DATABEHANDLERAFTALE

BILAG TIL AFTALE MED LESSOR A/S

Der indgås hermed følgende databehandleraftale ("Databehandleraftalen") mellem den juridiske enhed, der har indgået aftale om brug af Lessors programmer ("Kunden") og Lessor A/S, CVR nr.: 24240010, Engholm Parkvej 8, 3450 Allerød, Danmark ("Lessor"), der samlet benævnes "Parterne" og separat en "Part":

1 Databehandleraftalens omfang

1.1 Partnere har ved tidligere lejlighed indgået aftale om Kundens brug af Lessors programmer ("Aftalen"). Databehandleraftalen udgør et bilag til Aftalen og Aftalens vilkår, gælder for Databehandleraftalen, hvor Databehandleraftalen ikke angiver andet. I tilfælde af konflikt mellem vilkårene i Databehandleraftalen og Aftalen, har Databehandleraftalens vilkår forrang, jf. punkt 8 nedenfor.

1.2 Lessor er databehandler for Kunden, idet Lessor varetager de i Appendiks 1 beskrevne databehandlingsopgaver for Kunden.

1.3 De Personoplysninger, der behandles af Lessor, formålene med behandlingen, kategorierne af Personoplysninger og kategorierne af registrerede personer, er anført i Appendiks 1.

1.4 Databehandleraftalen regulerer alene den behandling af Personoplysninger, som Lessor foretager for Kunden som databehandler.

1.5 Ved "Personoplysninger" forstås enhver form for information om en identificeret eller identificerbar fysisk person, jf. artikel 4(1) i Forordning (EU) 2016/679 af 27. april 2016 ("Persondataforordningen").

2 Behandling af Personoplysninger

2.1 Lessor må kun behandle Personoplysninger efter dokumenteret instruks fra Kunden, herunder for så vidt angår overførsel af Personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Lessor er underlagt. I så fald underretter Lessor Kunden om dette retlige krav, inden behandling, medmindre den pågældende

ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

2.2 Instruks: Lessor er instrueret i alene at behandle Personoplysningerne med det formål at varetage de i Appendiks 1 fastsatte databehandlingsopgaver.

2.3 Lessor underretter omgående Kunden, hvis en instruks efter Lessors mening er i strid med Persondataforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

2.4 Kunden garanterer over for Lessor, at denne har fornøden ret til at behandle Personoplysninger omfattet af Databehandleraftalen og til at lade Lessor behandle disse Personoplysninger på vegne af sig, herunder men ikke begrænset til ved indsamling af relevante samtykker.

3 Krav til Lessor

3.1 Lessor skal behandle Personoplysninger i overensstemmelse med gældende dansk persondatalovgivning, herunder Persondataforordningen.

3.2 Lessor skal sikre, at de personer, der er autoriseret til at behandle Personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

3.3 Lessor skal iværksætte alle foranstaltninger, som kræves i henhold til Persondataforordningens artikel 32, herunder gennemføre de passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at de behandlede Personoplysninger

(i) hændeligt eller ulovligt tilintetgøres, fortabes eller ændres,
(ii) videregives eller gøres tilgængelige uden autorisation, eller
(iii) i øvrigt behandles i strid med lovgivningen, herunder Persondataforordningen.

3.4 Fastsættelsen af de passende tekniske og organisatoriske sikkerhedsforanstaltninger skal ske under hensyntagen til

(i) det aktuelle tekniske niveau,

(ii) omkostningerne ved implementeringen, samt

(iii) behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

3.5 Lessor skal i forbindelse med ovenstående som minimum iværksætte de tekniske og organisatoriske foranstaltninger, som er specificeret i Databehandleraftalens Appendiks 2.

3.6 Lessor skal på Kundens anmodning stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i Databehandleraftalen, til rådighed for Kunden og give mulighed for og bidrage til revisioner i overensstemmelse med Databehandleraftalen, herunder inspektioner, der foretages af Kunden eller en anden revisor, som er bemyndiget af Kunden.

