DATABEHANDLERAFTALE

Bilag til Aftale om Danløn

Denne databehandleraftale er et bilag til den mellem Parterne indgåede Aftale om Danløn ("Aftalen om Danløn") og udgør en integreret del deraf jf. Aftalen om Danløns bestemmelser vedrørende persondata.

Der indgås hermed følgende databehandleraftale ("Aftalen") mellem "Kunden" (den juridiske enhed der benævnes Kunden i Aftalen om Danløn) og Danske Lønsystemer A/S, CVR nr.: 15611472, Engholm Parkvej 8, 3450 Allerød ("Leverandøren"), der samlet benævnes "Parterne" og separat en "Part":

1 Aftalens omfang

1.1 Leverandøren er databehandler for Kunden, idet Leverandøren varetager de i Appendiks 1 beskrevne databehandlingsopgaver for Kunden.

1.2 De personoplysninger, der behandles af Leverandøren, formålene med behandlingen, kategorierne af personoplysninger og kategorierne af registrerede personer, er anført i Appendiks 1.

1.3 Aftalen regulerer alene den behandling af personoplysninger, som Leverandøren foretager for Kunden som databehandler.

1.4 Ved "personoplysning" 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 Leverandøren behandler alene 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 Leverandøren er underlagt. I så fald underretter Leverandøren Kunden om dette retlige krav, inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

2.2 Instruks: Leverandøren er instrueret i alene at behandle personoplysningerne med

det formål at varetage de i Appendiks 1 fastsatte databehandlingsopgaver.

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

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

3 Krav til Leverandøren

3.1 Leverandøren skal behandle personoplysninger i overensstemmelse med gældende dansk persondatalovgivning, herunder Persondataforordningen.

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

3.3 Leverandøren 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 Leverandøren skal endvidere overholde de lovgivningsmæssige krav til sikkerhedsforanstaltninger, som direkte forpligter Leverandøren, herunder kravene til sikkerhedsforanstaltninger i det land, hvor Leverandøren er etableret, eller i det land, hvor databehandlingen finder sted.

3.5 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.

3.6 Leverandøren skal i forbindelse med ovenstående som minimum iværksætte de tekniske og organisatoriske foranstaltninger, som er specificeret i Aftalens Appendiks 3.

3.7 Leverandøren 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.

3.8 Leverandøren skal hvert år, for egen regning, indhente en erklæring fra en uafhængig ekspert angående Leverandørens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Aftalen. Erklæringen uploades på Leverandørens hjemmeside www.danlon.dk en gang hvert år. Leverandøren kan ved skriftlig meddelelse til Kunden ændre den hjemmeside, hvorpå erklæringen skal uploades.

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

3.10 Leverandøren 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 Aftalen, medmindre orientering af Kunden er forbudt i henhold til EU-retten eller lovgivningen i en stat, som Leverandøren 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 Leverandøren i henhold til Aftalen, eller (b) enhver anden manglende overholdelse af Leverandørens forpligtelser efter punkt 3.3 og 3.4, eller

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

3.11 Leverandøren 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.

3.12 Leverandøren 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 Leverandøren, samt øvrige forpligtelser, der måtte påhvile Kunden efter EU-retten eller lovgivningen i en medlemsstat, hvor Leverandørens assistance er forudsat, dog alene i det omfang_Leverandørens assistance er nødvendig for, at Kunden kan overholde sine forpligtelser. Dette omfatter blandt andet, på anmodning at give Kunden alle nødvendige oplysninger om en hændelse omfattet af punkt 3.10 (ii), samt alle nødvendige oplysninger til brug for en konsekvensanalyse i medfør af artikel 35-36 i Persondataforordningen i det omfang, Leverandøren har adgang til sådan information.

3.13 I Appendiks 1 har Leverandøren oplyst den fysiske placering af servere, servicecentre mv. som indgår i udførelsen af databehandlingen. Leverandøren 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.

