INTERNE RETNINGSLINJER FOR PERSONDATABEHANDLING

1. GENERELLE BESTEMMELSER

1.1. Disse retningslinjer er udarbejdet med henblik på at fastlægge rammerne for, hvorledes personoplysninger behandles internt hos Wax Facility Service ApS (herefter "Virksomheden").

1.2. Formålet med disse retningslinjer er at sikre Virksomhedens overholdelse af 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 05/46/EF (herefter "Databeskyttelsesforordningen").

1.3. Retningslinjerne vil blive gennemgået med samtlige af Virksomhedens medarbejdere, i hvilken forbindelse de vil blive tilbudt rådgivning og instruktion, såfremt indholdet af retningslinjerne måtte give anledning til spørgsmål.

1.4. Ved tvivlsspørgsmål i relation til efterlevelsen af disse retningslinjer henstilles medarbejderne til at kontakte Virksomhedens til enhver tid siddende Direktør.

1.5. Som dokumentation for den enkelte medarbejders kendskab til disse retningslinjer, vedlægges som bilag 01, medarbejdernes underskrevne erklæringer herom.

1.6. Virksomhedens forretningsgange vil blive indrettet under hensyntagen til nærværende retningslinjer, således at det sikres, at enhver indhentelse og behandling af personoplysninger sker på en sikker og gennemsigtig måde for den registrerede.

1.7. Som bilag til retningslinjerne vedlægges Virksomhedens medarbejdererklæringer, risikovurdering, persondatapolitik, samtykkeerklæring, fortegnelser over behandlingsaktiviteter, samt databehandleraftaler.

2. INDHENTELSE AF PERSONOPLYSNINGER, KUNDER

2.1. <u>Dataminimering</u>

2.1.1. Virksomhedens indhentelse af personoplysninger fra kunder vil blive tilrettelagt således, at omfanget heraf begrænses til det minimum, som er nødvendigt for at opnå det konkrete formål.

2.1.2. I forhold til Virksomhedens kunder indebærer målet om dataminimering, at disse kun vil blive forespurgt om de oplysninger, som er nødvendige med henblik på fakturering og levering af den ønskede ydelse, samt at de indhentede oplysninger kun vil blive opbevaret i det tidsrum, som er nødvendigt med henblik på varetagelsen af aftaleforholdet.

2.1.3. For at sikre dataminimeringen vil Virksomhedens kontaktformularer blive udformet således, at der kun anmodes om de oplysninger, som er nødvendige for at tilgodese den enkelte aftaleform, ligesom Virksomhedens medarbejdere vil blive instrueret i, hvilke personoplysninger, som bør indhentes i forbindelse med den enkelte aftaleform.

2.2. <u>Behandlingsgrundlag</u>

2.2.1. I forbindelse med Virksomhedens udbud af tjenesteydelser, vil der blive udvekslet en række personoplysninger mellem kunden og Virksomheden.

2.2.2. De udvekslede oplysninger vil, som udgangspunkt, omfatte navn, adresse, e-mail, telefonnummer og betalingsoplysninger, hvorfor der alene vil blive indhentet og behandlet almindelige personoplysninger.

2.2.3. Indhentelsen vil ske med det formål at effektuere leveringen og betalingen i relation til opfyldelsen af den enkelte aftale, hvilken vil blive igangsat på kundens forudgående anmodning.

2.2.4. Virksomhedens hjemmeside www.waxfs.dk anvender cookies, som registrerer IP-adresse, søgehistorik og lignende med henblik på optimering af brugeroplevelsen, samt undersøgelse af adfærdsmæssige mønstre til brug for markedsføring.

2.3. Procedure

2.3.1. Virksomhedens indhentelse af personoplysninger fra kunder vil ske gennem kontaktformularen på Virksomhedens hjemmeside www.waxfs.dk, per e-mail og per telefon.

2.3.2. I forbindelse med indhentelsen, vil kunden altid blive orienteret om indholdet af Virksomhedens persondatapolitik, bilag 03.

2.3.3. Persondatapolitikken vil være frit tilgængeligt på Virksomhedens hjemmeside under fanebladet "Persondatapolitik", ligesom der vil blive indsat en henvisning hertil i medarbejdernes e-mailsignatur.

2.3.4. Ved telefonisk henvendelse vil medarbejderen mundtligt orientere om persondatapolitikken, i hvilken forbindelse kunden vil blive opfordret til at læse nærmere på hjemmesiden.

2.3.5. Ved skriftlig henvendelse vil medarbejderen skriftligt orientere om persondatapolitikken ved enten at henvise hertil eller direkte vedhæfte denne i sit svar, såfremt dette skønnes nødvendigt.

2.3.6. Virksomheden vil endvidere udlevere en flyer til kunden med henvisning til persondatapolitikken i forbindelse med udførelsen af den enkelte opgave, ligesom den udstedte faktura vil indeholde en eksplicit henvisning hertil.

2.3.7. De indhentede oplysninger, samt eventuelle bilag, vil blive registeret i SkvizBiz, hvorefter eventuelle genparter vil blive slettet.

2.3.8. Cookies lagres automatisk ved besøg på hjemmesiden. Den besøgende orienteres herom ved sit første besøg og kan altid fravælge brug af cookies, samt slette allerede lagrede cookies. Der henvises til cookiepolitikken på www.waxfs.dk.

3. INDHENTELSE AF PERSONOPLYSNINGER, PERSONALEADMINISTRATION

3.1. Dataminimering

3.1.1. Virksomhedens indhentelse og behandling af personoplysninger fra nuværende og tidligere medarbejdere, samt ansøgere, vil blive tilrettelagt således, at omfanget heraf begrænses til det minimum, som er nødvendigt for at opnå det konkrete formål.

3.1.2. I forhold til Virksomhedens medarbejdere indebærer datamineringen, at Virksomheden kun vil forespørge disse om oplysninger, som konkret er nødvendige med henblik på varetagelsen af

ansættelsesforholdet, samt at de indhentede oplysninger kun vil blive opbevaret i det tidsrum, som er nødvendigt med henblik på varetagelsen af behandlingens formål.

3.1.3. Virksomhedens HR-medarbejdere vil endvidere blive instrueret i kun at registrere oplysninger om medarbejderne i det omfang dette må anses som nødvendigt i forhold til varetagelsen af ansættelsesforholdet, ligesom enhver unødvendig oplysning vil blive slettet uanset dennes oprindelse.

3.1.4. Dataminimeringen sikres i forhold til ansøgere af stillinger i Virksomheden ved udformningen af Virksomhedens jobopslag, hvor Virksomheden som udgangspunkt kun vil anmode ansøgere om at angive navn, adresse, alder mv., samt dokumentere eventuelle faglige kvalifikationer. En ansøger vil som udgangspunkt kun blive anmodet om at afgive følsomme oplysninger i det omfang dette skønnes særligt relevant i forhold til vurderingen af dennes evne til at varetage den konkrete stilling.

3.2. <u>Behandlingsgrundlag</u>

3.2.1. I forbindelse med Virksomhedens personaleadministration vil der blive udvekslet en række personoplysninger mellem medarbejderen og Virksomheden.

3.2.2. De udvekslede oplysninger vil som udgangspunkt omfatte navn, adresse, e-mail, telefonnummer og betalingsoplysninger, idet varetagelsen af det enkelte ansættelsesforhold kan indebære, at Virksomheden ligeledes indhenter billede, personnummer, samt oplysninger om helbreds- og fagforeningsmæssige forhold, samt eventuel straffeattest.

3.2.3. Indhentelse og behandling af almindelige personoplysninger fra Virksomhedens medarbejdere vil ske med hjemmel i ansættelseskontrakten eller ud fra en konkret interesseafvejning, mens indhentelse og behandling af følsomme oplysninger vil foregå som led i overholdelsen af Virksomhedens eller medarbejderens arbejds- og offentligretlige forpligtelser, jævnfør dog nærmere nedenfor.

3.2.4. Indhentelse og behandling af medarbejderfotos til brug for Virksomhedens markedsføring på egen hjemmeside, sociale medier og lign. vil alene blive påbegyndt efter indhentelse af medarbejderens samtykke ved brug af Virksomhedens samtykkeerklæring, bilag 04.

3.2.5. Indhentelse og behandling af almindelige personoplysninger fra ansøgere vil ske ud fra en konkret interesseafvejning eller på baggrund af ansøgerens forudgående anmodning om indgåelse af en ansættelseskontrakt.

3.2.6. Indhentelse og behandling af straffeattest fra ansøgere/medarbejdere vil alene ske i det omfang dette konkret skønnes relevant, og vil udelukkende ske efter indhentelse af ansøgerens/medarbejderens samtykke ved brug af Virksomhedens samtykkeerklæring, bilag 05. Efter forevisning af straffeattest, vil denne blive slettet.

3.2.7. Indhentelse og behandling af almindelige personoplysninger fra ansøgere vil ske ud fra en konkret interesseafvejning eller på baggrund af ansøgerens forudgående anmodning om indgåelse af en ansættelseskontrakt.

3.3. <u>Procedure</u>

3.3.1. Virksomhedens indhentelse af personoplysninger om medarbejdere og ansøgere vil ske ved brug af e-mail, almindelig post, fysisk overlevering eller per telefon.

3.3.2. I forbindelse med indhentelsen, vil medarbejderen/ansøgeren altid blive orienteret om Virksomhedens persondatapolitik, bilag 03, hvilken vil fremgå af det enkelte stillingsopslag, ligesom den vil blive fremsendt ved Virksomhedens bekræftelse på modtagelsen af ansøgningen.

3.3.3. Persondatapolitikken vil endvidere være frit tilgængeligt på Virksomhedens hjemmeside under fanebladet "Persondatapolitik" og vil blive vedlagt ansættelseskontrakten, ligesom der vil blive indsat en henvisning hertil i medarbejdernes e-mailsignatur.

3.3.4. Ved brug af medarbejderfoto vil medarbejderen blive præsenteret for Virksomhedens samtykkeerklæring, bilag 04, hvorefter behandlingen først vil blive påbegyndt efter modtagelsen af medarbejderens samtykke.

3.3.5. Ved indhentelse af straffeattest, vil medarbejderen/ansøgeren blive præsenteret for Virksomhedens samtykkeerklæring, bilag 05, hvorefter behandlingen først vil blive påbegyndt efter modtagelsen af medarbejderens/ansøgerens samtykke. Efter forevisning af straffeattest, vil denne blive slettet.

3.3.6. De indhentede oplysninger, samt dertilhørende bilag, vil blive registeret i Virksomhedens fysiske medarbejderkartotek, hvorefter eventuelle genparter slettes.

4. BEHANDLING AF PERSONOPLYSNINGER

4.1. Virksomhedens behandling af personoplysninger vil blive tilrettelagt således, at omfanget heraf begrænses til det minimum, som er nødvendigt for at opnå det konkrete formål.

4.2. Virksomheden vil alene behandle de indhentede personoplysninger med henblik på at tilgodese det angivne formål ved indhentelsen, idet en videregående brug udelukkende vil finde sted, såfremt denne konkret skønnes forenelig med det oprindelige formål.

4.3. Virksomheden vil løbende sikre datakvaliteten ved at korrigere eventuelle fejl i de registrerede oplysninger, ligesom det regelmæssigt vil blive vurderet, hvorvidt behandlingen af de pågældende oplysninger fortsat er nødvendig.

5. LAGRING AF PERSONOPLYSNINGER

5.1. Virksomhedens persondatabehandling er baseret på et princip om dataminimering, hvorfor enhver personoplysning løbende vil blive slettet, såfremt det konkret vurderes, at opbevaringen ikke tjener et anerkendelsesværdigt formål.

5.2. Virksomheden vil, som minimum, foretage en årlig revision af SkvizBiz, samt det fysiske medarbejderkartotek med henblik på sletning af unødvendige personoplysninger.

5.3. Som generelle retningslinjer, opstilles følgende vejledende slettefrister:

a) Regnskabs- og betalingsoplysninger vil blive opbevaret i 5 år med henblik på overholdelse af Bogføringslovens dokumentationskrav.

b) Jobansøgninger vil blive opbevaret i 6 måneder efter modtagelsen med henblik på kontakt i forbindelse med eventuelle genopslag.
c) Personalesager vil blive opbevaret i 5 år med henblik på varetagelsen af eventuelle efterfølgende krav i anledning af ansættelsesforholdet.

6. VIDEREGIVELSE AF PERSONOPLYSNINGER

6.1. Virksomheden vil udelukkende videregive personoplysninger til tredjeparter i det omfang dette måtte være nødvendigt med henblik på varetagelsen af det angivne formål med indhentelsen heraf, ligesom videregivelsen skal være omfattet af det konkrete behandlingsgrundlag.

6.2. Virksomheden vil ved indhentelsen af personoplysninger orientere om de eventuelle kategorier af tredjeparter, som personoplysningerne vil blive videregivet til.

6.3. I forbindelse med faktureringen af Virksomhedens tjenesteydelser vil navn, adresse og kontooplysninger, som udgangspunkt, blive videregivet til de parter som er involverede i den konkrete betalingstransaktion, herunder bl.a. pengeinstitut, kortudsteder og lign.

6.4. I forbindelse med varetagelsen af personaleadministration vil både almindelige og særligt følsomme oplysninger, som udgangspunkt blive videregivet til relevante offentlige myndigheder, som f.eks. SKAT, ligesom der vil kunne forekomme videregivelse til pensionskasser, lønadministrator, fagforeninger og lign.

6.5. I det tilfælde en videregivelse måtte ligge uden for det oprindelige formål eller ikke er omfattet af den oprindelige behandlingsgrundlag, vil Virksomheden forudgående orientere den registrerede herom, samt eventuelt indhente samtykke til videregivelsen.