3.7 Lessor skal hvert år, for egen regning, indhente en erklæring fra en uafhængig ekspert angående Lessors overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Databehandleraftalen. Erklæringen uploades på Lessors hjemmeside www.lessor.dk en gang hvert år. Lessor kan ved skriftlig meddelelse til Kunden ændre den hjemmeside, hvorpå erklæringen skal uploades.

3.8 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.

3.9 Lessor skal uden unødig forsinkelse efter at være blevet opmærksom herpå skriftligt orientere Kunden om

(i) enhver anmodning fra en myndighed om videregivelse af Personoplysninger omfattet af Databehandleraftalen, medmindre orientering af Kunden er forbudt i henhold til EU-retten eller lovgivningen i en stat, som Lessor er underlagt,

(ii) enhver mistanke om, eller konstatering af, (a) brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til Personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet af Lessor i henhold til Databehandleraftalen, eller (b) enhver anden manglende overholdelse af Lessors forpligtelser efter punkt 3.3, eller

(iii) enhver anmodning om indsigt i Personoplysningerne modtaget direkte fra den registrerede eller fra tredjemand.

3.10 Lessor skal, under hensyntagen til behandlingens karakter, så vidt muligt bistå Kunden ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af Kundens forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i Persondataforordningens kapitel III, herunder eksempelvis anmodning om indsigt, berigtigelse, blokering eller sletning.

3.11 Lessor skal bistå Kunden med at sikre overholdelse af Kundens forpligtelser i medfør af Persondataforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Lessor, samt øvrige forpligtelser, der måtte påhvile Kunden efter EU-retten eller lovgivningen i en medlemsstat, hvor Lessors assistance er forudsat, dog alene i det omfang Lessors assistance er nødvendig for, at Kunden kan overholde sine forpligtelser. Dette omfatter blandt andet på anmodning at give Kunden alle nødvendige oplysninger til brug for en konsekvensanalyse i medfør af artikel 35-36 i Persondataforordningen i det omfang, Lessor har adgang til sådan information.

3.12 I Appendiks 1 har Lessor oplyst den fysiske placering af servere, servicecentre mv. som indgår i udførelsen af databehandlingen. Lessor forpligter sig til at give skriftligt varsel til Kunden forud for ændringer af den fysiske placering. Dette kræver ikke en formel ændring af Appendiks 1, forudgående skriftlig meddelelse er tilstrækkelig.

3.13 Kunden honorerer Lessor særskilt og efter medgået tid og materiale for at håndtere forespørgsler og opgaver i henhold til Databehandleraftalens pkt. 3.6, 3.8, 3.9 (i) og (iii), 3.10, 3.11 og 6.4. Honoreringen fastsættes efter Lessors til enhver tid gældende prisliste, der er tilgængelig på www.lessor.dk eller en anden hjemmeside valgt af Lessor.

4 Underdatabehandlere

4.1 Kunden giver Lessor en forudgående generel skriftlig godkendelse til at gøre brug af underdatabehandlere. På tidspunktet for indgåelsen af Databehandleraftalen anvender Lessor de i Appendiks 3 anførte underdatabehandlere. Lessor skal skriftligt underrette Kunden om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere senest 2 måneder inden ændringen træder i kraft, hvorefter Kunden inden 2 uger fra afgivelsen af meddelelsen om ændringen uden begrundelse kan gøre indsigelse mod ændringen ved at nægte brugen af den nye underdatabehandler, i hvilket tilfælde Lessor er berettiget til at opsige alle aftaler med Kunden, i henhold til hvilke Lessor behandler Personoplysninger for Kunden, med 2 måneders varsel.

4.2 Lessor skal forinden brug af en underdatabehandler indgå en skriftlig aftale med underdatabehandleren, hvori underdatabehandleren som minimum pålægges forpligtelser svarende til dem, som Lessor har påtaget sig ved Databehandleraftalen, herunder pligten til at gennemføre passende tekniske og organisatoriske foranstaltninger til sikring af, at behandlingen opfylder kravene i Persondataforordningen.

