Appendiks 2
Lessor Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

[NAVN]
CVR [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter "den dataansvarlige" eller "Kunden"

og

Lessor ApS
CVR 24240010
Engholm Parkvej 8
3450 Allerød
Danmark

herefter "databehandleren" eller "Lessor"

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

1. Indhold

2. Præampel

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 **Systemet** som Aftalen vedrører, 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. 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.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er

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

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 **2 måneders** 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. 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 ske uden unødig forsinkelse og om muligt **24 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 tilsynsmyndighed, 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 alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, 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 på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. 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.

4. 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.

5. Underskrift

Se venligst underskrifterne, der fremgår af Anvendelsesaftalen

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

På vegne af den dataansvarlige

Navn	[KONTAKTPERSON HOS KUNDEN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

På vegne af databehandleren

Navn	Peter Tvermoes Meier
Stilling	International Corporate Counsel
Telefonnummer	+45 24 29 04 21
E-mail	Peme@lessor.dk

Bilag A – Oplysninger om behandlingen

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

Formålet med at lade databehandleren foretage databehandlingen er at stille Systemet og funktionerne heri til rådighed for den dataansvarlige, samt yde support og konsulentassistance i forbindelse med implementering og daglig drift mv. af Systemet.

Såfremt det er aftalt at Systemet hostes af databehandleren, inkluderer den dataansvarliges instruks beskrevet nedenfor, at personoplysningerne også behandles med henblik på sådan hosting. Såfremt oplysninger ikke hostes af databehandleren, vil databehandleren alene have adgang til oplysninger og alene behandle oplysninger i forbindelse med særlige aftaler herom med den dataansvarlige, dette vil typisk være i forbindelse med fjernsupport- og/eller konsulentopgaver, men kan også ske som led i drift af VPN-tunnel eller andet, hvorom der indgås aftale.

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

Opbevaring af og adgang til personoplysninger.

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

Behandligen kan omfatte enhver type personoplysning, som er relevant for anvendelsen af systemet, herunder ikke-følsomme personoplysninger og følsomme personoplysninger.

System(er)	Typer af personoplysninger
Lessor Payroll, Lessor Time & Attendance og Lessor Human Resources til Microsoft Dynamics	De oplysninger, som Kunden registrerer om individer i systemerne, fx, men ikke nødvendigvis begrænset til: CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, or-lovsregistreringer, løndata, pensionsinformationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet, tidsregistrering (kun for Time & Attendance), opgaveregistrering (kun for Lessor Time & Attendance),
Lessor4	CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, orlovsregistreringer, løndata, pensionsinformationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger, som Kunden selv indberetter til Systemet.
Lessor4 Tid	CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, tidsregistrering, opgaveregistrering, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.
LessorLøn	CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, orlovsregistreringer, løndata, pensionsinformationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.

LessorPM	a) CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, løndata, pensionsinformationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, Loginoplysninger (krypteret), samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.
	b) CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mail, CV, ansøgninger, samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.
LessorPortalen	Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, lønsedler, fraværsoplysninger, kørselsoplysninger, tidsregistrering, opgaveregistrering, rejseoplysninger, kompetencer, uddannelse, pårørende, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.
LessorSP Tid	CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, tidsregistrering, opgaveregistrering, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger(krypteret), samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.
LessorWorkforce	Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, fraværsoplysninger, vagtplaner, tidsregistrering, opgaveregistrering, kompetencer, personlige dokumenter, samt alle oplysninger som den dataansvarlige selv indberetter til Systemet.

