Databehandleraftale

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Techems kunde

herefter "kunden" eller "den dataansvarlige"

og

Techem Danmark A/S
CVR 29 41 69 82
Trindsøvej 7 A-B
8000 Aarhus C
Danmark

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

techem

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af tjenesteydelser og leverancer til den dataansvarlige, herunder administration og levering af forbrugsregnskaber og/eller forbrugsdata inklusiv data fra sensorer, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

   c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

   d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 1 måneds varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. indsigtsretten
    d. retten til berigtigelse
    e. retten til sletning (”retten til at blive glemt”)
    f. retten til begrænsning af behandling
    g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
    h. retten til dataportabilitet
    i. retten til indsigelse
    j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

    a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

    b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

    c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

    d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente myndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette eller anonymisere alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet eller anonymiseret, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft når instruks er givet.

2. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

3. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via kontaktpersoner som aftalt nærmere mellem dem.

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Levering af tjenesteydelser og leverancer som nærmere defineret ved aftale mellem parterne, herunder administration og levering af forbrugsregnskaber og/eller forbrugsdata inklusiv data fra diverse sensorer i nærmere bestemte ejendomme, herunder løbende service, vedligehold og udvikling af vores systemer, inklusiv anvendelse af data som testdata.

Administrationen omfatter blandt andet aflæsning af forbrug, indgåelse af aftaletider i forbindelse med service og aflæsning, flytteaflæsninger, udarbejdelse af forbrugsregnskaber og håndtering af indsigelser.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Karakteren af behandlingen for personoplysninger vil udgøre indsamling, registrering, organisering, systematisering, opbevaring, brug, lagring, opdatering, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse, udveksling af data (på vegne af og efter instruks fra den dataansvarlige).

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen omfatter almindelige personoplysninger, såsom beboerens navn, adresse, telefonnummer, beboeridentifikationsnummer, beboelsesperiode og oplysninger om fraflytning, herunder tilflytningsadresse, indeklimaparametre, data fra diverse sensorer, beboerens energi- og vandforbrug herunder forbrugsmønster, e-mailadresse, registrering af manglende tilstedeværelse i ejendommen i forbindelse med manuel aflæsning.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter nuværende og fraflyttede beboere i de ejendomme, som er omfattet af det aftalte mellem databehandleren og den dataansvarlige.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen af personoplysninger på vegne af den dataansvarlige ophører, når den dataansvarlige er udtrådt af samarbejdet i overensstemmelse med det aftalte mellem databehandleren og den dataansvarlige, samt når databehandleren har modtaget en entydig instruks om at foretage sletning eller anonymisering.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Techem Energy Service GmbH		Haupstrasse 89, 65760 Eschborn, Tyskland	Behandling af alle data ifm. produktion af forbrugsregnskaber
Techem Bulgaria		Proff Georgi Pavlov 3 11 Sofia Bulgarien	Produktion af fordelingsregnskaber,
Hetzner Online GmbH		Industriestr. 25, 91710 Gunzenhausen	Behandling af almindelige personoplysninger i forbindelse med levering af web og database serverydelser, herunder webside, API'er og GraphQL.
Stoked ApS	36068469	Mejlgade 80, 5 8000 Aarhus C	Behandling af almindelige personoplysninger i forbindelse med levering af udviklingsydelser, herunder portaludvikling.
Mailjet		4, rue Jules Lefebre 75009 Paris	Håndtering af emails 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 af data fra fjernaflæste målere, samt bygningsstamdata
Podio (kun i Norge)			Planlægning af installationsopgaver – kun for norske kunder

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarlige skriftligt er blevet underrettet med

mindst 1 måneds varsel – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Se punkt 7.3.

techem

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren foretager aflæsninger og udarbejder fordelingsregnskaber og/eller forbrugsdata som nærmere aftalt med den dataansvarlige.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen sker af almindelige personoplysninger for stort antal data subjekter.

Databehandleren skal dog - under alle omstændigheder og som minimum - gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Operationel sikkerhed

Databehandleren skal sikre:

i) at det nødvendige og tilstrækkelige sikkerhedsniveau vedligeholdes og opretholdes, samt at eventuelle ændringer i databehandlerens sikkerhedsforanstaltninger relevante for personoplysningerne logges og dokumenteres,
ii) at ændringer og vedligeholdelse af databehandlerens sikkerhedsforanstaltninger så vidt muligt ikke påvirker den dataansvarliges forretning, herunder - men ikke begrænset til - it-systemer, netværk, forbindelser og svartider,
iii) at databehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang,
iv) at databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,
v) at databehandleren gennemfører kontroller for at opdage og forhindre uautoriseret adgang, malware mv., og
vi) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges.