4.3 Kunden har ret til at få udleveret en kopi af de dele af Lessors aftale med en underdatabehandler, som vedrører databeskyttelsesforpligtelser, som er obligatoriske i henhold til punkt 4.2.

4.4 Hvis en underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver Lessor fuldt ansvarlig over for Kunden for opfyldelsen af underdatabehandlerens forpligtelser.

5 Ændringer

5.1 Parterne kan til enhver tid aftale at ændre Databehandleraftalen. Ændringer skal være skriftlige.

6 Varighed og ophør af Databehandleraftalen

6.1 Databehandleraftalen træder i kraft på samme tidspunkt som Aftalen, som

Databehandleraftalen udgør et Bilag til, og er gældende indtil Aftalen ophører.

6.2 Hver Part kan opsige Databehandleraftalen efter samme vilkår, som er gældende for Aftalen, som Databehandleraftalen udgør et bilag til.

6.3 Uanset Databehandleraftalens formelle aftaleperiode skal Databehandleraftalen vedblive at gælde, så længe Lessor som databehandler behandler Personoplysninger for Kunden, som Kunden er dataansvarlig for.

6.4 Lessor skal efter Kundens valg slette eller tilbagelevere alle Personoplysninger til Kunden, efter at Aftalen er ophørt, og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af Personoplysningerne.

7 Meddelelser

7.1 I det tilfælde en Part i henhold til Databehandleraftalen skal afgive skriftlig meddelelse til den anden Part, kan denne pligt opfyldes ved at afsende en e-mail til den anden Parts senest oplyste e-mailadresse.

8 Forrang

8.1 I tilfælde af uoverensstemmelse mellem bestemmelserne i Databehandleraftalen og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem Parterne, skal bestemmelserne i Databehandleraftalen have forrang, medmindre andet eksplicit er aftalt mellem Parterne.

APPENDIKS 1

Dette Appendiks indeholder blandt andet Kundens instruks til Lessor i forbindelse med Lessors databehandling for Kunden og er en integreret del af Databehandleraftalen. Instruksen afhænger af, hvilke programmer Kunden har indgået aftale om med Lessor og derved opnået licens til.
Såfremt data ikke hostes ved Lessor, vil Lessor alene have adgang til data og alene behandle data i forbindelse med særlige aftaler herom med Kunden, 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.

Behandlingen af Personoplysninger og instruks vedrørende LessorRefusion:

Formål og karakteren af databehandlingen i Lessor Refusion

Formålet med at lade Lessor foretage databehandlingen er at lade Kunden anvende Lessor Refusion og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor Refusion anvendes som Kundens værktøj til at anmelde og anmode om udbetaling af refusion på baggrund af medarbejdernes fravær som følge af sygdom og barsel. Endvidere kan Kunden se forventet refusion og modtaget refusion, samt status på refusionssagerne.
Medarbejdernes fravær kan synkroniseres fra Lessor Portalen, Lessor SP Tid eller første fraværsdag kan tastes direkte i Lessor Refusion
Kategorier af registrerede personer for hvilke der registreres data
a) [Kundens nuværende ansatte]

Kategorier af Personoplysninger der behandles
Re a)
CPR-nummer, navn, adresse, ansættelsesforhold, fraværsregistreringer, orlovsregistreringer, løndata, loginoplysninger (krypteret og fødselsdato for nyfødte)

Behandlingen af Personoplysninger og instruks vedrørende Lessor Payroll, Lessor Time & Attendance og Lessor Human Resources til Microsoft Dynamics

Formål og karakteren af databehandlingen i Lessor Payroll, Lessor Time & Attendance og Lessor Human Resources til Microsoft Dynamics
Formålet med at lade Lessor foretage databehandlingen er at yde Kunden support- og/eller konsulentopgaver i forbindelse med Kundens brug af Lessors programmer til Microsoft Dynamics. Lessor vil kunne have behov for adgang til og udtræk fra Kundens miljø og dermed Personoplysninger deri for at kunne udføre sådanne opgaver. Personoplysningerne behandles med det formål at yde af Kunden efterspurgte support- og/eller konsulentydelser. Det bemærkes at programmerne ikke hostes

af Lessor, men af Kunden selv eller af tredjepart. Assistancen kan foregå ved, at Kunden beder den partner, som Kunden 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 Kunden. Data kan synkroniseres med enten Lessors Portal samt andre eksterne systemer der understøtter Lessor Integration Framework (LIF).