7. DEN REGISTREREDES RETTIGHEDER

7.1. Den registrerede vil, som udgangspunkt, have følgende rettigheder i forbindelse med behandlingen af dennes personoplysninger:

a) Ret til at få indsigt i de indhentede oplysninger
b) Ret til at få berigtiget de indhentede oplysninger
c) Ret til at få overført de indhentede oplysninger i et læsbart format
d) Ret til at få begrænset behandlingen af de indhentede oplysninger
e) Ret til at få slettet de indhentede oplysninger

7.2. <u>Udøvelse af rettigheder</u>

7.2.1. I det tilfælde den registrerede ved henvendelse måtte ønske at gøre brug af de i pkt. 7.1 nævnte rettigheder skal henvendelsen som udgangspunkt besvares senest en måned efter modtagelsen heraf.

7.2.2. Ved henvendelsen skal der ske en entydig identifikation af den registrerede, idet det må sikres, at der ikke sker videregivelse af de behandlede personoplysninger til uvedkommende parter. Kravene til denne identifikation vil afhænge af de konkrete oplysningers karakter, samt henvendelsesformen.

7.2.3. Det vil, som udgangspunkt, være gratis for den registrerede at benytte sig af de i pkt. 7.1 nævnte rettigheder, idet denne dog vil kunne blive opkrævet et gebyr, såfremt dennes anmodninger måtte forekomme grundløse eller overdrevne. Den registrerede vil i disse tilfælde modtage en begrundelse for opkrævningen.

7.2.4. Såfremt en henvendelse måtte give anledning til spørgsmål, vil medarbejderen skulle kontakte Virksomhedens til enhver tid siddende Direktør.

7.3. Procedure for indsigt

7.3.1. Den registrerede har ret til at få indsigt i hvilke oplysninger Virksomheden behandler om vedkommende, samt hvilken behandling, som finder sted.

7.3.2. Ved den registreredes anmodning om indsigt vil medarbejderen skulle identificere, hvorvidt den registrerede er en kunde, medarbejder eller ansøger.

7.3.3. Efter at have identificeret den registrerede vil medarbejderen kunne fremfinde de relevante oplysninger ved opslag i enten SkvizBiz eller det fysiske medarbejderkartotek. Medarbejderen vil herefter notere de forskellige personoplysninger, som foreligger om vedkommende, samt hvorledes disse behandles af Virksomheden.

7.3.4. Medarbejderen vil sammenfatte de pkt. 7.3.3 angivne oplysninger i en mail eller et brev, som herefter vil fremsendt til den registrerede. Besvarelsen vil blive vedlagt Virksomhedens persondatapolitik, bilag 03.

7.4. Procedure for berigtigelse

7.4.1. Den registrerede har ret til at få rettet urigtige oplysninger om sig selv, samt at få fuldstændiggjort ufuldstændige oplysninger.

7.4.2. Ved den registreredes anmodning om berigtigelse vil medarbejderen skulle identificere, hvorvidt den registrerede er en kunde, medarbejder eller ansøger.

7.4.3. Efter at have identificeret den registrerede vil medarbejderen kunne fremfinde de relevante oplysninger ved opslag i enten SkvizBiz eller det fysiske medarbejderkartotek. Medarbejderen vil herefter foretage en vurdering af, hvorvidt den registreredes indsigelse er berettiget. Afhængigt af indsigelsens berettigelse vil medarbejderen enten berigtige de angivne oplysninger eller tilføje et notat om den registreredes indsigelse. Såfremt urigtige oplysninger er blevet videregivet til tredjemand, vil medarbejderen ligeledes meddele denne om berigtigelsen.

7.5. Procedure for sletning

7.5.1. Den registrerede har i visse situationer ret til at få slettet oplysninger om sig selv.

7.5.2. Ved den registreredes anmodning om sletning vil medarbejderen skulle identificere, hvorvidt den registrerede er en kunde, medarbejder eller ansøger.

7.5.3. Efter at have identificeret den registrerede vil medarbejderen kunne fremfinde de relevante oplysninger ved opslag i enten SkvizBiz eller det fysiske medarbejderkartotek.

7.5.4. Medarbejderen vil herefter foretage en vurdering af, hvorvidt et af de i Databeskyttelsesforordningen, art. 17, stk. 1, litra a-f, nævnte forhold sig gør gældende.

7.5.5. Såfremt ingen af de i Databeskyttelsesforordningen, art. 17, stk. 3, nævnte undtagelser finder anvendelse, vil medarbejderen herefter slette de angivne oplysninger og alle genparter, samt underrette tredjemand om sletningen, såfremt videregivelse har fundet sted.

7.6. Procedure for overførsel i læsbart format

7.6.1. Den registrerede har, under visse betingelser, ret til at modtage sine personoplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format, samt at få disse direkte overført til en anden dataansvarlig.

7.6.2. Ved den registreredes anmodning om at få overført sine oplysninger i et læsbart format, vil medarbejderen skulle identificere, hvorvidt den registrerede er en kunde, medarbejder eller ansøger.

7.6.3. Efter at have identificeret den registrerede vil medarbejderen kunne fremfinde de relevante oplysninger ved opslag i enten SkvizBiz eller det fysiske medarbejderkartotek.

7.6.4. Medarbejderen vil herefter foretage en vurdering af, hvorvidt et af de i Databeskyttelsesforordningen, art. 20, stk. 1, litra a-b, nævnte forhold sig gør gældende.

7.6.5. Såfremt den registreredes henvendelse vurderes at være berettiget vil medarbejderen samle de foreliggende oplysninger i en pdf-fil, som herefter vil blive sendt til den registrerede eller en ny dataansvarlig, afhængigt af den registreredes ønske.

7.7. Procedure for begrænsning

7.7.1. Den registrerede har i visse situationer ret til at få begrænset behandlingen af sine personoplysninger, således at oplysningerne ikke må underlægges anden behandling end opbevaring.

7.7.2. Ved den registreredes anmodning om begrænsning vil medarbejderen skulle identificere, hvorvidt den registrerede er en kunde, medarbejder eller ansøger.

7.7.3. Efter at have identificeret den registrerede vil medarbejderen kunne fremfinde de relevante oplysninger ved opslag i enten SkvizBiz eller det fysiske medarbejderkartotek.

7.7.4. Medarbejderen vil herefter foretage en vurdering af, hvorvidt et af de i Databeskyttelsesforordningen, art. 18, stk. 1, litra a-d, nævnte forhold sig gør gældende.

7.7.5. Såfremt den registreredes henvendelse vurderes at være berettiget vil medarbejderen foretage en mærkning af personoplysningerne med henblik på at begrænse fremtidig behandling heraf.

7.7.6. De pågældende oplysninger vil herefter alene blive behandlet, såfremt et af de i Databeskyttelsesforordningen, art. 18, stk. 2, nævnte forhold gør sig gældende.

7.7.7. Ved en eventuel senere ophævelse af begrænsningen vil den registrerede blive underrettet.

8. SIKKERHEDSPROTOKOL

8.1. Adgangskoder

8.1.1. Adgangen til Virksomhedens systemer vil være begrænset med individuelle adgangskoder for den enkelte medarbejder, hvilke regelmæssigt vil blive udskiftet med henblik på at hindre misbrug.

8.1.2. Den enkelte medarbejders adgangskode skal overholde følgende krav:

a) Minimum 8 tegn
b) Store og små bogstaver
c) Et eller flere særlige tegn, som f.eks. "!?#"

8.1.3. Medarbejderen er forpligtet til at hemmeligholde sin kode, ligesom medarbejderen til enhver tid skal have adgangskodekrav indstillet som standard på sin computer.

8.2. Adgangskontrol

8.2.1. Virksomheden opsætter kontrolforanstaltninger, hvorefter medarbejdernes adgang til personoplysninger begrænses til kun at omfatte de arbejdsområder, som vedrører den pågældende medarbejder, ligesom der foretages logning af søgehistorik i SkvizBiz.

8.2.2. I det tilfælde behandlingen af enkelte personoplysninger måtte indebære en særlig risiko for brud på persondatasikkerheden, vil der endvidere blive opsat adgangsspærring i relation til de pågældende personoplysninger hvorefter kun særligt betroede medarbejdere vil have adgang hertil.

8.3. Antivirus og firewall

8.3.1. Virksomhedens it-systemer vil, som standard, blive udstyret med både antivirus og firewall.

8.3.2. Antivirus og firewall skal ved enhver brug være slået til som standard, ligesom såvel Virksomhedens it-ansvarlige, som den enkelte medarbejder vil være forpligtet til at sikre, at disse konstant er ajourførte med de nyeste opdateringer.

8.3.3. Der vil regelmæssigt blive foretaget systemscanninger med henblik på at opdage eventuelle sikkerhedsbrister.

8.4. Hjemmeside

8.4.1. Virksomhedens hjemmeside vil blive tilknyttet en udbyder, som garanterer at overholde relevante sikkerhedsforskrifter med hensyn til beskyttelse af personoplysninger, idet udbyderen, som minimum skal sikre SSL-certificering af Virksomhedens hjemmeside.

8.5. E-mails

8.5.1. Virksomheden har til brug for dens behandling af personoplysninger oprettet krypteret e-mail hos Windows Outlook.

8.6. Server

8.6.1. Virksomhedens data er placeret på en server i EU via IT Operators.

8.7. Fysiske sikkerhedsforanstaltninger

8.7.1. For at begrænse den fysiske adgang til Virksomhedens personoplysninger opbevares det fysiske medarbejderkartotek i et aflåst skab, ligesom de enkelte kontorer vil være aflåst, såfremt

der ikke er en medarbejder til stede. Alarm vil endvidere altid være slået til, når medarbejderne forlader kontoret.

8.7.2. Nøgler til kontorerne, samt adgangskode til alarmen, vil kun blive udleveret mod underskrift fra den enkelte medarbejder. Der vil blive opretholdt kontrol med det udleverede antal nøgler og tilbagelevering ved fratrædelse. Medarbejderen må ikke få lavet kopier af nøglerne.

8.8. Databehandlere

8.8.1. Virksomheden har indgået databehandleraftaler med en række virksomheder, hvorefter disse forpligter sig udelukkende til at handle efter Virksomhedens instruks og i øvrigt overholde Databeskyttelsesforordningens krav i forbindelse med den persondatabehandling som foretages på Virksomhedens vegne, bilag 08-10.

8.9. Brud på persondatasikkerheden

8.9.1. Ved brud på Virksomhedens datasikkerhed vil der uden unødig forsinkelse ske anmeldelse til Datatilsynet, ligesom den registrerede vil blive underrettet herom, medmindre det konkret vurderes, at bruddet ikke indebærer nogen risiko for den registreredes rettigheder.

8.9.2. Underretningen til henholdsvis Datatilsynet og den registrerede vil beskrive karakteren af bruddet, ligesom denne vil indeholde anbefalinger til den registrerede med henblik på at begrænse de mulige skadevirkninger.

9. BILAGSFORTEGNELSE

Bilag 01: Medarbejdererklæringer
Bilag 02: Risikovurdering
Bilag 03: Persondatapolitik
Bilag 04: Samtykkeerklæring - Medarbejderfotos
Bilag 05: Samtykkeerklæring – Straffeattest
Bilag 06: Fortegnelse over personaleadministration
Bilag 07: Fortegnelse over kundeadministration
Bilag 08: Databehandleraftale – SkvizBiz
Bilag 09: Databehandleraftale – Visma DataLøn
Bilag 10: Databehandleraftale – IT Operators

10. LEDELSENS PÅTEGNING

10.1. Virksomheden forpligter sig hermed til at tilrettelægge sin persondatabehandling i overensstemmelse med nærværende interne retningslinjer, samt om nødvendigt løbende at ajourføre disse.

Dato:

_____

RISIKOVURDERING

1. Virksomhedens behandling af personoplysninger vil primært foregå ved brug af edb, i hvilken forbindelse det må påregnes, at oplysningerne vil blive lagret i vores it-system, ligesom disse vil kunne indgå i Virksomhedens e-mailkorrespondance.

2. I forbindelse med Virksomhedens personaleadministration vil de indhentede oplysninger blive udskrevet og vedlagt fysiske mapper.

3. Foruden den interne behandling, vil oplysningerne kunne blive gjort til genstand for videregivelse til offentlige myndigheder, betalingstjenester, løn-/økonomiadministrator og lignende tredjeparter, hvorved der ligeledes opstår en risiko for uberettiget spredning.

4. De behandlede personoplysninger omfatter primært almindelige oplysninger, idet Virksomhedens personaleadministration dog vil nødvendiggøre en vis behandling af bl.a. cpr-nummer, samt lejlighedsvis særligt følsomme oplysninger om bl.a. helbred og strafbare forhold.

5. Som følge af den begrænsede behandling af følsomme oplysninger, må risikoen for sikkerhedsbrud betragtes som værende relativ lav, idet oplysningernes almindelige karakter begrænser tredjemands interesse heri.

6. Brud på persondatadatasikkerheden vil kunne ske ved tredjemands angreb på vores it-systemer, herunder virus, malware, diverse former for hacking mv., ligesom det må påregnes, at brud på persondatasikkerheden ligeledes vil kunne forekomme som følge af utilsigtede fejl fra Virksomhedens egne medarbejdere.

7. Ved lagring i fysiske sagsmapper vil brud ligeledes kunne forekomme ved tredjemands tyveri, herunder indbrud i Virksomhedens lokaler.

8. Ovenstående risici søges imødegået ved iagttagelse af de i Virksomhedens retningslinjer for persondatabehandling angivne foranstaltninger.

SAMTYKKEERKLÆRING

Undertegnede giver hermed samtykke til, at Wax Facility Service ApS i forbindelse med ansættelse indhenter og behandler arbejdsrelaterede portrætbilleder af mig i forbindelse med virksomhedens markedsføring på egen hjemmeside, sociale medier og i lokale dagblade.