Fortrolighed

Databehandleren skal implementere de nedenfor anførte foranstaltninger og processer:

i) Sikre brug af rollebaseret adgangskontrol og login til sektioner med personoplysninger (herunder mulighed for opfølgning på/justering af rollebaseret adgangskontrol), og at kun autoriserede enheder og relevante medarbejdere med arbejdsrelateret behov for databehandling har adgang til personoplysninger.
ii) Sikre, at medarbejdere, ved jobskifte, ikke bevarer adgangen til de midler, som de skulle bruge i deres tidligere job. Når medarbejdere fratræder, skal der sørges for at de ikke tager forretningskritiske oplysninger med dem. Der skal sikres at ingen tidligere medarbejdere eller eksterne konsulenter har adgangsrettigheder til de systemer, der indeholder personoplysninger. Der skal også løbende gennemgås adgangsrettigheder til ejere af systemer eller tjenester.
iii) Sikre brug af pseudonymisering og kryptering af personoplysninger, hvor det er muligt og lovpligtigt.
iv) Benytte sikre/krypterede overførsler af personoplysninger på det åbne internet, når de overførte personoplysninger ikke er tiltænkt offentligheden.
v) Databehandleren skal sikre, at enhver person, der udfører arbejde for databehandleren og får adgang til personoplysningerne, kun behandler sådanne oplysninger efter den dataansvarliges instruks, medmindre behandlingen er påkrævet i henhold til EU-lovgivningen eller EØS-medlemsstaternes nationale lovgivning.
vi) Databehandling må kun foretages på Pc'er med en påkrævet VPN forbindelse med stærk godkendt kryptering (AES 256 bit) herunder skal det sikres at firewall og bruger er beskyttet af to faktor godkendelse. Benyttes mobile medier skal disse være beskyttet af MDM (mobile device management).

Databehandleren skal derudover sikre sine fysiske lokaliteter, servere mv. mod uautoriseret adgang ved at:

i) have interne sikkerhedsprocedurer, der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres,
ii) opsætte passende låse eller anden fysisk kontrol på døre og vinduer i rum, hvor der opbevares computere,
iii) fysisk sikre ubemandede bærbare computere (f.eks. ved at låse dem i en sikker skuffe eller et skab),

iv) sørge for kontrol og beskyttelse af alle mobile medier, f.eks. flytbare harddiske, CD'er og USB-stik, der indeholder personoplysninger,
v) tilintetgøre eller fjerne alle personoplysninger fra medier, som f.eks. USB-stik, mobile medier og CD'er, inden de bortskaffes, og
vi) sikre, at alle personoplysninger fjernes fra harddiskene på servere og computere, inden de bortskaffes.

Backup
Databehandleren skal foretage backup af indhentede data mindst én gang i døgnet. Backup-overførslen skal være krypteret. Backup skal opbevares adskilt fra produktionsdata efter samme sikkerhedsniveau som produktionsdata.

Adgangskontrol
Databehandleren skal have procedurer for adgangskoder på plads, herunder brug af stærke adgangskoder, to-faktor godkendelse, periodisk opdatering af adgangskoder og sikring af, at medarbejderne ikke skriver dem ned.

Logning
Databehandleren skal logge mislykkede login-forsøg, herunder logning af tid, bruger mv. og blokere adgang efter et bestemt antal mislykkede login-forsøg for hver bruger.

Databehandleren skal logge brugeraktiviteter, herunder alle anvendelser af brugeroplyser, dvs. logning af tid, bruger, søgning, søgekriterier, adgang, ændring, lukning, udskrift, eksport, sletning mv. og automatisk sletning af log efter et bestemt tidsinterval.

Integritet og tilgængelighed
Databehandleren skal implementere følgende foranstaltninger og processer:

i) Beskytte netværk, systemer, logger og Personoplysninger mod manipulation.
ii) Sikre evnen til at genoprette tilgængeligheden af og adgangen til Personoplysninger rettidigt i tilfælde af en fysisk eller teknisk hændelse, herunder ved sikkerhedskopiering af data.

Modstandsdygtighed
Databehandleren skal have et sårbarhedsstyringsprogram, herunder løbende overvågning af potentielle sårbarheder og gennemførelse af penetrationstests på netværk og systemer, der anvendes til behandling af Personoplysninger.

Sårbarhedsstyringsprogrammet skal indeholde, men er ikke begrænset til:

i) At udføre sårbarhedsscanninger på interne og eksterne områder mindst hvert kvartal
ii) At gennemføre penetrationstests på eksterne netværk mindst hvert kvartal eller oftere i tilfælde af hændelser, der viser at der er behov for det
iii) At følge op på og afhjælpe eventuelle svagheder, som identificeres i forbindelse med sådanne scanninger og tests

Databehandleren skal løbende holde netværk og systemer ajour med nye versioner, opdateringer og patcher.

Sikkerheds- og datasikkerhedsteknologier
Databehandleren skal implementere de nedenfor anførte foranstaltninger og processer:

Sikre, at alle anvendte computere og servere har antivirus- eller antimalware software installeret, og at virusdefinitionerne opdateres mindst én gang om ugen. Al indgående og udgående trafik skal scannes for virus, såvel som enhver brugt disk eller flytbare medier. Computere og servere skal scannes for virus mindst én gang om ugen.
Hvis computere og servere har forbindelse til internettet, skal de stå bag en installeres en firewall, helst en Next Generation Firewall, og internetforbindelser gerne være beskyttet af anti-DDOS-beskyttelse samt være dækket af et overvågningssystem.