Kategorier af registrerede personer for hvilke der registreres data
a) De personer, som Kunden 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 Kunden.

Kategorier af Personoplysninger der behandles

Re a)
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, 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.

Behandlingen af Personoplysninger og instruks vedrørende Lessor 4

Formål og karakteren af databehandlingen i Lessor 4
Formålet med at lade Lessor foretage databehandlingen er at lade Kunden 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 Kundens valg.

Kategorier af registrerede personer for hvilke der registreres data i Lessor 4
a) Kundens nuværende medarbejdere
b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i Lessor 4

Re a)

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.

Re b)
CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, orlovs registreringer, løndata, pensions informationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende Lessor 4 Tid

Formål og karakteren af databehandlingen i Lessor 4 Tid
Formålet med at lade Lessor foretage databehandlingen er at lade Kunden 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.

Kategorier af registrerede personer for hvilke der registreres data i Lessor 4 Tid
a) Kundens nuværende medarbejdere
b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i Lessor 4 Tid
Re a)
CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, komme/gå registreringer, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger(krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Re b)
CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, komme/gå

registreringer, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger(krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende LessorLøn (tidligere benævnt Lessor 5)

Formål og karakteren af databehandlingen i LessorLøn
Formålet med at lade Lessor foretage databehandlingen er at lade Kunden 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.

Kategorier af registrerede personer for hvilke der registreres data i LessorLøn
a) Kundens nuværende medarbejdere
b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i LessorLøn

Re a)
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.

Re b)
CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mailadresse, ansættelsesforhold, fraværsregistreringer, orlovsregistreringer, løndata, pensions informationer, skattekortoplysninger, familiemedlemmer, medlemskaber, kompetencer, arbejdsskader, uddannelse og kurser, statsborgerskab, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende Lessor PM

Formål og karakteren af databehandlingen i Lessor PM

Formålet med at lade Lessor foretage databehandlingen er at lade Kunden anvende Lessor PM 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). Lessor PM har mulighed for integration til Skat, hvortil og fra der sendes og modtages data. Lønsedler kan sendes til e-Boks såfremt dette er valgt. Betalinger kan overføres af Kunden til Nets eller bank.

Kategorier af registrerede personer for hvilke der registreres data i Lessor PM
a) Kundens nuværende medarbejdere
b) Kundens tidligere medarbejdere
c) Ansøgere til ledige stillinger hos Kunden

Kategorier af Personoplysninger der behandles i Lessor PM

Re 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 Kunden selv indberetter til Systemet.

Re b)
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 Kunden selv indberetter til Systemet.

Re c) CPR-nummer, navn, adresse, alder, køn, stillingsbetegnelse, civil status, telefonnumre, e-mail, CV, ansøgninger, samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende Lessor Portalen

Formål og karakteren af databehandlingen i Lessor Portalen
Formålet med at lade Lessor foretage databehandlingen er at lade Kunden anvende Lessor Portalen og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor Portalen 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.

Kategorier af registrerede personer for hvilke der registreres data i Lessor Portalen

a) Kundens nuværende medarbejdere

b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i Lessor Portalen

Re a)

Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, lønsedler, fraværsoplysninger, kørselsoplysninger, komme/gå-oplysninger, rejseoplysninger, kompetencer, uddannelse, pårørende, personlige dokumenter, loginoplysninger (krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Re b)

Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, lønsedler, fraværsoplysninger, kørselsoplysninger, komme/gå-oplysninger, rejseoplysninger, kompetencer, uddannelse, Pårørende, personlige dokumenter, Loginoplysninger (krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende Lessor SP TID

Formål og karakteren af databehandlingen i Lessor SP TID

Formålet med at lade Lessor foretage databehandlingen er at lade Kunden anvende Lessor SP TID og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor SP 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.