3.14 Kunden honorerer Leverandøren særskilt og efter medgået tid og materiale for at håndtere forespørgsler og opgaver i henhold til Aftalens pkt. 3.7, 3.9, 3.10 (i) og (iii), 3.11, 3.12, 6.4 og 6.5. Honoreringen fastsættes efter Leverandørens til enhver tid gældende prisliste, der er tilgængelig på www.danlon.dk eller en anden hjemmeside valgt af Leverandøren.

4 Underdatabehandlere

4.1 Kunden giver Leverandøren en forudgående generel skriftlig godkendelse til at gøre brug af underdatabehandlere. På tidspunktet for indgåelsen af Aftalen anvender Leverandøren de i Appendiks 2 anførte underdatabehandlere. Leverandøren 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 Leverandøren er berettiget til at opsige alle aftaler med Kunden, i henhold til hvilke Leverandøren behandler personoplysninger for Kunden, med 1 måneds varsel.

4.2 Leverandøren skal forinden brug af en underdatabehandler indgå en skriftlig aftale med underdatabehandleren, hvori underdatabehandleren som minimum pålægges forpligtelser svarende til dem som Leverandøren har påtaget sig ved Aftalen, 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 Leverandørens 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 Leverandøren fuldt ansvarlig over for Kunden for opfyldelsen af underdatabehandlerens forpligtelser.

5 Ændringer og overdragelser

5.1 Aftalen kan ændres i henhold til Aftalen om Danløns bestemmelser om ændringer.

5.2 Leverandøren kan overdrage sine rettigheder og forpligtelser i henhold til Aftalen uden Kundens samtykke, forudsat at den, til hvem rettigheder og/eller pligter overdrages, forpligtes til at behandle personoplysninger i overensstemmelse med de krav, der gælder for Leverandøren, i henhold til Aftalen.

6 Varighed og ophør af Aftalen

6.1 Aftalen træder i kraft på samme tidspunkt, som Aftalen om Danløn og er gældende indtil Aftalen om Danløn ophører.

6.2 Hver Part kan opsige Aftalen efter samme vilkår, som er gældende Aftalen om Danløn.

6.3 Uanset Aftalens formelle aftaleperiode skal Aftalen vedblive at gælde, så længe Leverandøren som databehandler behandler personoplysninger for Kunden, som Kunden er dataansvarlig for.

6.4 I tilfælde af ophør af Aftalen er Leverandøren forpligtet til efter anmodning loyalt at medvirke til, at databehandlingen overgår til en anden leverandør eller tilbageføres til Kunden.

6.5 Leverandøren 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 Aftalen 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. Leverandøren kan ligeledes opfylde sin pligt til at afgive skriftlig meddelelse ved at udsende nyheder direkte i systemet, som kunden har fået tildelt en licens til at benytte i henhold til Aftalen om Danløn.

8 Forrang

8.1 I tilfælde af uoverensstemmelse mellem bestemmelserne i Aftalen og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem Parterne, skal bestemmelserne i Aftalen have forrang

APPENDIKS 1

Dette Appendiks indeholder blandt andet Kundens instruks til Leverandøren i forbindelse med Leverandørens databehandling for Kunden og er en integreret del af Aftalen.

Instruks og beskrivelse af behandlingen af personoplysninger i Danløn

Formål og karakteren af databehandlingen

Formålet med at lade Leverandøren foretage databehandlingen er at lade Kunden anvende Danløn, der er et IT-system, som Kunden tilgår via internettet, og som er hostet og drevet af Leverandøren. Danløn hjælper med at håndtere Kundens lønafregning, skatte- og pensionsforhold for Kundens medarbejdere, administration af medarbejdernes ferieopsparing og udbetaling m.v. Dette indebærer også videregivelse af oplysninger på vegne af Kunden, fx til SKAT, Nets, pensionsselskaber, Danmarks Statistik m.fl. på vegne af Kunden.