A.4. Behandlingen omfatter følgende kategorier af registrerede

System(er)	**Kategorier af registrerede**
Lessor Payroll, Lessor Time & Attendance og Lessor Human Resources til Microsoft Dynamics	De personer, som den dataansvarlige registrerer oplysninger om i de af Lessor udviklede produkter til Microsoft Dynamics i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
Lessor4	De personer, som den dataansvarlige registrerer oplysninger om i Lessor4 i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
Lessor4 Tid	De personer, som den dataansvarlige registrerer oplysninger om i Lessor4 Tid i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
LessorLøn	De personer, som den dataansvarlige registrerer oplysninger om i LessorLøn i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
LessorPM	a) De personer, som den dataansvarlige registrerer oplysninger om i LessorPM i det omfang,

	Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for.
	b) Ansøgere til ledige stillinger hos den dataansvarlige.
LessorPortalen	De personer, som den dataansvarlige registrerer oplysninger om i LessorPortalen i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
LessorSP Tid	De personer, som den dataansvarlige registrerer oplysninger om i LessorSP Tid i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).
LessorWorkforce	De personer, som den dataansvarlige registrerer oplysninger om i LessorWorkforce i det omfang, Lessor gives adgang til disse oplysninger i forbindelse med konkrete opgaver, som Lessor udfører for den dataansvarlige (herunder medarbejdere og/eller tidligere medarbejdere hos den dataansvarlige og/eller hos selskaber, som den dataansvarlige har ret til at benytte Systemet for).

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

Behandlingen finder sted indtil Aftalen ophører.

Uanset Bestemmelsernes formelle aftaleperiode, skal Bestemmelserne vedblive at gælde, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige.

Bilag B - Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

Underdatabehandler	CVR	Lokation(er)	Behandling
Post Danmark A/S	26663903	Hedegaardvej 88, 2300 København S, Danmark	I tilfælde hvor den dataansvarliges løsning er hostet af Lessor, samarbejder Lessor med Post Danmark A/S, der, såfremt dette er aftalt med den dataansvarlige, muliggør udsendelse af lønsedler via e-Boks.
Compaya A/S	31375428	Palægade 4, 2. tv, 1261 København K, Danmark	I tilfælde, hvor Systemet benyttes til at sende SMS-beskeder til den dataansvarliges ansatte, samarbejder Lessor med Compaya A/S, der håndterer udsendelse af SMS'er.
Emply International ApS	37048658	Lyngbyvej 102, 2100 København Ø, Danmark	I tilfælde, hvor den dataansvarlige anvender en Emply-løsning, samarbejder Lessor med Emply International ApS, som bl.a. leverer implementering og support.
InterLogic Danmark ApS	38179365	Ellestien 7, 8250 Egå, Danmark Dok 1 80-958 Gdańsk, Polen	I tilfælde, hvor Lessor får ekstern bistand til at løse en konkret support-sag, hvor der indgår personoplysninger i det materiale, som tilgås af den eksterne konsulent.
NetNordic Denmark A/S	33636431	Lyskær 1, DK2730 Herlev, Danmark Råsundavägen 4, 5TR, 16967 Solna, Sverige	I tilfælde, hvor den dataansvarliges løsning er hostet af Lessor, samarbejder Lessor med NetNordic Danmark A/S, der hoster back-up data.
Netic A/S	26762642	Alfred Nobels Vej 25, 9220 Aalborg, Denmark	Hosting og drift af it-systemer
Trifork Security A/S	44562162	Alfred Nobels Vej 25, 9220 Aalborg Øst, Danmark	Lessor anvender Trifork Security i forhold til levering af Managed Security Services, der sikrer og kontrollerer trafik på Lessors servere.
Fullview ApS	42552259	Kultorvet 11, 1175 København, Danmark	Lessor anvender Fullviews værktøj til at yde kundesupport ved direkte live kommunikation og vejledning. Det er Cloud platform for hosting af service og opbevaring. Fullview hoster deres løsning hos OVH Cloud server i Tyskland.

			OVH Groupe SA 2 rue Kellermann 59100 Roubaix. EU hostet.

Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst **2 måneders** varsel.

