mobile medier og CD-er, før de kastes og
vi) forsikre deg om at alle personlige data fjernes fra harddiskene på servere og datamaskiner før de kastes.

*Sikkerhetskopi*
Databehandleren må sikkerhetskopiere innsamlede data minst én gang daglig. Sikkerhetskopioverføringen må være kryptert. Sikkerhetskopiering må lagres separat fra produksjonsdata i henhold til samme sikkerhetsnivå som produksjonsdata.

*Adgangskontroll*
Databehandler må ha rutiner for passord på plass, herunder bruk av sterke passord, to faktorautentisering, periodisk oppdatering av passord og påse at ansatte ikke skriver dem ned.

*Logging*
Databehandler skal logge mislykkede innloggingsforsøk, herunder logging av tid, bruker etc. og sperre tilgang etter et visst antall mislykkede påloggingsforsøk for hver bruker.

Databehandler skal logge brukeraktiviteter, herunder all bruk av brukerinformasjon, dvs. logging av tid, bruker, søk, søkekriterier, tilgang, endring, lukking, utskrift, eksport, sletting etc. og automatisk sletting av logg etter et visst tidsintervall.

*Integritet og tilgjengelighet*
Databehandleren skal gjennomføre følgende tiltak og prosesser:

i) Beskytt nettverk, systemer, logger og personopplysninger mot manipulering.
ii) Sikre muligheten til å gjenopprette tilgjengeligheten av og tilgangen til personopplysninger i tide i tilfelle en fysisk eller teknisk hendelse, inkludert ved å sikkerhetskopiere data.

*Motstandsdyktighet*
Databehandleren skal ha et sårbarhetshåndteringsprogram, inkludert kontinuerlig overvåking av potensielle sårbarheter og gjennomføring av penetrasjonstester på nettverk og systemer som brukes til behandling av personopplysninger.

Programmet for sårbarhetshåndtering må inkludere, men er ikke begrenset til:

i) Å utføre sårbarhetsskanninger på interne og eksterne områder minst kvartalsvis
ii) Å gjennomføre penetrasjonstester på eksterne nettverk minst kvartalsvis eller oftere i tilfelle hendelser som viser behovet for det
iii) For å følge opp og rette opp eventuelle svakheter som er identifisert under slike skanninger og tester

Databehandler skal kontinuerlig holde nettverk og systemer oppdatert med nye versjoner, oppdateringer og oppdateringer.

*Sikkerhets- og datasikkerhetsteknologier*
Databehandleren skal gjennomføre tiltakene og prosessene som er oppført nedenfor:

Kontroller at alle datamaskiner og servere som brukes, har antivirus- eller antimalware-programvare installert, og at virusdefinisjoner oppdateres minst én gang i uken. All innkommende og utgående trafikk må skannes for virus, samt eventuelle brukte disker eller flyttbare medier. Datamaskiner og servere må skannes for virus minst en gang i uken.

Hvis datamaskiner og servere er koblet til Internett, bør de være bak en installert brannmur, helst en neste generasjons brannmur, og Internett-tilkoblinger bør beskyttes av anti-DDOS-beskyttelse, samt dekkes av et overvåkingssystem.

Systemer som oppbevarer, lagrer eller på annen måte behandler personopplysninger, skal testes minst en gang i året med sårbarhetsskanning og penetrasjonstesting.

*Bevisstgjøring, opplæring og sikkerhetskontroll i forhold til ansatte*
Databehandleren skal gjennomføre tiltakene og prosessene som er oppført nedenfor:

i) Utfør integritetskontroller på alle nye ansatte for å verifisere informasjonen som ansatte gir, om deres bakgrunn, erfaring eller kvalifikasjoner er riktige. Likeledes må databehandleren ha en hensiktsmessig prosedyre for innhenting av rent rulleblad for teknikere som kommer til private hjem og forretningslokaler. I tillegg må det gjennomføres årlige stikkprøver.
ii) Introduser ansatte (nye så vel som nåværende) til informasjonssikkerhet, og sørg for at de leser og forstår informasjonssikkerhetspolitikken. Det må sikres at de ansatte kontinuerlig vet hvor de kan finne informasjon om standarder og prosedyrer for informasjonssikkerhet som er relevante for deres rolle og ansvar.

*Hendelseshåndtering og forretningskontinuitet*
Databehandleren skal gjennomføre tiltakene og prosessene som er oppført nedenfor:

i) Opplæring av ansatte, inkludert ansattes forståelse av brudd på personopplysninger, sikkerhets-hendelser samt skilt og hensiktsmessige reaksjoner på henholdsvis brudd og sikkerhetshendelser. En sikkerhetshendelse er enhver hendelse som kan skade eller kompromittere konfidensialiteten, integriteten eller tilgjengeligheten til forretningskritisk informasjon eller systemer.
ii) Databehandleren må ha en plan på plass for å sikre forretningskontinuitet i tilfelle en alvorlig sikkerhets-hendelse og må teste planen minst en gang i året. Etter en hendelse eller prøvinger der planen anvendes, skal den gjennomgås og ajourføres.

*Revisjon*
Databehandler skal overvåke og sikre oppdatering av alle tiltak, prosesser og risikoanalyser.

Databehandleren skal implementere en prosedyre for regelmessig testing, vurdering og evaluering av effektiviteten av de tekniske og organisatoriske tiltakene for å sikre behandlingssikkerheten, inkludert, men ikke begrenset til, tiltakene som er angitt her.