Systemer der holder, opbevarer eller på anden måde behandler personoplysninger skal mindst en gang årligt testes med sårbarhedsscanning og penetrationstest.

Awareness, træning og sikkerhedskontrol i forhold til personale
Databehandleren skal implementere de nedenfor anførte foranstaltninger og processer:

i) Foretage integritetskontrol på alle nye medarbejdere for at verificere de oplysninger, som medarbejderne angiver, om deres baggrund, erfaring eller kvalifikationer, er korrekte. Ligeledes skal databehandleren have en passende procedure for indhentelse af rene straffeattester for teknikere, som kommer i private boliger og forretningslokaler. Ydermere skal der foretages årlige stikprøver.
ii) Introducere medarbejdere (nye såvel som nuværende) til informationssikkerhed, og sikre, at de læser og forstår informationssikkerhedspolitikken. Det skal sikres, at medarbejderne løbende ved, hvor de skal finde oplysninger om de standarder og procedurer for informationssikkerhed, der er relevante for deres rolle og ansvar.

Hændelseshåndtering og forretningskontinuitet
Databehandleren skal implementere de nedenfor anførte foranstaltninger og processer:

i) Træning af medarbejdere, herunder medarbejdernes forståelse for brud på persondatasikkerheden, sikkerhedshændelser samt tegn og hensigtsmæssige reaktioner på hhv. brud og sikkerhedshændelser. En sikkerhedshændelse er enhver begivenhed, der kan skade eller kompromittere fortroligheden, integriteten eller tilgængeligheden af forretningskritiske oplysninger eller systemer.
ii) Databehandleren skal have udarbejdet en plan for at sikre forretningskontinuitet i tilfælde af en alvorlig sikkerhedshændelse og skal afprøve planen mindst én gang om året. Efter en hændelse eller tests, hvori planen anvendes, skal den gennemgås og ajourføres.

Auditering
Databehandleren skal overvåge og sørge for ajourføring af alle foranstaltninger, processer og risikoanalyser.

Databehandleren skal implementere en procedure for regelmæssig testning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed, herunder, men ikke begrænset til, de heri angivne foranstaltninger.

Databehandleren skal implementere procedurer for effektiv opfølgning på manglende overholdelse.

Audit skal ske mindst én gang om året.

Myndigheder
Databehandleren samarbejder efter anmodning med Datatilsynet og eventuelle øvrige tilsynsmyndigheder i forbindelse med udførelsen af sådanne tilsynsmyndigheders opgaver. Databehandleren er herunder berettiget til at give Datatilsynet adgang til alle personoplysninger og oplysninger, der er nødvendige for at varetage Datatilsynets opgaver.

Databehandleren træffer de nødvendige foranstaltninger til at sikre overholdelse af en afgørelse fra Datatilsynet. Databehandleren underretter på den datasvarliges vegne Datatilsynet om de foranstaltninger, der er truffet for at overholde afgørelsen.

Meddeler Datatilsynet databehandleren påbud, skal databehandleren efterkomme sådant påbud i overensstemmelse med den nærmere angivne måde og inden for den angivne frist.

C.3 Bistand til den dataansvarlige

Databehandleren har den dataansvarliges generelle godkendelse til at bistå den dataansvarlige med dennes forpligtelser efter disse Bestemmelser, herunder i relation til de registreredes rettigheder, udarbejdelse af konsekvensanalyser vedrørende databeskyttelse og bistand i forbindelse med forudgående høring af Datatilsynet.

C.4 Opbevaringsperiode/sletterutine

Databehandleren skal slette personoplysninger efter 5 år

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller anonymisere personoplysningerne i overensstemmelse med bestemmelse 11.1,

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden skriftligt og forudgående varsel af den dataansvarliges ske på andre lokaliteter end de i Bilag B.1 angivne.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren og de godkendte underdatabehandlere, jf. Bilag B.1, overfører ikke personoplysninger til tredjelande.

Ved ændring af lokationer for databehandlerens behandling af personoplysninger, som vil medføre overførsel til usikre tredjelande, er databehandleren forpligtet til skriftligt at oplyse den dataansvarlige med mindst 3 måneders skriftligt varsel, hvorved den dataansvarlige får mulighed for at gøre indsigelse mod overførsel, jf. Bilag C.5.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige kan udbede sig skriftlig bekræftelse, fx Uafhængig revisorerklæring eller foretage en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

Den dataansvarlige kan en gang årligt fremsende tilsynsskema til databehandleren. Evt. omkostninger til udfyldelse af skriftlig tilsyn, afholdes af databehandler.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre et yderligere skriftligt tilsyn eller en inspektion hos databehandleren, såfremt den dataansvarlige finder det nødvendigt.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal føre tilstrækkeligt tilsyn med dennes underdatabehandleres overholdelse af databeskyttelseslovgivningen, og indgåede databehandler aftaler. Dette tilsyn kan være et tilsynsskema, en uafhængig revisorerklæring eller et fysisk tilsyn.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Bilag D **Parternes regulering af andre forhold**

-