Bilac C - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

System(er)	Beskrivelse af behandlingen
LessorRefusion	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende Lessor Refusion og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor Refusion anvendes som den dataansvarliges værktøj til at anmelde og anmode om udbetaling af refusion på baggrund af medarbejdernes fravær som følge af sygdom og barsel. Endvidere kan den dataansvarlige se forventet refusion og modtaget refusion, samt status på refusionssagerne. Medarbejdernes fravær kan synkroniseres fra LessorPortalen, LessorSP Tid eller første fraværsdag kan tastes direkte i LessorRefusion.
Lessor Payroll, Lessor Time & Attendance og Lessor Human Resources til Microsoft Dynamics	Formålet med at lade Lessor foretage databehandlingen er at yde den dataansvarlige support- og/eller konsulentopgaver i forbindelse med den dataansvarliges brug af Lessors programmer til Microsoft Dynamics. Lessor vil kunne have behov for adgang til og udtræk fra den dataansvarliges miljø og dermed personoplysninger deri for at kunne udføre sådanne opgaver. Personoplysningerne behandles med det formål at yde af den dataansvarlige efterspurgte support- og/eller konsulentydelser. Det bemærkes at programmerne ikke hostes af Lessor, men af den dataansvarlige selv eller af tredjepart. Assistancen kan foregå ved, at den dataansvarlige beder den partner, som den dataansvarlige har indgået aftale med, om assistance, og denne partner derefter inddrager Lessor i forbindelse med den pågældende assistance, hvorved Lessor modtager de omhandlede personoplysninger fra partneren frem for den dataansvarlige. Data kan synkroniseres med enten Lessors Portal samt andre eksterne systemer der understøtter Lessor Integration Framework (LIF).
Lessor4	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende Lessor 4 og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor 4 anvendes til håndtering af lønudbetaling og pensionsudbetaling. Det er muligt at indtaste registreringer, som kørsel, variable løndele, fravær og registrering af medarbejderoplysninger. Det er endvidere muligt at indlæse data fra eksterne systemer. Data kan synkroniseres med enten Lessor Portal, Lessors tidssystemer eller HR-systemer, samt andre eksterne systemer der understøtter Lessor Integration Framework (LIF). Lønsedler kan sendes til e-Boks såfremt dette er valgt. Betalinger kan overføres via Nets eller en bank efter den dataansvarliges valg.
Lessor4 Tid	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende Lessor 4 TID og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor 4 TID er en online tidsregistreringsløsning, der anvendes af medarbejdere, ledere og administration til håndtering af medarbejderes vagtplaner og registrering af variable løndele, fravær og tidsregistrering. Brugere kan benytte Systemet via en Windows-klient, webbrowser, app eller industriterminal. Medarbejderen kan se og eventuelt vedligeholde egne stamdata. Data kan udveksles med Lessors øvrige systemer til behandling af løn, vagtplanlægning og HR og der findes mulighed for integration til 3. part systemer via XML eller filudveksling. Lederne har mulighed for godkendelse eller afvisning af inddateringer og ændringer, inden variable løndele udveksles.
LessorLøn	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende LessorLøn og funktionerne heri samt yde support og konsulentassistance til denne brug. LessorLøn anvendes til håndtering af lønudbetaling, pensionsudbetaling,