Kategorier af registrerede personer

I. Kundens potentielle medarbejdere hvis kunden indtaster information om disse i Danløn.
II. Kundens nuværende medarbejdere hvis kunden indtaster information om disse i Danløn.
III. Kundens fratrådte medarbejdere hvis kunden indtaster information om disse i Danløn.

Kategorier af personoplysninger

For de ovenfor nævnte personkategorier, behandles navn, adresse, CPR-nummer og ansættelsesdato. Derudover behandles oplysninger vedrørende de registreredes lønforhold, såsom løn, skat, pension, ferie, udlæg, kørselspenge mv, herunder de oplysninger som Kunden registrerer om de registrerede i Danløn. For optimal udnyttelse af DANLØN registreres også e-mailadresse, mobiltelefonnummer og bankkontooplysninger.
For personerne i kategori III registreres tillige fratrædelsesdato.

Særlige kategorier af personoplysninger

Afhængigt af hvilken feriepengemodtager den registrerede persons feriepenge skal afregnes til, kan det udledes hvilken fagforeningstilknytning personen har.

Lokation(er), inklusive angivelse af land for behandlingen

Gydevang 46
3450 Allerød
Danmark

Skomagervej 10
7100 Vejle
Danmark

Videregivelse af data

Leverandøren kan videregive persondata på vegne af Kunden som led i Leverandørens services til kunden, herunder eksempelvis til SKAT, pensionsselskaber, NETS, Danmarks Statistik m.fl.

APPENDIKS 2

Brug af underdatabehandlere

Leverandøren samarbejder 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

Appendiks 3

Introduktion

Leverandøren anvender en risikobaseret tilgang til IT-sikkerhed og beskyttelse af de personoplysninger, vi behandler om vores kunder og vores kunders medarbejdere. Leverandøren har fastsat nedenstående tekniske og organisatoriske sikkerhedsforanstaltninger for at mitigere de risici, der er forbundet med behandling af personoplysninger i Danløn, hvor Leverandøren agerer som databehandler for Kunden. Leverandøren 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.

Fysisk sikkerhed i Leverandørens lokaler og datacentre

Leverandøren 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 Leverandørens faciliteter og datacentre.

Der er implementeret alarmsystemer i Leverandørens 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.

Leverandøren 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.
Leverandørens interne netværk kan kun tilgås af dertil autoriserede personer.

Kryptering

Der anvendes effektiv og stærk kryptering baseret på en anerkendt algoritme ved transmission af personoplysninger via internettet og/eller e-mail.
Kundens UserID (brugernavn) og password krypteres ved brug af en anerkendt algoritme.

Back-up og tilgængelighed

De tekniske foranstaltninger og Leverandørens systemer testes løbende ved sårbarhedsscanninger og penetrationstests.
Alle ændringer til systemer, databaser og netværk følger fastlagte Change Mangement 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 indenfor medarbejderens arbejdsområde.
Der er fastsat procedurer for at sikre, at fratrædende medarbejdere bliver frataget deres tildelte brugerrettigheder.

Leverandøren har implementeret en passwordpolitik, der er med til at sikre at medarbejderes adgangskoder ikke kommer uvedkommende til hænde, samt at der kun godkendes adgangskoder, der er tilstrækkeligt komplicerede og at adgangskoder skiftes regelmæssigt.
Der er etableret beskyttelse af flytbare enheder. Medarbejderes laptop computere er bl.a. beskyttet med anerkendt kryptering og passwords på harddiskdrev-niveau. Der anvendes desuden VPN-forbindelse og to-faktor autentificering ved fjernadgang.
Eksterne personer, der færdes på Leverandørens lokationer og i datacentre, hvor der potentielt er adgang personoplysninger, informeres om Leverandørens sikkerhedsregler og underskriver en fortrolighedserklæring.

Kontroller

Leverandøren 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 Leverandøren 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 Leverandøren har etableret og opretholder et tilstrækkeligt IT-sikkerhedsniveau.