I forbindelse med behandlingen vil du ved henvendelse til Wax Facility Service ApS have mulighed for at udøve følgende rettigheder:

- Ret til at få indsigt i de indhentede oplysninger
- Ret til at få berigtiget de indhentede oplysninger
- Ret til at få overført de indhentede oplysninger i et læsbart format
- Ret til at få begrænset behandlingen af de indhentede oplysninger
- Ret til at få slettet de indhentede oplysninger

Undertegnede er bekendt med, at afgivelsen af dette samtykke er frivillig, ligesom samtykket til enhver tid vil kunne tilbagekaldes ved henvendelse til Wax Facility Service ApS.

Tilbagekaldelse og øvrige henvendelser kan adresseres til nedenstående:

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
E-mail: ck@waxfs.dk
Tlf.nr.: 28 44 26 05
Kontaktperson: Camillo Krog
CVR-nr. 32 10 20 18

Såfremt du måtte have indvendinger mod den foretagne behandling, vil du have mulighed for at indgive klage herom til Datatilsynet ved brug af følgende kontaktoplysninger:

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf. 33193200
E-mail dt@datatilsynet.dk

Dato:

_____

SAMTYKKEERKLÆRING

Undertegnede giver hermed samtykke til, at Wax Facility Service ApS i forbindelse med min anmodning om indgåelse af en ansættelseskontrakt indhenter en privat straffeattest fra Kriminalregisteret.

Formålet med indhentelsen er, at Wax Facility Service ApS ønsker at vurdere din egnethed til at bestride den pågældende stilling, i hvilken forbindelse, eventuelle strafbare forhold kan blive tillagt betydning.

I forbindelse med behandlingen vil du ved henvendelse til Wax Facility Service ApS have mulighed for at udøve følgende rettigheder:

- Ret til at få indsigt i de indhentede oplysninger
- Ret til at få berigtiget de indhentede oplysninger
- Ret til at få overført de indhentede oplysninger i et læsbart format
- Ret til at få begrænset behandlingen af de indhentede oplysninger
- Ret til at få slettet de indhentede oplysninger

Undertegnede er bekendt med, at afgivelsen af dette samtykke er frivillig, ligesom samtykket til enhver tid vil kunne tilbagekaldes ved henvendelse til Wax Facility Service ApS.

Tilbagekaldelse og øvrige henvendelser kan adresseres til nedenstående:

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
E-mail: ck@waxfs.dk
Tlf.nr.: 28 44 26 05
Kontaktperson: Camillo Krog
CVR-nr. 32 10 20 18

Såfremt du måtte have indvendinger mod den foretagne behandling, vil du have mulighed for at indgive klage herom til Datatilsynet ved brug af følgende kontaktoplysninger:

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf. 33193200
E-mail dt@datatilsynet.dk

Dato:

_____

EKSTERN PERSONDATAPOLITIK

1. GENEREL INFORMATION

Ved denne persondatapolitik skal vi hermed informere dig om, at Wax Facility Service ApS behandler personoplysninger om dig.

I det følgende vil vi kort opliste de forskellige persongrupper om hvem vi behandler personoplysninger, samt hvorledes behandlingen finder sted i de enkelte tilfælde.

Dernæst vil vi oplyse dig om dine rettigheder og klagemuligheder i forbindelse med behandlingen af dine personoplysninger.

Ved gennemlæsning af denne persondatapolitik, vil du blive oplyst om følgende forhold:

a) Hvilke oplysninger som behandles
b) Hvilken behandling som finder sted
c) Hvor længe behandlingen finder sted
d) Hvilke rettigheder du har som registreret
e) Hvem du kan rette henvendelse til hos Wax Facility Service ApS
f) Hvem du kan klage til, såfremt du er utilfreds med den foreliggende behandling

2. PERSONOPLYSNINGER – KUNDER

Wax Facility Service ApS behandler en række oplysninger om dig i forbindelse med dit køb af vores tjenesteydelser.

I forbindelse med dit køb, vil du, som udgangspunkt, blive anmodet om at afgive navn og adresse, samt kontakt- og betalingsoplysninger.

Formålet med indhentelsen er at effektuere levering og betaling i relation til opfyldelsen af dit køb.

Ovenstående behandling vil indebære, at de pågældende oplysninger i forbindelse med faktureringen vil blive videregivet til de parter, som er involverede i den konkrete betalingstransaktion, herunder bl.a. pengeinstitut, kortudsteder mv.

De omhandlede personoplysninger vil blive behandlet i forbindelse med afviklingen af den enkelte ordre, hvorefter disse vil blive lagret i vores regnskabssystem i 5 år med henblik på at overholde Bogføringslovens dokumentationskrav.

Virksomhedens hjemmesider anvender cookies, som registrerer IP-adresse, søgehistorik og lignende med henblik på optimering af brugeroplevelsen, samt undersøgelse af adfærdsmæssige mønstre til brug for markedsføring. Du kan altid fravælge brug af cookies, samt slette allerede lagrede cookies. Der henvises til cookiepolitikken på www.waxfs.dk.

Ved brug af Wax Facility Service ApS' facebookside bliver der indhentet, behandlet og videregivet personoplysninger fra dig, idet Facebook anvender cookies.

Personoplysningerne anvendes til markedsføring, i hvilken forbindelse Facebook videregiver dine personoplysninger til deres samarbejdspartnere. Indhentelsen foretages uanset, om du har en Facebookprofil.

Wax Facility Service ApS har ikke indflydelse på Facebooks cookiepolitik, men du vil altid kunne fravælge brug af cookies, samt slette allerede lagrede cookies.

Facebook stiller endvidere statiske værktøjer til rådighed for Wax Facility Service ApS med henblik på at optimere kundeoplevelsen. Wax Facility Service ApS modtager alene disse personoplysninger i anonymiseret form.

Afsnittet om behandling af personoplysninger ved besøg på Wax Facility Service ApS' Facebookside vil løbende blive opdateret.

Såfremt der måtte forekomme ændringer i relation til omfanget eller formålet med vores behandling af deres personoplysninger, vil vi naturligvis altid informere dig herom.

3. PERSONOPLYSNINGER - MEDARBEJDERE

Wax Facility Service ApS behandler en række oplysninger om dig i forbindelse med din ansættelse hos os.

I forbindelse med din ansættelse vil du blive anmodet om af angive navn, adresse, kontaktoplysninger, personnummer og betalingsoplysninger, ligesom det enkelte ansættelsesforhold ofte vil indebære, at vi ligeledes vil indhente eller komme besiddelse af oplysninger om dine helbreds- og fagforeningsmæssige forhold, samt eventuelt diverse portrætfotos og din straffeattest.

Formålet med indhentelsen af ovenstående personoplysninger er personaleadministration, herunder tilrettelæggelsen af din ansættelse hos Wax Facility Service ApS, samt overholdelse af arbejds- og offentligretlige forpligtelser.

I den udstrækning vi måtte ønske at indhente eller anvende oplysninger, som ikke er direkte nødvendige for at varetage dit ansættelsesforhold, vil vi altid indhente dit samtykke.

Ovenstående behandling vil indebære videregivelse til offentlige myndigheder, herunder bl.a. SKAT, ATP mv., samt fagforeninger, lønadministrator, pensionskasser og lign.

De omhandlede personoplysninger vil blive behandlet under din ansættelse hos os, hvorefter disse vil blive lagret i vores medarbejderkartotek i 5 år med henblik på varetagelsen af eventuelle efterfølgende krav i anledning af ansættelsesforholdet.

Virksomhedens hjemmeside anvender cookies, som registrerer IP-adresse, søgehistorik og lignende med henblik på optimering af brugeroplevelsen, samt undersøgelse af adfærdsmæssige mønstre til brug for markedsføring. Du kan altid fravælge brug af cookies, samt slette allerede lagrede cookies. Der henvises til cookiepolitikken på www.waxfs.dk.

Såfremt der måtte forekomme ændringer i relation til omfanget eller formålet med vores behandling af deres personoplysninger, vil vi naturligvis altid informere dig herom.

4. PERSONOPLYSNINGER – ANSØGERE

Wax Facility Service ApS behandler en række oplysninger om dig i forbindelse med din ansøgning om en stilling hos os.

I forbindelse med din ansøgning vil du, som udgangspunkt, blive anmodet om af angive navn, adresse, alder og kontaktoplysninger, samt dokumentere eventuelle faglige kvalifikationer.

Formålet med indhentelsen af ovenstående personoplysninger er at vurdere dine kvalifikationer i relation til varetagelsen af den opslåede stilling.

Såfremt din ansøgning vurderes relevant, vil du ligeledes blive anmodet om at afgive oplysninger om din straffehistorik, såfremt dette skønnes særligt relevant i forhold til vurderingen af din evne til at varetage den opslåede stilling,

I den udstrækning vi måtte ønske at indhente eller anvende oplysninger om strafbare forhold, vil vi altid indhente dit samtykke.

De omhandlede personoplysninger vil blive behandlet i forbindelse med ansøgningsprocessen, hvorefter disse vil blive lagret i vores medarbejderkartotek i 6 måneder med henblik på kontakt i forbindelse med eventuelle genopslag.

Såfremt der måtte forekomme ændringer i relation til omfanget eller formålet med vores behandling af deres personoplysninger, vil vi naturligvis altid informere dig herom.

5. DINE RETTIGHEDER

I forbindelse med behandlingen vil du ved henvendelse til Wax Facility Service ApS have mulighed for at udøve følgende rettigheder:

a) Ret til at få indsigt i de indhentede oplysninger
b) Ret til at få berigtiget de indhentede oplysninger
c) Ret til at få overført de indhentede oplysninger i et læsbart format
d) Ret til at få begrænset behandlingen af de indhentede oplysninger
e) Ret til at få slettet de indhentede oplysninger

Henvendelse skal ske ved brug af følgende kontaktoplysninger:

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
E-mail: ck@waxfs.dk
Tlf.nr.: 28 44 26 05
Kontaktperson: Camillo Krog
CVR-nr. 32 10 20 18

6. KLAGE

Såfremt du måtte have indvendinger mod den foretagne behandling, vil du have mulighed for at indgive klage herom til Datatilsynet ved brug af følgende kontaktoplysninger:

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.nr.: 33193200
E-mail: dt@datatilsynet.dk

FORTEGNELSE OVER PERSONALEADMINISTRATION

1. DATAANSVARLIG

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
E-mail: ck@waxfs.dk
Tlf.nr.: 28 44 26 05
Kontaktperson: Camillo Krog
CVR-nr. 32 10 20 18

2. FORMÅL

a) Personaleadministration

3. KATEGORIER AF REGISTREREDE

a) Ansøgere
b) Medarbejdere
c) Tidligere medarbejdere

4. KATEGORIER AF PERSONOPLYSNINGER

a) Identifikationsoplysninger
b) Oplysninger vedrørende ansættelsesforholdet til brug for administration
c) Fagforeningsmæssigt tilhørsforhold
d) Helbredsoplysninger
e) Strafbare forhold
f) Billeder

5. KATEGORIER AF MODTAGERE

a) Løn- og økonomiadministrator
b) Offentlige myndigheder, fx SKAT, Guldborgsund Kommune m.fl.
c) Banker
d) Pensionskasser
e) Fagforeninger

6. VIDEREGIVELSE TIL TREDJELANDE OG INTERNATIONALE ORGANISATIONER

a) Ingen

7. SLETNING

a) Oplysninger om såvel ansøgere, medarbejder og tidligere medarbejdere slettes løbende, såfremt det konkret vurderes, at opbevaringen ikke tjener et anerkendelsesværdigt formål

b) Oplysninger om ansøgere slettes senest efter 6 måneder efter ansøgningsfristens udløb

c) Oplysninger om medarbejdere og tidligere medarbejdere slettes senest 5 år efter ansættelsesforholdets ophør

8. TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

a) Behandling af personoplysninger sker i overensstemmelse med Virksomhedens interne retningslinjer, som fastsætter sikkerhedsforskrifter i relation til såvel medarbejderes som uvedkommendes adgang til henholdsvis fysisk og elektronisk lagrede personoplysninger.

FORTEGNELSE OVER KUNDEADMINISTRATION

1. DATAANSVARLIG

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
E-mail: ck@waxfs.dk
Tlf.nr.: 28 44 26 05
Kontaktperson: Camillo Krog
CVR-nr. 32 10 20 18

2. FORMÅL

a) Kundeadministration

3. KATEGORIER AF REGISTREREDE

a) Kunder

4. KATEGORIER AF PERSONOPLYSNINGER

a) Identifikationsoplysninger
b) Betalingsoplysninger

5. KATEGORIER AF MODTAGERE

a) Banker
b) Økonomiadministrator

6. VIDEREGIVELSE TIL TREDJELANDE OG INTERNATIONALE ORGANISATIONER

a) Ingen

7. SLETNING

a) Oplysninger om kunder slettes løbende, såfremt det konkret vurderes, at opbevaringen ikke tjener et anerkendelsesværdigt formål

b) Oplysninger om kunder slettes senest 5 år efter betaling med henblik på overholdelse af Bogføringslovens dokumentationskrav.

8. TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

a) Behandling af personoplysninger sker i overensstemmelse med Virksomhedens interne retningslinjer, som fastsætter sikkerhedsforskrifter i relation til såvel medarbejderes som uvedkommendes adgang til henholdsvis fysisk og elektronisk lagrede personoplysninger.

MEDARBEJDERERLÆRING

Undertegnede bekræfter hermed at have gennemlæst og modtaget instruktion om Wax Facility Service ApS' interne retningslinjer for persondatabehandling, og forpligter sig til at efterleve disse i forbindelse med sit arbejde hos Wax Facility Service ApS.