	budgetlægning samt understøttelse af virksomhedens HR-funktioner. Det er muligt at indtaste registreringer, som kørsel, variable løndele, fravær og registrering af HR-oplysninger. Det er endvidere muligt at indlæse data fra eksterne systemer. Data kan synkroniseres med enten Lessor Portal, Lessors tidssystemer eller HR-systemer, samt andre eksterne systemer der understøtter Lessor Integration Framework (LIF). LessorLøn har integration til Skat og CPR-registreret, hvortil og fra der kan sendes og modtages data. Lønsedler sendes til e-Boks såfremt dette er valgt. Betalinger kan overføres via Nets.
LessorPM	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende LessorPM og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor PM anvendes til håndtering af lønudbetaling, samt understøttelse af virksomhedens HR-funktioner. Det er muligt at indtaste registreringer, som kørsel, variable løndele, fravær og registrering af HR-oplysninger. Det er endvidere muligt at indlæse data fra eksterne systemer. Data kan synkroniseres med enten Lessors Portal, tidssystemer og HR-systemer, samt andre eksterne systemer der understøtter Lessor Integration Framework (LIF). LessorPM har mulighed for integration til Skattestyrelsen, hvortil og fra der sendes og modtages data. Lønsedler kan sendes til e-Boks såfremt dette er valgt. Betalinger kan overføres af den dataansvarlige til Nets eller bank.
LessorPortalen	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende LessorPortalen og funktionerne heri samt yde support og konsulentassistance til denne brug. LessorPortalen anvendes som medarbejder selvservice- og lederportal til inddatering af registreringer, som kørsel, variable løndele, fravær, komme/gå-oplysninger og rejseomkostninger. Endvidere kan medarbejderen se og eventuelt vedligeholde egne stamdata. Data kan synkroniseres med enten Lessors lønsystemer, tidssystemer eller HR-systemer. Lederne har mulighed for godkendelse eller afvisning af inddateringer eller ændringer inden data synkroniseres.
LessorSP Tid	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende LessorSP Tid og funktionerne heri samt yde support og konsulentassistance til denne brug. LessorSP Tid er en online tidsregistreringsløsning, der anvendes af medarbejdere, ledere og administration til håndtering af medarbejderes vagtplaner og registrering af variable løndele, fravær og tidsregistrering. Brugere kan benytte Systemet via en Windows-klient, webbrowser, app eller industriterminal. Medarbejderen kan se og eventuelt vedligeholde egne stamdata. Data kan udveksles med Lessors øvrige systemer til behandling af løn, vagtplanlægning og HR og der findes mulighed for integration til 3. part systemer via XML eller filudveksling. Lederne har mulighed for godkendelse eller afvisning af inddateringer og ændringer, inden variable løndele udveksles. Data kan synkroniseres med Lessors Portal.
LessorWorkforce	Formålet med at lade Lessor foretage databehandlingen er at lade den dataansvarlige anvende LessorWorkforce og funktionerne heri samt yde support og konsulentassistance til denne brug. LessorWorkforce er en online vagtplanløsning, der anvendes af medarbejdere, ledere og administration til håndtering af medarbejderes vagtplaner og registrering af variable løndele, fravær og tidsregistrering. Brugere kan benytte Systemet via en webbrowser eller via en App. Medarbejderen kan se og eventuelt vedligeholde egne stamdata. Data kan udveksles med Lessors øvrige systemer til behandling af løn, tid og HR og der findes mulighed for integration til 3. part systemer via webservice. Lederne har mulighed for godkendelse eller afvisning af inddateringer og ændringer, inden variable løndele udveksles.

Videregivelse af personoplysninger

Afhængigt af det af den dataansvarlige brugte system og såfremt Lessor hoster det af den dataansvarlige brugte system, kan Lessor videregive personoplysninger på vegne af den dataansvarlige som led i Lessors services til den dataansvarlige, herunder eksempelvis til Skattestyrelsen, pensionsselskaber, Nets, Danmarks Statistik, KOMBIT m.fl.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter opbevaring af og adgang til almindelige (herunder også fortrolige) og, i nogle tilfælde, følsomme personoplysninger. Behandlingen sker som led i den dataansvarliges brug af Systemet, og den dataansvarlige har mulighed for at kontrollere, hvilke personoplysninger, der indgår i de(t) pågældende system(er).