Databehandler skal implementere prosedyrer for effektiv oppfølging av manglende overholdelse.

Revisjon skal finne sted minst én gang i året.

*Myndigheter*
Databehandleren samarbeider på forespørsel med Datatilsynet og eventuelle andre tilsynsmyndigheter i forbindelse med utførelsen av oppgavene til slike tilsynsmyndigheter. Databehandleren har rett til å gi Datatilsynet tilgang til alle personopplysninger og opplysninger som er nødvendige for å utføre oppgavene til Datatilsynet.

Databehandleren tar de nødvendige forholdsregler for å sikre overholdelse av en beslutning fra Datatilsynet. På vegne av den behandlingsansvarlige informerer databehandleren Datatilsynet om tiltakene som er truffet for å overholde beslutningen.

Hvis Datatilsynet utsteder en ordre til databehandleren, må databehandleren overholde et slikt pålegg i samsvar med den angitte måten og innen den angitte fristen.

**C.3 Bistand til den behandlingsansvarlige**
Databehandleren har den behandlingsansvarliges generelle godkjenning til å bistå behandlingsansvarlig med dens forpliktelser i henhold til disse Bestemmelsene, herunder i forhold til de registrertes rettigheter, utarbeidelse av vurderinger av personvernkonsekvenser og bistand i forbindelse med forutgående konsultasjon med Datatilsynet.

**C.4 Lagringsperiode/sletterutiner**
Databehandleren må slette personopplysningene etter 5 år etter 6 uker etter innsigelsesfristen for hver finansrapport.

Ved opphør av tjenesten vedrørende behandling av personopplysninger skal databehandleren enten slette eller anonymisere personopplysningene i samsvar med bestemmelse 11.1, med mindre behandlingsansvarlig – etter ikrafttredelsen av disse bestemmelsene – har endret den behandlingsansvarliges opprinnelige valg. Slike endringer skal dokumenteres og lagres skriftlig, herunder elektronisk, i forbindelse med Bestemmelsene.

**C.5 Lokalitet for behandling**
Personopplysninger som omfattes av bestemmelsene kan ikke behandles uten skriftlig og forutgående varsel fra behandlingsansvarlig på andre steder enn de som er angitt i vedlegg B.1.

**C.6 Instruks om overføring av personopplysninger til tredjeland**
Databehandleren og de godkjente underdatabehandlerne, jf. vedlegg B.1, overfører ikke personopplysninger til tredjeland.

Ved stedsendring for databehandlerens behandling av personopplysninger, som vil medføre overføring til usikre tredjeland, plikter databehandleren å informere behandlingsansvarlig skriftlig med minst 3 måneders skriftlig varsel, og dermed gi behandlingsansvarlig mulighet til å protestere mot overføringen, jf. vedlegg C.5.

Dersom den behandlingsansvarlige ikke gir dokumenterte instrukser i disse Bestemmelsene eller senere om overføring av personopplysninger til et tredjeland, har databehandleren ikke rett til å foreta slike overføringer innenfor rammen av disse Bestemmelsene.

**C.7 Prosedyrer for revisjoner, herunder inspeksjoner, utført av behandlingsansvarlig for behandling av personopplysninger som er betrodd databehandleren**

Den behandlingsansvarlige eller en representant for den behandlingsansvarlige kan be om skriftlig bekreftelse eller gjennomføre en fysisk inspeksjon av lokalene der databehandleren behandler personopplysninger, herunder fysiske lokaler og systemer som brukes til eller i forbindelse med behandlingen, for å fastslå databehandlerens overholdelse av personvernforordningen, bestemmelser om vern av personopplysninger i annen unionsrett eller medlemsstatsrett og disse Bestemmelsene.

I tillegg til det planlagte tilsynet kan den behandlingsansvarlige gjennomføre et skriftlig tilsyn eller en inspeksjon hos databehandleren når den behandlingsansvarlige anser det som nødvendig.

Eventuelle utgifter som den behandlingsansvarlige pådrar seg i forbindelse med en fysisk inspeksjon, skal bæres av den behandlingsansvarlige selv. Databehandleren er imidlertid forpliktet til å allokere ressursene (hovedsakelig tiden) som er nødvendige for at behandlingsansvarlig skal kunne utføre sin inspeksjon.

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

Den behandlingsansvarlige kan – dersom det anses nødvendig – velge å iverksette og delta i en fysisk inspeksjon hos underdatabehandleren. Dette kan bli relevant dersom den behandlingsansvarlige vurderer at databehandlerens inspeksjon av underdatabehandleren ikke har gitt behandlingsansvarlig tilstrekkelig sikkerhet for at behandlingen av underdatabehandleren finner sted i samsvar med personvernforordningen, databeskyttelsesbestemmelser i annen EU-lov eller medlemsstatenes nasjonale lovgivning og disse Bestemmelsene.

Den behandlingsansvarliges deltakelse i en inspeksjon av underdatabehandleren endrer ikke det faktum at databehandleren fortsatt er fullt ut ansvarlig for underdatabehandlerens overholdelse av personvernforordningen, databeskyttelsesbestemmelser i annen EU-lov eller medlemsstatenes nasjonale lovgivning og disse Bestemmelsene.

## Vedlegg D Partenes regulering av andre forhold

-