Navn (med blokbogstaver):

_____

Dato og underskrift:

_____

FLYER/FAKTURA/E-MAILSIGNATUR

E-mail-/faktura-/flyertekst:

”Wax Facility ApS behandler personoplysninger om dig, som led i ydelsen af vores services, læs nærmere herom på www.waxfs.dk/persondatapolitik”

Databehandleraftale

Revision 2018.01

Mellem

Den dataansvarlige:
WAX FACILITY SERVICE APS, KØBENHAVNSVEJ 11, 4800 NYKØBING F, Danmark, CVR-nr: 32102018

Kontaktperson:
Camillo Krog, ck@waxfs.dk, 2844 2605

og

Databehandleren:
SkvizBiz ApS, Dyrehavegårdsvej 17, 6000 Kolding, Danmark, CVR-nr: 37243221

Kontaktperson:
Michael Larsen, gdpr@skvizbiz.dk, 7734 0917

Begge Parter bekræfter, at de har fuldmagt til at underskrive Aftalen.

Indhold

1. Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Aftalen 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)*, som stiller specifikke krav til indholdet af en databehandleraftale.
3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes "hovedaftale": Abonnement på SkvizBiz, som er indgået i forbindelse med bestilling.
4. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.
   Denne databehandleraftale er derfor udstyret med et revisionsnummer, og i fald den revideres af databehandleren er den tidligere databehandleraftale fortsat gældende indtil den dataansvarliges godkendelse af den reviderede udgave.
5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".
6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandleraftalen.
7. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
8. Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".
11. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.
12. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

2. Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangs-punkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål der må foretages behandling.
3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

3. 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 underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.
2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.
3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

5. Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.
3. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

6. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).
2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.
3. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.
4. Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.
5. Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.
6. Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at

underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

7. Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.
8. Underdatabehandleraftalen 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 der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
9. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.
10. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

7. Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel **(overladelse, videregivelse samt intern anvendelse)** af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.
2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – indenfor rammerne af databehandleraftalen - derfor bl.a. ikke:
   a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
   b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
   c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

8. 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 3.

   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. den registreredes indsigtsret
   d. retten til berigtigelse
   e. retten til sletning (»retten til at blive glemt«)
   f. retten til begrænsning af behandling
   g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering
2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

   Dette indebærer, at databehandleren under hensynstagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
   a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
   b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
   c. forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

e. forpligtelsen til at høre tilsynsmyndigheden (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

Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes "hovedaftale" eller af denne aftales bilag C og bilag D.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter at denne er blevet bekendt med bruddet og dets omfang, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 8, stk. 2, litra b, skal databehandleren - under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden, såfremt bruddet er sket hos databehandleren eller en eventuel underdatabehandler.

   Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

   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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden

   c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

10. Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

11. Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.
3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.
4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12. Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgår af parternes "hovedaftale" eller af denne aftales Bilag D.
2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.

13. Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.
2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.
3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.
4. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "hovedaftalen". Hvis begge parter er indforstået med det, kan opsigelsen dog også ske hurtigere.
5. Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.
6. Underskrift:
   Aftalen accepteres elektronisk af begge parter gennem systemet SkvizBiz.

14. Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Bilag A

Oplysninger om behandlingen

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

- at den dataansvarlige kan anvende systemet SkvizBiz, som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om den dataansvarliges kunder og medarbejdere.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om:

- at databehandleren stiller systemet SkvizBiz til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges kunder og medarbejdere på virksomhedens servere.

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

- Navn, e-mailadresse, telefonnummer, adresse, regnskabsoplysninger (herunder fakturaer, betalingspåmindelser, rykkere og inkassovarsler udstedt af den dataansvarlige til den registrerede og information om betalinger til den dataansvarlige.)
- Notater som den dataansvarlige gør sig i forbindelse med den registrerede, som f.eks. adgangsforhold på adressen, placering af ekstranøgler den registrerede har oplyst om, tidsrum for hvornår eventuelle aftaler mellem den dataansvarlige og den registrerede bedst udføres, og andre notater i forbindelse med den dataansvarliges opfyldelse af sine forpligtelser over for den registrerede, som den dataansvarlige har hjemmel til at notere.

A.4. Behandlingen omfatter følgende kategorier af registrerede:

- Personer som er eller har været kunder hos den dataansvarlige.
- Personer som har modtaget eller står i begreb med at modtage tilbud fra den dataansvarlige.
- Ansatte eller underleverandører til den dataansvarlige.

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales krafttræden.

A.5. Behandlingen har følgende varighed:

- Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

Bilag B

Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1. Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 1 måned før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 14 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

B.2. Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden ingen godkendte underdatabehandlere.

Bilag C

Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/ instruks

Databehandleren skal udelukkende behandle personoplysninger på vegne af og som følge af den dataansvarliges instruktioner. Ved at indgå denne aftale, instruerer den dataansvarlige databehandleren i at behandle personoplysninger på følgende måder:

a. i overensstemmelse med gældende lovgivning,
b. for at opfylde sine forpligtelser i henhold til abonnementsvilkår for systemet SkvizBiz,

c. som yderligere specificeret ved den dataansvarliges normale brug af systemet SkvizBiz, og

d. som beskrevet i denne aftale.

Som dokumentation for instruktioner ifølge Bilag C, stk. 1, litra c føres en log over den dataansvarliges brug af programmet. Loggen slettes løbende under hensyntagen til retten til sletning (»retten til at blive glemt«), og dokumentation for den dataansvarliges instrukser gennem normal brug af systemet SkvizBiz vil dermed kun blive gemt i en efter databehandlerens skøn rimelig periode.

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

- Databehandleren opbevarer de data den dataansvarlige videregiver, og stiller systemet SkvizBiz til rådighed med alle de funktioner som systemet indeholder, herunder søgning i personoplysninger og samkørsel mellem bankdata og debitorer.
- I nogle tilfælde indebærer behandlingen også, at databehandleren efter den dataansvarliges instruks videregiver informationer til tredje part. Det kan for eksempel være i forbindelse med opkrævning af en debitors faktura via BetalingsService, hvor det kan være nødvendigt for servicens udførsel at videregive visse persondata til udbyderen af BetalingsService, men det vil altid være efter udtrykkelig og åbenbar instruks via systemet SkvizBiz.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- At der kun er tale om almindelige persondata, både i forbindelse med den dataansvarliges kundekartotek og regnskabsføring, og i forbindelse med navne på eventuelle medarbejdere, hvorfor der etableres et almindeligt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne. Hvis det kan påvirke sikkerheden negativt, vil databehandleren ikke være forpligtet til i detaljer at udlevere oplysninger om de enkelte tekniske sikkerhedsforanstaltninger.

C.3. Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slette eller tilbageleveret.

C.4. Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

Databehandleren kan overføre persondata til tredjelande i det omfang den dataansvarlige specifikt giver sin instruks herom. Det kan f.eks. være hvis den dataansvarlige ønsker at bruge sin egen SMTP-server som er placeret i udlandet, og herefter gennem systemet giver instruks om at afsende et kontoudtog via den valgte SMTP-server. Den dataansvarlige godkender enhver overførsel som er nødvendig i forbindelse med servicen SkvizBiz, når den udføres som følge af en instruks den dataansvarlige selv har afgivet.

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke indenfor rammerne af databehandleraftalen foretage en sådan overførsel.

C.5. Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Den dataansvarlige er berettiget til at igangsætte en revision af Databehandlerens forpligtelser i henhold til databehandleraftalen én gang årligt. Hvis den dataansvarlige er forpligtet hertil efter gældende lovgivning, kan der foretages revision oftere en én gang årligt. Den dataansvarlige skal i forbindelse med anmodning om en revision medsende en detaljeret revisionsplan med en beskrivelse af omfang, varighed og startdato minimum fire uger forud for den foreslåede startdato. Det skal besluttes i fællesskab mellem den dataansvarlige og databehandleren, hvis en tredjepart skal foretage revisionen. Imidlertid kan den Dataansvarlige lade Databehandleren bestemme, at revisionen af sikkerhedsårsager skal foretages af en neutral tredjepart efter databehandlerens valg, såfremt der er tale om et behandlingsmiljø hvor flere dataansvarliges data er anvendt.

Hvis det foreslåede omfang for revisionen følger en ISAE, ISO eller lignende certificeringsrapport udført af en kvalificeret tredjepartsrevisor inden for de forudgående tolv måneder, og databehandleren bekræfter, at der ikke har været nogen materielle ændringer i de foranstaltninger, som har været under revision, skal den dataansvarlige acceptere denne revision i stedet for at anmode om en ny revision af de foranstaltninger, som allerede er dækket.

Under alle omstændigheder skal revision finde sted i normal kontortid på den relevante facilitet i overensstemmelse med databehandlerens politikker, og må ikke på urimelig vis forstyrre databehandlerens sædvanlige kommercielle aktiviteter.

Den dataansvarlige er ansvarlig for alle omkostninger i forbindelse med anmodningen om revision. Databehandlerens assistance i forbindelse hermed, som overskrider den almindelige service som databehandleren skal stille til rådighed som følge af gældende databeskyttelseslovgivning, afregnes særskilt i henhold til den til enhver tid gældende prisliste fra databehandleren.

C.6. Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Den dataansvarlige kan for egen regning selv, eller gennem en repræsentant for den dataansvarlige, indhente en revisionserklæring angående en eventuel underdatabehandlers overholdelse af denne databehandleraftale, når der

efter den dataansvarliges vurdering opstår et behov herfor.

Den dataansvarliges eventuelle udgifter i forbindelse med en revisionserklæring afholdes af den dataansvarlige selv, ligesom eventuelle ressourcer der skal afsættes af databehandleren også vil skulle afholdes af den dataansvarlige.

Hvis databehandleren selv indhenter en revisionserklæring eller på anden måde initierer en inspektion hos en eventuel underdatabehandler, er den dataansvarlige uvedkommende, og er ikke forpligtet til at afholde nogen udgifter herfor.

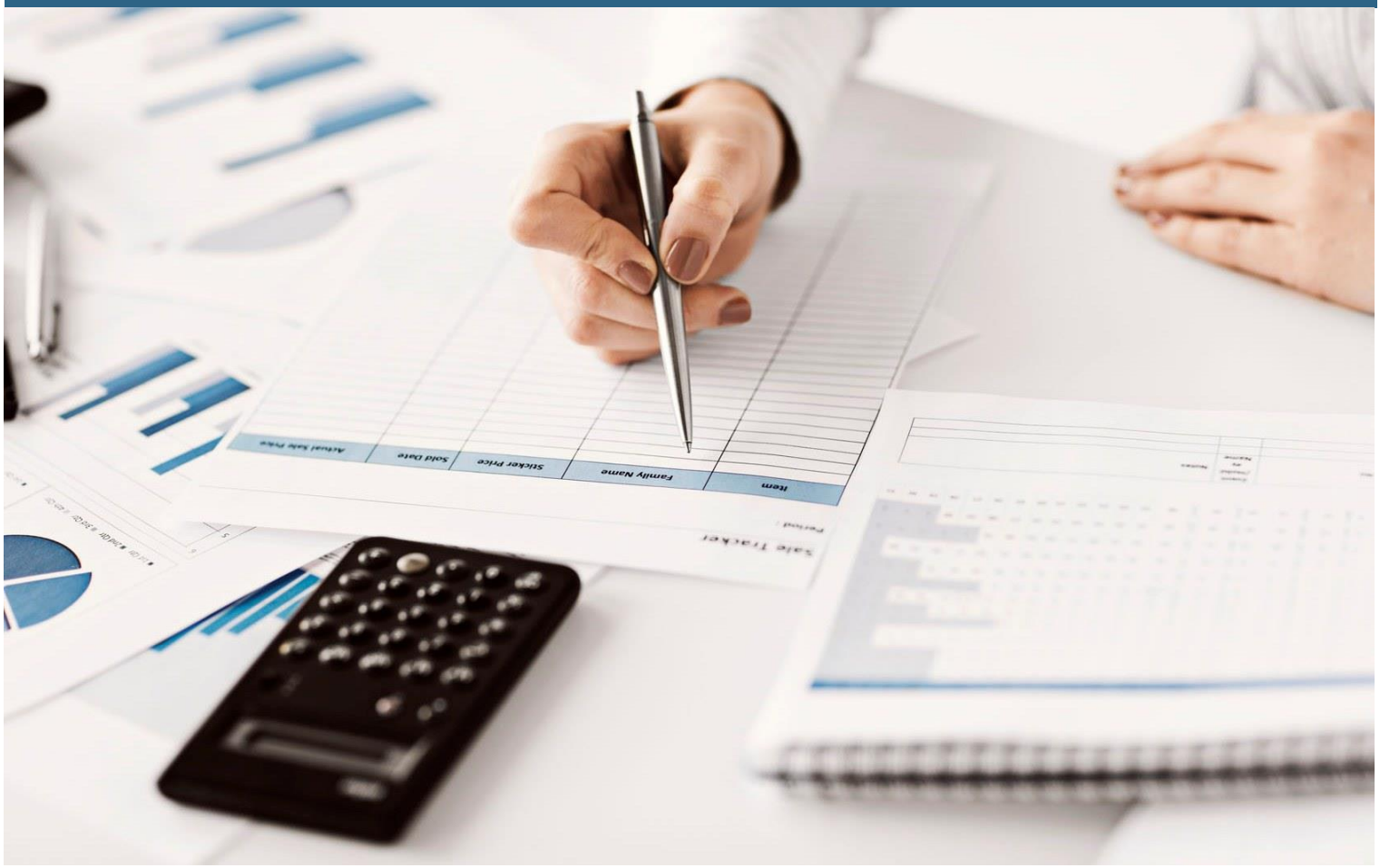
Bilag D

Parternes regulering af andre forhold

D.1. Yderligere sikkerhedsforanstaltninger

Hvis den dataansvarlige ønsker at få indført yderligere sikkerhedsforanstaltninger udover hvad databehandleren har vurderet er nødvendigt og acceptabelt, eller ønsker denne aftale ændret, vil omkostningerne herfor, medmindre det reguleres særskilt i parternes "hovedaftale", tilfalde den dataansvarlige.