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Lessor anvender en risikobaseret tilgang til IT-sikkerhed og beskyttelse af de personoplysninger, vi behandler om den dataansvarlige og den dataansvarliges medarbejdere. Lessor har fastsat nedenstående tekniske og organisatoriske sikkerhedsforanstaltninger for at mitigere de risici, der er forbundet med behandling af personoplysninger i Systemet, hvor Lessor agerer som databehandler for den dataansvarlige. Lessor vil altid som minimum iværksætte de nedenstående sikkerhedsforanstaltninger, men kan til enhver tid opgradere sikkerhedsniveauet og de dertilhørende foranstaltninger i forbindelse med en udvikling i risikoscenariet.

Da Lessors løsninger leveres som SaaS-løsninger, der hostes af Lessor, og/eller on-premise-løsninger, der hostes af den dataansvarlige selv, beskrives Lessors sikkerhedsforanstaltninger nedenfor opdelt for disse to leveringsformer.

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

For SaaS-løsninger hostet af Lessor gælder følgende sikkerhedsforanstaltninger i relation til behandling af personoplysninger:	
Fysisk sikkerhed i Lessors lokaler og datacentre	Lessor har etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå adgang til lokaler og datacentre, hvor der opbevares og behandles personoplysninger. Eksterne konsulenter og andre besøgende får kun adgang til datacentre i følgeskab med en autoriseret medarbejder. Der foretages videoovervågning af Lessors faciliteter og datacentre. Der er implementeret alarmsystemer i Lessors lokaler og datacentre og der er kun adgang med nøgle eller adgangskort og dertilhørende kode. Datacentrene har implementeret kølesystem, redundant strømforsyning, brandsikring, fibernet og monitoreringssystem.
Logning	Al netværkstrafik og alle serverlogs bliver overvåget og logget. Følgende logges i systemer, databaser og netværk: • Alle adgangsforsøg, • Alle søgninger, • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser, herunder (i) deaktivering af logning, (ii) ændringer i systemrettigheder og (iii) mislykkede forsøg på log-on.

	Lessor opererer ikke med fælles log-in, så det vil altid være muligt at identificere den medarbejder, der har foretaget en aktivitet. Som standardfunktion har en bruger 3 adgangsforsøg inden brugeren afvises (dette kan ændres af Kunden). De relevante logfiler lagres og beskyttes mod manipulation og tekniske fejl. Logfilerne gennemgås løbende for at sikre normal drift og for at undersøge utilsigtede hændelser eller incidents.
Antivirus og firewalls	Al ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en sikret firewall med en restriktiv protokol. Der er etableret port- og IP-adresse filtrering for at sikre begrænset adgang til porte og for specifikke IP-adresser. Der er installeret antivirus software og Intrusion Prevention System (IPS) på alle systemer og databaser, der anvendes til behandling af personoplysninger, for at beskytte imod fjendtlige angreb. Den anvendte antivirus software opdateres regelmæssigt. Beskyttelse mod XSS og SQL-injektioner er implementeret i alle tjenester. Lessors interne netværk kan kun tilgås af dertil autoriserede personer.
Kryptering	Der anvendes kryptering baseret på en algoritme ved transmission af personoplysninger via internettet og/eller e-mail (minimum TLS 1.2). Data i hvile (at rest) er også krypteret, Der anvendes HTTPS forbindelse ved dataoverførsler. Kundens UserID (brugernavn) og password krypteres ved brug af en algoritme.
Back-up og tilgængelighed	De tekniske foranstaltninger og Lessors systemer testes løbende ved sårbarhedsscanninger og penetrationstests. Alle ændringer til systemer, databaser og netværk følger fastlagte Change Management procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. Der foretages systemovervågning af alle systemer, hvori der behandles personoplysninger. Datamiljøet overvåges for sårbarheder og eventuelle identificerede problemer afhjælpes. Der foretages back-up, så det sikres at alle systemer og data, herunder personoplysninger, kan genoprettes, hvis de går tabt eller ændres.
Autorisation, adgangsbegrænsninger og sikkerhed	Det er kun medarbejdere med et arbejdsbetinget behov, der får adgang til personoplysninger. Alle vurderinger af en medarbejders arbejdsbetingede behov foretages ud fra en "need-to-have" tilgang, for at sikre overholdelse af princippet om dataminimering. Medarbejdernes adgang revurderes regelmæssigt. Der gennemføres løbende awareness-træning af medarbejdere i relation til IT-sikkerhed og behandlingssikkerhed for personoplysninger. Alle medarbejdere informeres om den af ledelsen godkendte skriftlige informationssikkerhedspolitik. Der foretages screening af alle nye medarbejdere. Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver nye medarbejdere introduceret til