Kategorier af registrerede personer for hvilke der registreres data i Lessor SP TID

a) Kundens nuværende medarbejdere

b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i Lessor SP TID

Re a)
CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, komme/gå registreringer, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger(krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Re b)
CPR-nummer, navn, adresse, køn, telefonnumre, e-mailadresse, ansættelsesforhold, stillingsbetegnelse, kontaktoplysninger, pårørende, fraværsoplysninger, saldi, vagtplaner, komme/gå registreringer, kompetencer, sygesamtaleoplysninger, personlige dokumenter, loginoplysninger(krypteret), samt alle oplysninger som Kunden selv indberetter til Systemet.

Behandlingen af Personoplysninger og instruks vedrørende Lessor Workforce

Formål og karakteren af databehandlingen i Lessor Workforce
Formålet med at lade Lessor foretage databehandlingen er at lade Kunden anvende Lessor Workforce og funktionerne heri samt yde support og konsulentassistance til denne brug. Lessor Workforce 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.

Kategorier af registrerede personer for hvilke der registreres data i Lessor Workforce
a) Kundens nuværende medarbejdere
b) Kundens tidligere medarbejdere

Kategorier af Personoplysninger der behandles i Lessor Workforce

Re a)
Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, fraværsoplysninger, vagtplaner, komme/gå-registreringer, kompetencer, personlige dokumenter, samt alle oplysninger som Kunden selv indberetter til Systemet.

Re b)
Ansættelsesforhold, CPR-nummer, navn, stillingsbetegnelse, kontaktoplysninger, fraværsoplysninger, vagtplaner, komme/gå-registreringer, kompetencer, personlige dokumenter, samt alle oplysninger som Kunden selv indberetter til Systemet.

Lokationer for behandlingen

Primær lokation (Datacenter og medarbejderadgang til data (fx ved support))

3450 Allerød

Danmark

Sekundær lokation (Back-up og medarbejderadgang til data (fx ved support))

7100 Vejle

Danmark

Videregivelse af data

Afhængig af det af Kunden brugte system og såfremt Lessor hoster det af Kunden brugte system, kan Lessor videregive Personoplysninger på vegne af Kunden som led i Lessors services til Kunden, herunder eksempelvis til SKAT, pensionsselskaber, NETS, Danmarks Statistik, KOMBIT m.fl.

Appendiks 2

Introduktion

Lessor anvender en risikobaseret tilgang til IT-sikkerhed og beskyttelse af de Personoplysninger, vi behandler om vores Kunder og vores Kunders medarbejdere. Lessor har fastsat nedenstående tekniske og organisatoriske sikkerhedsforanstaltninger for at mitigere de risici, der er forbundet med behandling af Personoplysninger i Lessors systemer, hvor Lessor agerer som databehandler for Kunden. 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 Kunden selv, beskrives Lessors sikkerhedsforanstaltninger nedenfor opdelt for disse to leveringsformer.

Re a) 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, og
- 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.

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.

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 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.

Re b) 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 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.

APPENDIKS 3 - angivelse af nuværende underdatabehandlere

I tilfælde hvor Kundens løsning er hostet af Lessor, samarbejder Lessor med Post Danmark A/S, der, såfremt dette er aftalt med Kunden, muliggør udsendelse af lønsedler via e-Boks.

Post Danmark A/S

Hedegaardvej 88

2300 København S

Denmark

I tilfælde hvor Systemet benyttes til at sende SMS-beskeder til Kundens ansatte, samarbejder Lessor med Compaya A/S, der håndterer udsendelse af SMS'er.

Compaya A/S

Palægade 4, 2. tv

1261 København K

Danmark

I tilfælde, hvor Kunden anvender Lessor AX Payroll, anvender Lessor SaPagi til udførelsen af datakontroller, bug-søgninger og applikationstests mv.

SaPagi ApS

Nordre Strandvej 173

3140 Ålgårde

Danmark