DATALØN



Vilkår for DataLøn

Gældende fra 25. maj 2018

1. Hvad er DataLøn?

DataLøn er et lønsystem. Kernen i DataLøn er en standard IT-løsningen, der på baggrund af Kundens indberetninger til Visma DataLøn foretager lønbehandling for Kunden, herunder:

- beregner Medarbejdernes løn,
- foretager alle beregninger og indberetninger til og foranlediger pengeoverførsler til SKAT, ATP, ferie- og barselsfonde, pensionskasser m.v. på Kundens vegne,
- foretager indberetning af statistik til arbejdsgiverforening og Danmarks Statistik på Kundens vegne,
- sender lønsedler til Medarbejdernes e-Boks og
- gemmer Kundens lønbilag i et elektronisk arkiv i 5 år efter udløbet af det år, hvor lønbilaget produceres.
- yder hjælp til opstart og oprettelse af Kunden og Medarbejderne, og
- leverer support- og konsulentydelser telefonisk og online fra Visma DataLøns lønkonsulenter, når Kunden har brug for hjælp.

Afhængig af abonnementstypen indeholder DataLøn også en personaleadministrativ vejledning, personalejuridisk rådgivning og skabeloner til personaleadministrativt arbejde m.v. Materialet ajourføres løbende.

En nærmere beskrivelse af DataLøn, herunder de forskellige abonnementstyper og tilhørende produktindhold, er tilgængelig på dataløn.dk.

Visma DataLøn foretager ingen udvikling eller tilpasning af DataLøn i forhold til Kundens specifikke behov eller ønsker.

2. Definitioner

2.1. Aftale

Nærværende vilkår for DataLøn inkl. bilag samt Prislisten. Aftalen udgør det samlede aftalegrundlag mellem Visma DataLøn og Kunden i relation til DataLøn.

2.2. Bankdag

Alle dage undtagen lørdage, søndage og helligdage, fredag efter Kr. himmelfartsdag, 5. juni samt 24. og 31. december.

2.3. Betalingsgrundlag

Det betalingsgrundlag, som Visma DataLøn danner ved lønbehandlingen, der danner grundlag for pengeoverførsler til Kundens medarbejdere, SKAT, ATP, pensionskasser m.v.

2.4. DataLøn

Der henvises til punkt 1.

2.5. dataløn.dk

Det til enhver tid værende indhold på hjemmesiden www.dataløn.dk.

2.6. Grundmateriale

Samtlige oplysninger om Kunden og Medarbejderne til brug for lønbehandlingen, som Kunden leverer til Visma DataLøn, eller som Visma DataLøn indhenter på vegne af Kunden.

2.7. Kunden

Den virksomhed (arbejdsgiver), som Visma DataLøn har indgået nærværende Aftale med om brug af DataLøn.

2.8. Medarbejdere

De af Kundens medarbejdere, konsulenter m.v., som Kunden har registreret i DataLøn (hver enkelt betegnes "Medarbejder").

2.9. NemRefusion

Offentlig digital indberetningsløsning til brug for anmeldelse af fravær på grund af sygdom eller barsel samt anmodning om refusion af dagpenge efter sygedagpenge eller barselsloven.

2.10. Overførselsservice

Overførselsservice er et af Nets Denmark A/S udbudt produkt, hvor Nets Denmark A/S på vegne af Kunden behandler og videresender Betalingsgrundlaget til Kundens pengeinstitut med henblik på gennemførelse af pengeoverførsler til beløbsmodtager.

2.11. Prislisten

Visma DataLøns til enhver tid gældende prisliste for DataLøn, som er tilgængelig på dataløn.dk.

2.12. Samlet Betaling

ATP administrerer Samlet Betaling, der på tidspunktet for indgåelse af Aftalen omfatter beregning og opkrævning af bidrag til AUB, AES, Barsel DK og Finansieringsbidrag. Bidraget til de til enhver tid værende ordninger under Samlet Betaling bliver automatisk beregnet på baggrund af ATP-bidrag. Bidrag til Samlet Betaling opkræves kvartalsvis.

2.13. Stamoplysninger

De personoplysninger og andre oplysninger, som registreres for den enkelte medarbejder, og som dokumenteres på medarbejderens stamkort, herunder oplysninger om pensionsordninger, feriepenge, SH og fritvalgsordning.

2.14. Visma DataLøn

Visma DataLøn A/S, CVR-nr. 48 11 77 16, er det selskab, der udbyder DataLøn.

3. Pengeoverførsel

3.1. Overførsel vedrørende lønbehandling

Overførsel af (i) beløb til Medarbejderne på baggrund af Betalingsgrundlaget, (ii) Kundens betaling til Visma DataLøn for ydelser i henhold til Aftalen og (iii) beløb til SKAT, ATP, ferie- og barselsfonde, pensionskasser m.v., sker fra den konto i pengeinstituttet, som Kunden har oplyst til Visma DataLøn. Overførsler sker via Overførselsservice.

Overførsler sker i henhold til de gældende regler for henholdsvis Overførselsservice og for Kundens betalingskonto i Kundens pengeinstitut. Disse regler er Visma DataLøn uvedkommende.

3.2. Overførsel via Samlet Betaling

Ved tilmelding til Samlet Betaling i DataLøn giver Kunden samtykke til, at ATP må iværksætte betalinger fra Kunden til ATP. Overførsler til Samlet Betaling sker via Overførselsservice.

Kunden kan framelde sig Samlet Betaling inden den 1. i måneden før sidste rettidige betalingsdag.

4. Kundens forpligtelser

4.1. Registreringsforhold

Visma DataLøn er over for SKAT forpligtet til at kontrollere, at Kunden er korrekt registreret i forhold til eIndkomst, inden Visma DataLøn må rekvirere eSkattekort og indberette til eIndkomst.

Kunden giver fuldmagt til, at Visma DataLøn kan forespørge på Kundens registreringsforhold i forhold til eIndkomst og ajourføre registreringen i Det Centrale Virksomhedsregister i forhold til ovenstående, hvis den ikke er korrekt og dækkende.

Uanset ovenstående er det Kundens ansvar og en forudsætning for Kundens anvendelse af DataLøn, at Kundens virksomhed kan registreres korrekt i Det Centrale Virksomhedsregister. Er dette ikke tilfældet, betragtes det som væsentlig misligholdelse af Aftalen.

4.2. Aftale om Overførselsservice

For at Kunden kan gennemføre pengeoverførsler, jf. punkt 3, skal der til enhver tid bestå en aftale mellem Kunden og Nets Denmark A/S om brug af Overførselsservice.

4.3. Medarbejdernes Stamoplysninger

Kunden er forpligtet til at kontrollere, at de Stamoplysninger, Visma DataLøn registrerer ved oprettelse eller ændring af Medarbejdere på grundlag af Grundmateriale fra Kunden, til enhver tid er korrekte.

4.4. Grundmaterialet

Kunden skal levere Grundmaterialet til Visma DataLøn som beskrevet på dataløn.dk under DataLøn ved (i) Kundens egen indtastning direkte i DataLøn eller (ii) at indsende Grundmaterialet til Visma DataLøn i et format, der fremgår af dataløn.dk, herunder i relation til form, opbygning, indhold og tidsfrister.

4.5. Kundens IT-udstyr

Kundens IT-udstyr skal opfylde de systemkrav, der fremgår af dataløn.dk.

4.6. Kundens hæftelse

Kunden hæfter for alle dispositioner, som Kunden, Medarbejderne eller andre uden for Visma DataLøn har foretaget via DataLøn, også selv om misbrug har fundet sted.

4.7. Kundens opbevaring

Kunden skal opbevare Grundmaterialet i henhold til lovgivningen, herunder bogføringsloven.

Hvis Kunden ønsker at gemme skabeloner til personaleadministrativt arbejde (afhænger af abonnementstypen), leveret af Visma DataLøn og udfyldt af Kunden, skal Kunden selv opbevare disse, da Visma DataLøn ikke opbevarer dette materiale.

4.8. Kundeoplysninger

Kunden er forpligtet til løbende over for Visma DataLøn at ajourføre alle relevante oplysninger, som Kunden har givet til Visma DataLøn i forbindelse med indgåelse af Aftalen, herunder oplysninger om Kundens navn, adresse, telefonnummer, e-mailadresse og pengeinstitutkonto.

5. Databehandling

5.1. Dataansvarlig

Kunden er dataansvarlig og har ansvar for behandlingen af de personoplysninger, som Kunden behandler og sender til Visma DataLøn med henblik på Visma DataLøns opfyldelse af Aftalen.

5.2. Databehandler

Visma DataLøn er databehandler, jf. den til enhver tid gældende Databeskyttelsesforordning og Databeskyttelseslov, og behandler udelukkende oplysninger på den dataansvarliges vegne. De nærmere vilkår

herfor er reguleret i databehandleraftalen vedlagt som bilag 1.

6. Priser og betaling

6.1. Prisliste

Visma DataLøns ydelser faktureres i henhold til Prislisten med tillæg af moms.

Kunden skal ikke til Visma DataLøn særskilt betale for Kundens brug af Overførselsservice i relation til DataLøn. Eventuel opkrævning fra Kundens pengeinstitut vedrørende brug af Kundens betalingskonto er Visma DataLøn uvedkommende.

6.2. Betaling

Kundens betaling for ydelser i henhold til Aftalen sker ved, at Visma DataLøn overfører det fakturerede beløb fra Kundens konto, jf. punkt 3.1.

7. Rekvisition af oplysninger fra CPR

Kunden kan gennem DataLøn rekvirere oplysninger om Medarbejdernes navn og adresse i Det Centrale Personregister (CPR). Anvender Kunden denne funktion, sker det på følgende betingelser:

- Kunden må alene rekvirere oplysninger i CPR om personer, som Kunden i kraft af aftale skal udbetale løn, honorar mv. til.
- Kundens behandling af de modtagne oplysninger fra CPR skal ske i overensstemmelse med den til enhver tid gældende Databeskyttelsesforordning og Databeskyttelseslov.

Forsætlig eller groft uagtsom overtrædelse af ovennævnte betingelser for rekvisition af oplysninger fra CPR er strafbar.

Visma DataLøn registrerer bruger-id, tidspunkt og cpr-nummer for enhver rekvisition af oplysninger fra CPR i Kundens navn. Visma DataLøn opbevarer disse oplysninger i 6 måneder, hvorefter de slettes. På forlangende udleverer Visma DataLøn oplysningerne til CPR.

8. Refusionsanmodninger m.v.

Hvis Kunden ønsker, at Visma DataLøn indberetter refusionsanmodninger på vegne af Kunden, kan Kunden give Visma DataLøn en erhvervsfuldmagt hertil. Når Kunden giver Visma DataLøn en erhvervsfuldmagt, giver Kunden samtidig samtykke til, at Visma DataLøn kan indberette data til NemRefusion for Kunden.

Indberetning til NemRefusion sker på følgende betingelser:

- Der kan alene indberettes oplysninger til NemRefusion for Medarbejdere, der er omfattet af nærværende Aftale.
- Kunden er ansvarlig for korrektheden af de data, der indberettes til Visma DataLøn til brug for behandling af refusionsanmodninger. Visma DataLøn kontrollerer ved hjælp af fejlmeddelelser og kvitteringer fra NemRefusion, at indberetninger accepteres i NemRefusion og sikrer, at de eventuelle fejl og mangler, som NemRefusion giver meddelelse om, rettes.
- Indberetninger, der ikke er signeret (”kladder”), slettes fra NemRefusion efter 6 måneder fra Kundens sidste anvendelse uden yderligere varsel. Signerede indberetninger slettes fra NemRefusion efter 24 måneder fra signeringstidspunktet uden yderligere varsel.
- Indberetning af urigtige eller vildledende oplysninger til brug for afgørelser efter sygedagpengelov eller lov om ret til orlov og dagpenge ved barsel kan straffes efter straffeloven. Det samme gælder ved fortielse af oplysninger af betydning for sådanne afgørelser.
- Den kommune, som modtager de indberettede oplysninger, har adgang til Kundens lokaler og arbejdssteder med henblik på at kontrollere lønudbetalinger mv., som danner grundlag for beregning af syge- og barselsdagpenge.

9. Opbevaring af Grundmaterialet

Visma DataLøn opbevarer Grundmaterialet, jf. punkt 4.3, i minimum 45 dage og i øvrigt i henhold til Databeskyttelsesforordningen og Databeskyttelsesloven. Visma DataLøn opbevarer derudover kopi af det materiale, som Visma DataLøn danner som led i lønbehandlingen (løn- og bogføringsmateriale) året ud plus 5 år regnet fra produktionstidspunktet, hvorefter materialet slettes.

Visma DataLøn optager telefonsamtaler mellem Kunden og Visma DataLøns kundecentre for at kunne fastslå samtalernes indhold. Samtalerne opbevares i 6 måneder, hvorefter de slettes.

10. Ansvar og ansvarsfraskrivelse

10.1. Parternes ansvar

Hvor andet ikke fremgår af Aftalen, er parterne erstatningsansvarlige efter dansk rets almindelige regler.

Parterne er kun ansvarlige for deres egne ydelser og forhold (inklusive deres underleverandører, andre leverandører og medarbejdere).