	informationssikkerhedspolitikken og procedurer for behandling af de personoplysninger, der ligger inden for medarbejderens arbejdsområde. Der er fastsat procedurer for at sikre, at fratrædende medarbejdere bliver frataget deres tildelte brugerrettigheder. Lessor har implementeret en passwordpolitik, der er med til at sikre (i) at medarbejderes adgangskoder ikke kommer uvedkommende i hænde, samt (ii) at der kun godkendes adgangskoder, der er tilstrækkeligt komplicerede, og (iii) at adgangskoder skiftes regelmæssigt. Der anvendes multifaktorautentisering på Lessors forskellige løsninger. Der er etableret beskyttelse af flytbare enheder. Medarbejderes laptop computere er bl.a. beskyttet med kryptering og passwords på harddiskdrev-niveau. Der anvendes desuden VPN-forbindelse og to-faktor autentificering ved fjernadgang. Eksterne personer, der færdes på Lessors lokationer og i datacentre, hvor der potentielt er adgang til personoplysninger, informeres om Lessors sikkerhedsregler og underskriver en fortrolighedserklæring.
Kontroller	Lessor udfører intern revision og kontrol af de fastsatte tekniske og organisatoriske sikkerhedsforanstaltninger baseret på kontrollerne i den anerkendte ISO 27002-standard. ISO 27002-standarden anvendes til at sikre kontrol med implementeringen af det Information Security Management System ("ISMS"), som Lessor bruger til risikostyring i forbindelse med fastlæggelsen af de nødvendige sikkerhedstiltag. Derudover udarbejdes der årligt en ISAE 3402-erklæring af en uafhængig revisor. ISAE 3402-erklæringen har fokus på, at Lessor har etableret og opretholder et tilstrækkeligt IT-sikkerhedsniveau.
For on-premise-løsninger gælder følgende sikkerhedsforanstaltninger i relation til Lessors behandling af personoplysninger som databehandler:	
Sikkerhedsforanstaltninger i forbindelse med konkret fjernsupport	Lessor vil indledningsvis træffe de nødvendige foranstaltninger for at sikre, at henvendelsen kommer fra den pågældende Kunde. Alle henvendelser registreres i Lessors sagsbehandlingssystem. Størstedelen af alle henvendelser kan håndteres i et supportopkald mellem Kunden og supportkonsulenten. Hvis en supportkonsulent har brug for adgang til Kundens system, og Kundens platform tillader direkte adgang, kan supportkonsulenten anvende fjernadgang til at betjene Kundens systemer. Brug af fjernadgang kræver specifik godkendelse fra Kunden, idet Kunden skal godkende, at supportkonsulenten overtager kontrollen af Kundens skærm, tastatur og mus. Ved brug af fjernadgang kan Kunden se alle handlinger, som supportkonsulenten har foretaget på Kundens skærm. Der anvendes krypteret kommunikation i forbindelse med fjernadgang. For at Lessor kan udføre fejlsøgning i Lessors testmiljø, kan Kunden transmittere uddrag af datasæt fra Systemet eller sende screen shots fra Systemet til Lessor. Lessor anbefaler, at datasæt og screen shots alene transmitteres som krypterede filer til Lessor via krypterede forbindelser, da datasættene kan indeholde fortrolige personoplysninger, hvilket medfører krav om kryptering fra Datatilsynet. Lessor stiller et fildelingsværktøj til rådighed for krypteret transmittering af data.
Autorisation og adgangsbegrænsninger	Det er kun supportkonsulenter med et arbejdsbetinget behov, der får adgang til personoplysninger i forbindelse med supportsager. Alle vurderinger af en supportkonsulents arbejdsbetingede behov foretages ud fra en "need-to-have" tilgang, for at sikre overholdelse

	af princippet om dataminimering. Der gennemføres løbende awareness-træning af supportkonsulenter i relation til IT-sikkerhed og behandlingssikkerhed for personoplysninger. Alle supportkonsulenter informeres om den af ledelsen godkendte informationssikkerhedspolitik. Der foretages screening af alle nye supportkonsulenter. Ved ansættelse underskriver supportkonsulenterne en fortrolighedsaftale. Endvidere bliver nye supportkonsulenter introduceret til informationssikkerhedspolitikken og procedurer for behandling af de personoplysninger, der ligger inden for supportkonsulentens arbejdsområde. Der er fastsat procedurer for at sikre, at fratrædende supportkonsulenter bliver frataget deres tildelte brugerrettigheder. Lessor har implementeret en passwordpolitik, der er med til at (i) sikre at medarbejderes adgangskoder ikke kommer uvedkommende i hænde, samt (ii) at der kun godkendes adgangskoder, der er tilstrækkeligt komplicerede, og (iii) at adgangskoder skiftes regelmæssigt. Der anvendes multifaktorautentisering på Lessors forskellige løsninger. Der er etableret beskyttelse af flytbare enheder. Supportkonsulenters bærbare computere er bl.a. beskyttet medkryptering og passwords på harddiskdrev-niveau. Der anvendes desuden VPN-forbindelse og to-faktor autentificering ved fjernadgang. Eksterne personer, der færdes på Lessors lokationer, hvor der potentielt er adgang til personoplysninger, informeres om Lessors sikkerhedsregler og underskriver en fortrolighedserklæring. Lessor har derudover clean-desk policy.
Fysisk sikkerhed	Lessor har etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå adgang til Lessors lokaler og datacentre, hvor der opbevares og behandles personoplysninger. Eksterne konsulenter og andre besøgende får kun adgang til datacentre i følgeskab med en autoriseret medarbejder. Der foretages videoovervågning af Lessors faciliteter. Der er implementeret alarmsystemer i Lessors lokaler, og der er kun adgang med nøgle eller adgangskort og dertilhørende kode.
Antivirus og firewalls	Al ekstern adgang til systemer, der anvendes til behandling af personoplysninger, sker gennem en sikret firewall med en restriktiv protokol. Der er etableret port- og IP-adresse filtrering for at sikre begrænset adgang til porte og for specifikke IP-adresser. Der er installeret antivirus software og Intrusion Prevention System (IPS) på alle systemer, der anvendes til behandling af personoplysninger, for at beskytte imod fjendtlige angreb. Den anvendte antivirus software opdateres regelmæssigt. Beskyttelse mod XSS og SQL-injektioner er implementeret i alle tjenester. Lessors interne netværk kan kun tilgås af dertil autoriserede personer.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Personoplysninger, som indgår i Systemet, som den dataansvarlige har adgang, kan til enhver tid tilgås og kontrolleres af den dataansvarlige på egen hånd, eller ved at kontakte databehandleren, som bistår med at skaffe den dataansvarlige den fornødne adgang til personoplysningerne.
- Databehandleren har indrettet sig organisatorisk således, at relevante kontaktpersoner hos databehandleren kan rapportere eller eskallere spørgsmål om bl.a. bistand til relevante medlemmer af databehandlerens ledelse og/eller til databehandlerens tekniske og juridiske personale.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i overensstemmelse med de sletteregler, som den dataansvarlige enten selv, eller med bistand fra databehandleren, har opsat i Systemet, hvorefter de slettes hos databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- Engholm Parkvej 8, 3450 Allerød, Danmark
- Industriparken 35, 2750 Ballerup, Danmark