Visma DataLøn påtager sig således blandt andet intet ansvar for

- Kundens egne fejl eller forsømmelser, herunder fejlindtastninger, forkert anvendelse eller misbrug af DataLøn,
- om DataLøns funktionalitet og indhold understøtter Kundens specifikke behov,
- om lønbehandlingen, herunder Grundmaterialet eller Betalingsgrundlaget, er i overensstemmelse med Medarbejdernes ansættelsesvilkår og/-eller de(n) arbejdsmarkedsoverenskomst(er), som Medarbejderne måtte være omfattet af,
- forhold hos Kundens pengeinstitut, en administrator af DataLøn, som Kunden har indgået aftale med, eller andre leverandører af lønadministration, programmel, hardwareenheder eller andet udstyr, kommunikationslinjer, eller andre leverancer, som er nødvendige eller hensigtsmæssige for at bruge Visma DataLøns ydelse, eller
- fejl og dispositioner hos tredjeparts leverandører, fx SKAT eller e-Boks.

10.2. Egenskaber for skabeloner til personaleadministrativt arbejde m.v. (afhænger af abonnementstypen)

Visma DataLøn er ikke ansvarlig for, om en skabelon har den ønskede egenskab.

Hvis Kunden ændrer i en skabelon (bortset fra udfyldelse af standardoplysninger som navn m.v.), er Visma DataLøn ikke længere ansvarlig for den pågældende skabelon.

10.3 Force majeure

Visma DataLøn er ikke ansvarlig for tab, herunder tab forårsaget af nedbrud i/manglende adgang til it-systemer eller beskadigelser af data i disse systemer, som skyldes force majeure eller lignende forhold. Som force majeure anses forhold, der er uden for Visma DataLøns rimelige kontrol, og som Visma DataLøn ikke burde have forudset ved Aftalens indgåelse, herunder som følge af:

- svigt i strømforsyning eller telekommunikation,
- lovindgreb eller forvaltningsakter,
- naturkatastrofer, vandskade, jordskælv eller ekstreme vejrforhold,
- brand,
- indtruffet eller truende krig, oprør, borgerlige uroligheder, sabotage, terror (herunder cyberterrorisme) eller eksplosioner,
- indbrud eller hærværk (herunder computervirus og -hacking), eller
- strejke, lockout, boykot eller blokade, uanset om konflikten er rettet mod eller iværksat af parterne selv eller deres organisation, og uanset konfliktens årsag. Det gælder også, når konflikten kun rammer dele af en parts organisation.

Ansvarsfriheden består, så længe force majeure begivenheden består.

10.4. Ansvarsbegrænsning

I intet tilfælde er Visma DataLøn ansvarlig for Kundens eller tredjemands indirekte tab, herunder men ikke begrænset til tab af produktion, salg, fortjeneste, goodwill, forbrugt intern arbejdstid, image, medarbejdere, kunder eller renter.

Visma DataLøn er ansvarlig for produktansvar efter dansk rets almindelige regler, idet ansvarsbegrænsningerne i nærværende punkt 10 og punkt 22 dog skal finde anvendelse i videst muligt omfang tilladt efter dansk ret.

Visma DataLøns samlede erstatningsansvar for hvert enkelt krav under denne Aftale er begrænset til (i) det beløb, som Kunden har betalt til Visma DataLøn i de 12 måneder forud for det tidspunkt, hvor Kunden skriftligt fremsatte kravet overfor Visma DataLøn *fratrukket* (ii) eventuelle øvrige erstatninger, som Visma DataLøn måtte have pådraget sig over for Kunden i samme 12-måneders periode. Ansvarsbegrænsningen i dette afsnit under punkt 10.4 gælder dog ikke erstatninger, Visma DataLøn har betalt i henhold til punkt 22 nedenfor.

Ansvarsbegrænsningerne i punkterne nævnt oven for gælder for enhver type af krav, herunder Kundens direkte krav og for Kundens regreskrav for erstatning udbetalt af Kunden.

Begrænsningerne i dette punkt gælder ikke, såfremt Visma DataLøn har handlet forsætligt eller groft uagtsomt.

11. Mangler og forsinkelse

11.1. Mangler

Hvis der er mangler ved Visma DataLøns ydelser, og dette skyldes Visma DataLøn, kan Visma DataLøn vælge at

- afhjælpe manglen, i det omfang det er praktisk muligt og kan ske uden uforholdsmæssige økonomiske konsekvenser, eller
- foretage omlevering af udført arbejde.

11.2. Forsinkelse

Hvis Visma DataLøns ydelse forsinkes af årsager, som Kunden er uden ansvar for, kan Kunden over for Visma DataLøn fremsætte påkrav om, at leveringen påbegyndes.

11.3. Mangler og forsinkelser som Visma DataLøn ikke har ansvaret for

Hvis Visma DataLøn ikke er ansvarlig for fejl eller forsinkelser, kan Visma DataLøn efter Kundens anmodning medvirke ved afhjælpning eller omlevering mod et rimeligt vederlag.

11.4. Reklamationsfrist

Mangler eller forsinkelser i Visma DataLøns ydelser, som Kunden bliver bekendt med eller burde være blevet bekendt med, og som Kunden ønsker at påberåbe sig, skal straks meddeles skriftligt til Visma DataLøn. Hvis en mangel eller forsinkelse, som Kunden opdager eller burde have opdaget, ikke straks meddeles skriftligt til Visma DataLøn, kan denne ikke senere gøres gældende.

11.5. Krav

Krav mod Visma DataLøn i anledning af mangler eller forsinkelser, som Kunden rettidigt har reklameret over, jf. punkt 11.4, skal altid fremsættes skriftligt og inden rimelig tid og senest 6 måneder efter reklamationsfristens udløb, jf. punkt 11.4.

12. Licens

12.1. Kundens brugsret

Visma DataLøn giver Kunden en ikke-eksklusiv og ikke-overdragelig brugsret til i Aftalens løbetid at benytte DataLøn, herunder materiale, som Visma DataLøn har leveret til Kunden i henhold til denne Aftale, erhvervsmæssigt på de betingelser, der er fastsat i Aftalen.

Brugsretten omfatter kun Kundens anvendelse af DataLøn til Kundens egen brug. Kunden er berettiget til at benytte en administrator, der selv har anskaffet en brugsret fra Visma DataLøn til at anvende DataLøn.

13. Immaterielle rettigheder

Visma DataLøn har ejendomsret, ophavsret og enhver anden rettighed til DataLøn, herunder programmel, dataløn.dk og Visma DataLøns dokumentation og vejledninger om DataLøn, dog med undtagelse af programmel eller andet materiale fra leverandører, jf. punkt 16.

14. Tredjemands rettigheder

14.1. Krænkelse af tredjemands rettigheder

Så vidt det er Visma DataLøn bekendt, krænker DataLøn ikke tredjemands rettigheder, herunder patenter eller ophavsrettigheder.

14.2. Sag mod Kunden

Hvis tredjemand over for Kunden fremsætter påstand om, at DataLøn krænker tredjemands rettigheder, (i) skal Kunden straks meddele dette skriftligt til Visma DataLøn og holde Visma DataLøn løbende orienteret om alle forhold relateret hertil, og (ii) har Visma DataLøn for egen regning ret til at indtræde i sagen, hvorved Visma DataLøn kan foretage enhver handling på Kundens vegne i forhold til sagen, herunder (a) at forsvare eller forlige krav fremsat mod Kunden og (b) at engagere eksterne rådgivere, der kan handle på Kundens vegne.

Foreligger der krænkelse af tredjemands ret, skal Visma DataLøn for egen regning skaffe Kunden retten til fortsat at benytte DataLøn eller bringe krænkelsen til ophør ved at ændre eller erstatte Visma DataLøns ydelse, hvis det er praktisk muligt, og Visma DataLøns omkostninger i forbindelse hermed står i rimeligt forhold til (i) Kundens vederlag for DataLøn eller (ii) den del af Visma DataLøns ydelse, der skal ændres eller erstattes.

Visma DataLøn skal holde Kunden skadesløs for beløb, som Kunden i henhold til endelig domstolsafgørelse pålægges at betale til tredjemand som følge af krænkelsen. Visma DataLøns erstatningsansvar for tab er dog begrænset som beskrevet i punkt 10.

Hvis Visma DataLøn vælger ikke at indtræde i sagen, skal Visma DataLøn holde Kunden skadesløs for dennes egne udgifter til advokat og sagsomkostninger, som Kunden måtte blive pålagt at betale til sagsøger. Visma DataLøns erstatningsansvar for tab er dog begrænset som beskrevet i punkt 10.

Bestemmelserne i punkt 14 gælder ikke for ydelser fra leverandører, jf. punkt 16.

15. Tavshedspligt

Visma DataLøn overholder de fortrolighedsbestemmelser, der gælder for behandling af personoplysninger, jf. databehandleraftalen vedlagt som bilag 1.

Endvidere har Visma DataLøn og Visma DataLøns medarbejdere tavshedspligt med hensyn til enhver fortrolig oplysning om Kunden, forretningshemmeligheder, oplysninger om forretningsforbindelser samt andre fortrolige forhold, som Visma DataLøn får kendskab til ved Aftalens opfyldelse.

Fortrolige oplysninger fra Kunden må kun anvendes og opbevares som led i Aftalens opfyldelse.

16. Brug af andre leverandører

16.1. Visma DataLøns underleverandører

Visma DataLøn kan anvende underleverandører. Visma DataLøn hæfter for sine underleverandørers ydelser på samme måde som for sine egne forhold.

16.2. Kundens underleverandører

Kunden skal for egen regning indgå aftale med andre leverandører om levering og installation af programmel, kommunikationslinjer og/eller andet udstyr, som er nødvendige eller hensigtsmæssige for at bruge Visma DataLøns ydelse.

17. Ændringer

17.1. Ændring af DataLøn og dataløn.dk

Visma DataLøn er til enhver tid berettiget til uden varsel at foretage ændringer af DataLøn, dataløn.dk og Visma DataLøns dokumentation og vejledninger om DataLøn, herunder som følge af opdatering, fornyelse og vedligeholdelse.

17.2. Ændring af nærværende Aftale

Visma DataLøn kan ændre nærværende vilkår for DataLøn, herunder Prislisten, med 1 måneds skriftligt varsel til den 1. i en måned. Dette gælder dog ikke, hvis myndighedskrav, sikkerhedshensyn eller lignende forhold nødvendiggør et kortere varsel.

Visma DataLøn varsler Kunden om ændringer ved brev eller elektronisk, f.eks. via e-mail, indbakke-besked eller bogføringsbilag.

18. Opsigelse og ophævelse

18.1. Opsigelse

Kunden kan opsige Aftalen med 1 måneds skriftligt varsel til den 1. i en måned. Visma DataLøn kan opsige Aftalen med 3 måneders skriftligt varsel til den 1. i en måned.

18.2. Ophævelse

Aftalen kan ophæves helt eller delvist uden varsel af:

- Visma DataLøn, hvis Kunden væsentligt misligholder Aftalen, f.eks. ved (i) at der ikke er dækning for beløb faktureret af Visma DataLøn, jf. punkt 6, eller (ii) at der ikke til enhver tid består en aftale mellem Kunden og Nets Denmark A/S om brug af Overførselsservice.
- Kunden, hvis Visma DataLøn væsentligt misligholder Aftalen, og Visma DataLøn efter modtagelse af et skriftligt påkrav om afhjælpning af manglen, jf. punkt 11.1, eller skriftligt påkrav om påbegyndelse af levering, jf. punkt 11.2, ikke inden rimelig tid har afhjulpet manglen, eller
- hver af parterne, hvis den anden part erklæres konkurs, tages under rekonstruktionsbehandling eller lignende gældsordning, medmindre boet efter konkurslovens regler har ret til at indtræde i eller videreføre Aftalen og vælger at gøre dette.

18.3. Udestående ydelser

Selv om Aftalen er ophørt, gælder den stadig for forpligtelser, der skal opfyldes i op til 6 måneder efter, at Aftalen er ophørt.

Disse ydelser leveres i henhold til Aftalen og på Aftalens vilkår.

Ophører Aftalen som følge af konkurs, gennemføres de ydelser, der er udestående, ikke.

19. Overdragelse

Ingen af parterne kan uden den anden parts skriftlige samtykke overdrage sine rettigheder og forpligtelser ifølge Aftalen til tredjemand. Visma DataLøn har dog ret til at overdrage sine rettigheder og forpligtelser ifølge Aftalen til et andet selskab i Visma DataLøn-koncernen uden Kundens samtykke.

20. Forrang, lovvalg og værneting

I tilfælde af uoverensstemmelse har nærværende vilkår for DataLøn forrang i forhold til dataløn.dk og Visma DataLøns dokumentation og vejledninger om DataLøn samt Prislisten.

Aftalen er undergivet dansk ret. Eventuelle uoverensstemmelser mellem parterne, som ikke kan løses ved forhandling, kan indbringes for de ordinære domstole med Visma DataLøns hjemting som værneting.

Supplerende vilkår for personalejuridisk rådgivning

Kunder i DataLøn har adgang til personalejuridisk rådgivning, evt. mod særskilt betaling (afhænger af abonnementstype). Følgende supplerende vilkår gælder, når Visma DataLøn leverer personalejuridisk rådgivning som en del af DataLøn:

21. Hvad er personalejuridisk rådgivning?

Generel og konkret telefonisk og/eller skriftlig juridisk rådgivning om ansættelsesretlige forhold på grundlag af oplysninger fra Kunden, jf. gældende ydelsesbeskrivelser for personalejuridisk rådgivning.

Visma DataLøns rådgivere er enten jurister eller andre medarbejdere, som er internt uddannet i personalejura hos Visma DataLøn.

Alle opgaver udføres i overensstemmelse med god skik for juridisk rådgivning.