Lokaliteterne for underdatabehandlernes behandling findes i oversigten i Bilag B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren overfører ikke personoplysningerne til tredjelande, medmindre dette aftales specifikt og særskilt med den dataansvarlige. Såfremt den dataansvarlige og databehandleren aftaler, at der skal ske overførsel til tredjelande, sikrer parterne i fællesskab, at et passende overførselsgrundlag er på plads forinden sådanne overførsler iværksættes.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels 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

Databehandleren skal hvert år, for egen regning, indhente en erklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Bestemmelserne, og erklæringen uploades på databehandlerens hjemmeside http://www.lessor.dk/.

Databehandleren kan ved skriftlig meddelelse til den dataansvarlige ændre den hjemmeside, hvorpå erklæringen uploades.

Der er enighed mellem parterne om, at følgende typer af revisionserklæring(er) altid kan anvendes i overensstemmelse med disse bestemmelser:

- ISAE 3402

- ISAE 3000

Derudover har Kunden ret til for egen regning at udpege en uafhængig ekspert, som skal have adgang til de dele af Lessors fysiske faciliteter, hvor behandling af personoplysninger finder sted, samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt Lessor har gennemført de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger. Kundens uafhængige ekspert kan ikke opnå adgang til oplysninger om Lessors generelle omkostningsstruktur eller til oplysninger, der vedrører andre af Lessors kunder. Eksperten skal på Lessors anmodning underskrive en sædvanlig fortrolighedserklæring og skal under alle omstændigheder behandle enhver information indhentet hos eller modtaget fra Lessor fortroligt, og må alene dele informationen med Kunden. Kunden må ikke viderebringe informationen eller benytte informationen til andre formål end at vurdere hvorvidt, Lessor har truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

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

Databehandleren fastsætter passende procedurer vedrørende tilsyn med den pågældende underdatabehandler, baseret på den konkrete risiko som de overladte personoplysninger udgør, jf. risikobaseret tilgang nævnt i Bilag C.2., samt Datatilsynets vejledning vedrørende tilsyn med databehandlere.

Bilag D - Parternes regulering af andre forhold

1. **Definitioner:** Bestemmelserne udgør et Bilag til den aftale, som er indgået mellem Kunden og Lessor vedrørende køb af licens til et eller flere af Lessors systemer (Aftalen). Definerede ord og udtryk i Bestemmelserne har samme betydning, som angivet i Aftalen, medmindre andet fremgår eksplicit af Bestemmelserne.

2. **Forrang:** I tilfælde af uoverensstemmelse mellem Bestemmelserne og bestemmelser i andre skriftlige eller mundtlige aftaler indgået mellem parterne, skal Bestemmelserne have forrang, medmindre andet eksplicit er aftalt mellem parterne.

3. **Særskilt honorar:** Den dataansvarlige honorerer databehandleren særskilt for at håndtere konkrete forespørgsler og opgaver i henhold til Bestemmelse 6 (Behandlingssikkerhed), 9 (Bistand til den dataansvarlige) og 12 (Revision, herunder inspektion) samt Bilag C.7 og C.8, i det omfang, at det ikke fremgår eksplicit, at opgaverne leveres for databehandlerens egen regning. Honoraret beregnes ud fra medgået tid og materiale og på baggrund af databehandlerens til enhver tid gældende timetakster.

4. **Underdatabehandlere:** Efter Lessor skriftligt har underrettet Kunden om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere jf. Bestemmelse 7.3, kan Kunden uden begrundelse gøre indsigelse mod ændringen. En indsigelse fra Kunden skal ske inden 2 uger fra afgivelsen af meddelelsen om ændringen. Hvis Kunden gør indsigelse mod ændringen er Lessor berettiget til at opsige alle aftaler med Kunden, hvor Lessor behandler personoplysninger for Kunden, med 2 måneders varsel.