22. Ansvarsfraskrivelse

I relation til ansvar, der udspringer af personalejuridisk rådgivning, erstattes tredje afsnit under punkt 10.4 ovenfor af følgende:

I det omfang Visma DataLøn ved levering af personalejuridisk rådgivning er ansvarlig for Kundens direkte tab, er Visma DataLøns erstatningsansvar begrænset til kr. 250.000 pr. opgave.

Bilag 1

Databehandleraftale

1. Indledning

Som en del af parternes Aftale, gælder følgende Databehandleraftale mellem Databehandleren, Visma Dataløn A/S og den Dataansvarlige, Kunden, med mindre andet er udtrykkeligt specificeret i andre aftaler mellem parterne.

Formålet med Databehandleraftalen er at regulere, hvordan og til hvilket formål Databehandleren skal behandle Personoplysninger på vegne af den Dataansvarlige samt at sikre, at den Dataansvarliges Personoplysninger behandles i henhold til den Dataansvarliges retningslinjer og instrukser samt gældende databeskyttelseslovgivning.

Kategorier af Registrerede og Personoplysninger, der behandles, fremgår af bilag A.

2. Definitioner

Personoplysninger, Særlige kategorier af Personoplysninger (Følsomme persondata), Behandling af personoplysninger, den Registrerede, den Dataansvarlige og Databehandler skal have den betydning, som følger af gældende lovgivning om behandling af personoplysninger, herunder Databeskyttelses-forordningen (GDPR).

3. Den Dataansvarliges forpligtelser

Den Dataansvarlige har ansvaret for, at behandlingen af Personoplysninger lever op til kravene i Databeskyttelsesforordningen og Databeskyttelsesloven.

Den Dataansvarlige er ved brug af de tjenester, som Databehandler stiller til rådighed i henhold til Aftalen, forpligtet til at behandle Personoplysninger i overensstemmelse med bestemmelserne i gældende lovgivning om behandling af personoplysninger.

Den Dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som Databehandleren instrueres i at foretage.

4. Databehandlerens forpligtelser

Databehandleren behandler udelukkende Personoplysninger på vegne af og på baggrund af instrukser fra den Dataansvarlige.

Databehandling skal ske på følgende måde:

- Alene i overensstemmelse med gældende lovgivning,
- For at opfylde alle forpligtelser i henhold til Aftalen,
- Som nærmere angivet gennem den Dataansvarliges almindelige brug af Databehandlerens tjenester,
- Som angivet i denne Databehandleraftale.

Databehandler underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Databehandler skal sikre, at Personoplysningerne er underlagt fortrolighed, integritet og tilgængelighed i henhold til gældende lovgivning om behandling af personoplysninger.

Databehandler og dennes medarbejdere skal sikre fortrolighed vedrørende de behandlede Personoplysninger. Denne bestemmelse gælder også efter Aftalens ophør.

Databehandler sikrer, at de personer, der er autoriseret til at behandle Personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Databehandler skal bistå den Dataansvarlige med passende tekniske og organisatoriske foranstaltninger, så vidt dette er muligt, for opfyldelse af den Dataansvarliges forpligtelser til at svare på anmodninger fra Registrerede og om generel udøvelse af Registreredes rettigheder i henhold til Databeskyttelsesforordningens Kapitel 3 og Artikel 32 til 36.

Databehandler giver, uden unødig forsinkelse, meddelelse til den Dataansvarlige om hændelser, som den Dataansvarlige i henhold til lovgivningen er forpligtet til at meddele til Datatilsynet eller Registrerede.

Desuden giver Databehandler, i det omfang det er hensigtsmæssigt og lovligt, den Dataansvarlige meddelelse om:

- Anmodninger om videregivelse af Personoplysninger modtaget fra en Registreret.
- Anmodninger om videregivelse af Personoplysninger fra offentlige myndigheder, såsom politiet.

Databehandleren besvarer ikke direkte henvendelser fra Registrerede, medmindre der foreligger samtykke fra den Dataansvarlige. Databehandleren videregiver ikke Personoplysninger til offentlige myndigheder, såsom politiet, medmindre der foreligger lovligt grundlag.

Databehandleren har ikke ejerskab til, eller kontrol med, hvorvidt og hvordan den Dataansvarlige vælger at benytte sig af eventuel tredjeparts integrationer via Databehandler API, via direkte databasekobling eller lignende. Ansvaret for sådanne integrationer med tredjepart påhviler udelukkende Dataansvarlig.

5. Sikkerhed

Databehandler skal indføre systematiske, organisatoriske og tekniske foranstaltninger til sikring af et passende sikkerhedsniveau under hensyntagen til teknologien og omkostningerne til indførelse i forhold til de risici, som behandlingen indebærer, samt arten af de Personoplysninger der skal beskyttes.

Databehandler er forpligtet til at sikre et højt sikkerhedsniveau i sine produkter og tjenester. Databehandler yder dette sikkerhedsniveau gennem organisatoriske, tekniske og fysiske sikkerhedsforanstaltninger i henhold til kravene til informationssikkerhedsforanstaltninger, som fremgår af Databeskyttelsesforordningens Artikel 32.

Desuden har de interne rammer for beskyttelse af personoplysninger, som er udarbejdet af Visma-koncernen, til formål at sikre fortroligheden, integriteten, sikkerheden og tilgængeligheden af personoplysninger. Følgende foranstaltninger har særlig betydning i denne forbindelse:

- Klassificering af Personoplysninger for at sikre iværksættelse af sikkerhedsforanstaltninger svarende til risikovurderinger.
- Vurdering af brug af kryptering og anonymisering som risikobegrænsende foranstaltninger.
- Begrænsning af tilgang til Personoplysninger til dem, som har brug for adgang til opfyldelse af forpligtelser i henhold til Aftalen.
- Kontrolsystemer, der registrerer, genopretter, forebygger og rapporterer brud i forbindelse med behandling af Personoplysninger.
- Sikkerhedsprocedurer som angivet i Bilag C.

Hvis den Dataansvarlige anmoder om oplysninger om sikkerhedsforanstaltninger, dokumentation eller andre former for oplysninger omkring, hvordan Databehandler behandler Personoplysninger, og sådanne overskrider de standardoplysninger, som Databehandler har stillet til rådighed for opfyldelse af gældende lovgivning om behandling af Personoplysninger som Databehandler, og dette medfører ekstra arbejde for Databehandler, er Databehandler berettiget til at opkræve den Dataansvarlige betaling for sådanne ekstra arbejder.

Databehandler underretter uden unødig forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandler eller en eventuel underdatabehandler.

6. Kontrol

Den Dataansvarlige kan foretage kontrol for at påse, at Databehandler overholder denne Aftale, op til 1 gang om året.

Hvis det er et lovkrav gældende for den Dataansvarlige, kan den Dataansvarlige anmode om hyppigere kontrol.

For at anmode om at foretage en kontrol skal den Dataansvarlige fremsende en detaljeret kontroloversigt mindst fire uger forud for den foreslåede kontroldato til Databehandler med beskrivelse af det foreslåede omfang, varighed og starttidspunkt for kontrollen.

Hvis tredjeparter skal foretage kontrollen, skal det som hovedregel aftales mellem Parterne. Hvis behandling sker i et "multitenant" miljø eller lignende, giver den Dataansvarlige Databehandler ret til at bestemme, af sikkerhedsmæssige årsager, at kontrollerne skal foretages af en neutral tredjepartskontrollant efter Databehandlers valg.

Hvis det anmodede kontrolomfang er behandlet i ISAE, ISO eller lignende sikkerhedsrapport, varetaget af en kvalificeret tredjepartskontrollant inden for de sidste 12 måneder, og Databehandler bekræfter, at der ikke er foretaget nogle væsentlige ændringer i de kontrollerede foranstaltninger, bekræfter den Dataansvarlige, at sådanne resultater accepteres i stedet for at anmode om en ny kontrol af de foranstaltninger, der er omfattet af rapporten.

I alle tilfælde skal kontroller foretages inden for normal arbejdstid på det pågældende sted, i medfør af Databehandlers politikker og må ikke på urimelig måde gribe forstyrrende ind i Databehandlers forretningsdrift.

Den Dataansvarlige afholder alle omkostninger i forbindelse med den Dataansvarliges anmodede kontroller.

Ligeledes fakturerer Databehandler den Dataansvarlige for bistand, som overstiger den standardydelse, som Databehandler eller Visma-koncernen stiller til rådighed for opfyldelse af gældende lovgivning om behandling af personoplysninger.

7. Brug af underdatabehandlere og overførsel af data

Som en del af leveringen af tjenester til den Dataansvarlige har Databehandler den Dataansvarliges ge-

nerelle tilladelse til at gøre brug af underdatabehandlere. Disse underdatabehandlere kan være andre selskaber i Visma-koncernen eller eksterne tredjepartsleverandører.

Databehandler skal sikre, at underdatabehandlere pålægges de samme forpligtelser, som fastsat i denne Databehandleraftale. Enhver brug af underdatabehandlere er underlagt Visma-koncernens Privacy Statement.

Den Dataansvarlige har ret til at anmode om at få et overblik over underdatabehandlere, der aktuelt gøres brug af, med adgang til Personoplysninger, som angivet i Bilag B. Desuden har den Dataansvarlige ret til at anmode om at få fuldt overblik og mere detaljerede oplysninger om disse underdatabehandlere.

Den Dataansvarlige skal på forhånd underrettes om eventuel udskiftning af underdatabehandlere, som behandler Personoplysninger. Den Dataansvarlige kan gøre indsigelse mod ændringerne, såfremt den Dataansvarlige har rimelige, konkrete årsager hertil.

Databehandler må ikke lade behandling af Personoplysninger foregå uden for EU/EØS uden den Dataansvarliges samtykke.

Såfremt den Dataansvarlige giver samtykke til, at Databehandleren foretager behandling af Personoplysninger uden for EU/EØS, fremgår dette af bilag B. Databehandler skal sikre et korrekt juridisk grundlag for overførsel af Personoplysninger uden for EU/EØS på vegne af den Dataansvarlige, herunder ved indgåelse af EU-kommissionens Standardkontrakt eller overførsel af Personoplysninger i henhold til Privacy Shield.

8. Varighed og ophør

Denne Databehandleraftale er gældende, så længe Databehandler behandler Personoplysninger på vegne af den Dataansvarlige i henhold til Aftalen. Databehandleraftalen ophører automatisk ved opsigelse af Aftalen.

Ved denne Aftales ophør sletter, returnerer eller opbevarer Databehandler, de på vegne af den Dataansvarlige behandlede Personoplysninger efter aftale med den Dataansvarlige.

Medmindre andet er skriftligt aftalt, tager omkostninger til sådanne foranstaltninger udgangspunkt i:

- Timetakst for den tid Databehandler har brugt, og
- Sværhedsgraden af den anmodede behandling.

Databehandler kan tilbageholde Personoplysninger efter opsigelse af Aftalen i det omfang, det er påkrævet ved lov, som er underlagt samme tekniske og organisatoriske sikkerhedsforanstaltninger, som fremgår af denne Databehandleraftale.

9. Ændringer og tilføjelser

Ændringer til dette bilag skal udfærdiges i et nyt bilag til Aftalen.

Hvis nogen bestemmelse i denne Databehandleraftale bliver ugyldig, påvirker dette ikke gyldigheden af de øvrige bestemmelser. Parterne skal erstatte den ugyldige bestemmelse med en lovlig bestemmelse, der afspejler formålet med den ugyldige bestemmelse.

10. Ansvar

Ansvaret for brud på bestemmelserne i denne Databehandleraftale reguleres af ansvarsbestemmelserne i Vilkår for DataLøn. Dette gælder også for eventuelle brud begået af Databehandlers underdatabehandlere.

Underbilag A - Kategorier af Persondata og Registrerede

1. Kategorier af Registrerede og Persondata, der er underlagt behandling, i henhold til nærværende Aftale

a. Kategorier af registrerede
   i. Kundens slutbrugere
   ii. Kundens medarbejdere
   iii. Kundens kontaktpersoner

b. Kategorier af personoplysninger
   i. Kontaktoplysninger, som navn, adresse, mail, telefon
   ii. CPR-nr.
   iii. Stillingskategori, oplysninger om løn, arbejdstid, fravær, pension, skat, bankkonto
   iv. evt. øvrige personoplysninger, der er nødvendige for, at den Dataansvarlige kan administrere ansættelsesforholdet.

c. Behandlingsaktiviteter
   Databehandleren varetager via it-systemer håndteringen af den Dataansvarliges lønadministration, udarbejdelse af lønsedler, opbevaring og lagring af Personoplysninger om den Dataansvarliges og den Dataansvarliges medarbejdere, rapportering og overførsel af information til den Dataansvarlige, Nets Danmark A/S, pengeinstitutter, pensionsselskaber, evt. pligtige rapporteringer i arbejdsgiverforeninger, offentlige styrelser (SKAT, statistik m.m.).

Herudover forestår Databehandleren drift, test, vedligeholdelse, udvikling samt fejlretning af systemer og applikationer.

2. Typer af følsomme persondata, der er underlagt behandling, i henhold til Aftalen

Den Dataansvarlige skal give Databehandler meddelelse om, og angive nedenfor, eventuelle typer følsomme persondata i henhold til gældende lovgivning om behandling personoplysninger.

Databehandler skal på vegne af den Dataansvarlige behandle oplysninger om:	**Ja**	**Nej**
Race eller etnisk, politisk, filosofisk eller religiøs overbevisning		X
At en person er mistænkt, sigtet eller dømt for en forbrydelse		X
Helbredsoplysninger		X
Seksuel orientering		X
Medlemskab af fagforening		X
Genetiske eller biometriske data		X

Underbilag B - Oversigt over aktuelle underdatabehandlere

Databehandlers aktuelle underdatabehandlere, der kan få adgang til den Dataansvarliges Personoplysninger, omfatter ved ikrafttrædelsen af denne Aftale:

Navn	Sted/land	Juridisk overdragelsesmekanisme, hvis underdatabehandleren har adgang til personoplysninger fra lande uden for EU	Bistår Databehandleren med
Nets Denmark A/S Lautrupbjerg 10 2750 Ballerup CVR 20016175	Danmark	Ikke relevant	Datalagring Lønkørsler
Atea A/S Lautrupvang 6 2750 Ballerup CVR 25511484	Danmark	Ikke relevant	Datalagring
Solipsis Marktplein 2 5306 BA Brakel	Holland	Ikke relevant	Datalagring, E-arkiv
NetNordic Enterprise Communications A/S Lyskær 1 2730 Herlev CVR 29797056	Danmark	Ikke relevant	Datalagring, telefonsamtaler
Cohaesio A/S Per Henrik Lings Allé 4, 4. 2100 København Ø CVR 26079209	Danmark	Ikke relevant	Infrastruktur
Visma ITC AS Karenlyst alle 56 0277 Oslo	Norge	Ikke relevant	Infrastruktur
OnlineCity ApS Buchwaldsgade 50 5000 Odense C CVR 27364276	Danmark	Ikke relevant	Udsendelse af sms i forbindelse med log-on
Cim Mobilty Fælledvej 17 7600 Struer CVR 27913334	Danmark	Ikke relevant	Udsendelse af sms i forbindelse med log-on
Visma Labs SIA Sporta Street 11 Riga LV 1013 Latvia	Letland	Ikke relevant	Udvikling og fejlretning

For Kunder med abonnementstype ”LønAdministration” kan følgende aktuelle underdatabehandlere tillige få adgang til den Dataansvarliges Personoplysninger:

BtB Consult ApS Greve Bygade 22 2670 Greve CVR 29195951	Danmark	Ikke relevant	Sagsbehandling mv. i forbindelse med Databehandlers levering af lønadministration
Viborg Erhvervsservice ApS Gl. Skivevej 73 A 8800 Viborg CVR 21522783	Danmark	Ikke relevant	Sagsbehandling mv. i forbindelse med Databehandlers levering af lønadministration

Underbilag C – Databehandlerens sikkerhedsprocedurer

Sikkerhedsprocedurer

Informationssikkerheden i Visma Dataløn er baseret på standarden ISO / IEC 27001: 2013 Informationsteknologi – Sikkerhedsteknikker.

Standarden indeholder Statement of Applicability (SOA), som er en del af Visma Dataløn Information Security Management System (ISMS). SOA udgør politikker, procedurer, processer, organisatoriske beslutningsprocesser og aktiviteter inden for følgende informationssikkerhedskontrolområder i Visma DataLøn:

- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring
- Compliance

Informationssikkerhed

Visma Dataløn har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

- **Fortrolighed**

Sikre at uautoriserede personer ikke kan få adgang til data, som kan misbruges til skade for Visma DataLøns kunder, forretningsforbindelser og ansatte.

- **Integritet**

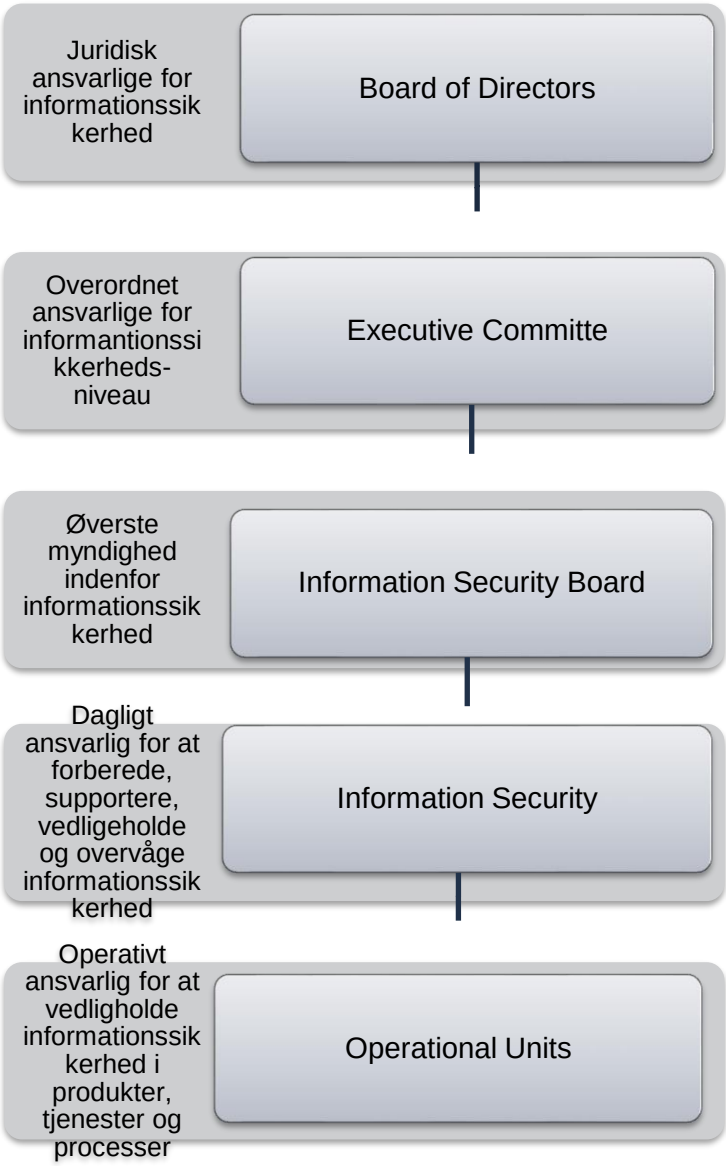
Sikre at systemer indeholder akkurat og komplet information.

- **Tilgængelighed**

Sikre at relevant information og relevante systemer er tilgængelige og stabile.

Styring af informationssikkerhed
Styring af informationssikkerhed i Visma Dataløn er baseret på ISO 27005 Informationsteknologi - Sikkerhedsteknikker - Risikostyring af informationssikkerhed.

Informationssikkerhed, Organisation
Visma Dataløn har etableret et ledelsesrammeværk til initiering og styring af implementering samt drift af informationssikkerhed.



Personalesikkerhed
Visma Dataløn har sikret, at medarbejdere og aftaleparter har forstået deres ansvar og er kompetente til at varetage deres roller.

Asset management
Visma Dataløn har identificeret organisatoriske aktiver og defineret passende beskyttelse.

Adgangsstyring
Visma Dataløn har via godkendelses- og autorisationsprocesser sikret, at det kun er muligt at opnå en

arbejdsrelateret adgang til informations- og informationsbehandlingsfaciliteter.

Kryptografi
Visma Dataløn har sikret en korrekt og effektiv brug af kryptografi for at beskytte fortrolighed, autenticiteten og integriteten af information.

Fysisk sikring og miljøsikring
Visma Dataløn forhindrer uautoriseret fysisk adgang, skade og forstyrrelse i virksomhedens informationer og databehandlingslokationer.

Driftsikkerhed
Visma Dataløn har sikret korrekt og sikker drift gennem dokumenterede procedurer og processer.

Kommunikationssikkerhed
Visma Dataløn har sikret beskyttelse af information på netværk og databehandlingslokationer.

Anskaffelse, udvikling og vedligeholdelse af systemer
Al ekstern erhvervelse eller forbedring/fornyelse af informationssystemer, tjenester og komponenter i Visma Dataløn er centralt evalueret og godkendt for at sikre compliance.

Politik til udvikling og vedligeholdelse af services er etableret og anvendes til udviklingen i organisationen.

Leverandørforhold
Visma Dataløn har sikret beskyttelse af virksomhedens aktiver, der er tilgængelige for leverandører, herunder regelmæssig overvågning og revision af leverandørleverancer.

Styring af informationssikkerhedsbrud
Visma Dataløn har en konsekvent og effektiv tilgang til styring af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og svagheder.

Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring
Visma DataLøn sikrer kontinuitet og rettidig genopretning af forretningskritiske processer og systemer i tilfælde af en kritisk situation og sikrer, at kritiske processer virker på et hensigtsmæssigt niveau.

Compliance
Visma Dataløn har implementeret procedurer for at undgå brud på juridiske, lovmæssige eller kontraktlige forpligtelser i forbindelse med informationssikkerhed og eventuelle sikkerhedskrav.

Databehandleraftale

Mellem

IT Operators ApS
Jættevej 50b
4100 Ringsted
CVR 33255535
(herefter ”Databehandleren”)

og

Wax Facility Service ApS
Københavnsvej 11
4800 Nykøbing Falster
CVR 32102018
(herefter den ”Dataansvarlige”)

er der indgået nedenstående databehandleraftale (herefter ”Aftalen”) om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

1. Generelt

1.1 Aftalen vedrører Databehandlerens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer forbindelse med behandling af personoplysninger (herefter "Databeskyttelsesforordningen").

1.2 Databehandleren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

2.1 Databehandleren behandler i medfør af aftale med den Dataansvarlige Wax Facility Service ApS (herefter "Hovedaftalen") personoplysninger for den Dataansvarlige, hvor Databehandlerens behandlinger og formålet med behandlingerne er beskrevet.

3. Den Dataansvarliges rettigheder og forpligtelser

3.1 Den Dataansvarlige er dataansvarlig for de personoplysninger, som den Dataansvarlige instruerer Databehandleren om at behandle. Den Dataansvarlige har ansvaret for, at de personoplysninger, som den Dataansvarlige instruerer Databehandleren om at behandle må behandles af Databehandleren, herunder at behandlingen er nødvendig og saglig i forhold til den Dataansvarliges opgavevaretagelse.

3.2 Den Dataansvarlige har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen jf. Aftalens pkt. 1.1 og 1.2.

4. Databehandlerens forpligtelser

4.1 Databehandleren er databehandler for de personoplysninger, som Databehandleren behandler på vegne af den Dataansvarlige jf. pkt. 6. Databehandleren har som databehandler de pligter, som er pålagt en databehandler i medfør af lovgivningen jf. Aftalens pkt. 1.1 og 1.2.

4.2 Databehandleren behandler alene de overladte personoplysninger efter instruks fra den Dataansvarlige jf. pkt. 6, og alene med henblik på opfyldelse af Hovedaftalen.

4.3 Databehandleren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger som beskrevet i Databeskyttelsesforordningen.

4.4 Databehandleren skal ved forespørgsel fra den Dataansvarlige udarbejde en skriftlig redegørelse for sin behandling af de personoplysninger, der modtages fra den

Dataansvarlige. Denne redegørelse skal udleveres til den Dataansvarlige. Databehandleren har ret til en rimelig kompensation for omkostningerne herved. Kompensationen aftales skriftligt mellem Databehandleren og den Dataansvarlige med afsæt den tid og de ressourcer, Databehandleren har brugt.

4.5 Databehandleren skal på opfordring fra den Dataansvarlige mod rimelig kompensation for sine omkostninger herved hjælpe med at opfylde den Dataansvarliges forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt den Dataansvarliges forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud.

4.6 Databehandleren skal hjælpe den Dataansvarlige med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens art. 32-36.

4.7 Databehandleren garanterer fra 25. Maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Databehandlerens behandling af den Dataansvarliges personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

4.8 Hvis Databehandleren er etableret i en anden EU-medlemsstat, skal behandleren frem til 25. Maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

5.1 Ved underdatabehandler forstås en underleverandør, til hvem Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige.

5.2 Databehandleren er forpligtet til at oplyse den Dataansvarlige om, hvilke underleverandører, der anvendes. Den dataansvarlige kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler, medmindre der foreligger en konkret saglig begrundelse herfor.

5.3 Databehandleren skal indgå en skriftlig aftale med sine underdatabehandlere.

5.4 Underdatabehandleraftalen jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Databehandleren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. Maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder

kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5 Når Databehandleren overlader behandlingen af personoplysninger, som den Dataansvarlige er dataansvarlig for til underdatabehandlere, har Databehandleren over for den Dataansvarlige ansvaret for underdatabehandlerens overholdelse af disses forpligtelser jf. pkt. 5.3.

5.6 Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den Dataansvarlige.

5.7 Al kommunikation mellem Databehandlerens underdatabehandlere og den Dataansvarlige sker gennem Databehandleren, medmindre der er indgået særskilt aftale mellem den Dataansvarlige og underdatabehandleren. Den Dataansvarlige har pligt til skriftligt at orientere Databehandleren om sådanne aftaler.

5.8 Databehandleren skal forsikre sig mod eventuelle sanktioner fra myndighederne og regreskrav fra den Dataansvarlige i forbindelse med brud på persondatasikkerheden.

6. Instrukser

6.1 Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker udelukkende efter dokumenteret instruks. Det er Databehandlerens ansvar at sikre, at eventuelle underdatabehandlere får tilsendt den Dataansvarliges instruks.

6.2 Hvis en instruks fra den Dataansvarlige efter Databehandlerens opfattelse er i strid med lovgivningen jf. pkt. 1.2, skal Databehandleren give den Dataansvarlige besked herom.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Databehandleren skal fra 25. Maj 2018 iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et tilstrækkeligt sikkerhedsniveau.

7.2 Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget jf. pkt. 7.1.

7.3 Databehandleren og dennes ansatte og underdatabehandlere er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

7.4 Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Databehandlerens personoplysninger, om Databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed jf. pkt. 9.

7.5 Databehandleren er forpligtet til straks at underrette den Dataansvarlige om ethvert sikkerhedsbrud, samt ved manglende overholdelse af Databehandlerens samt eventuelle underdatabehandleres forpligtelser.

7.6 Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud jf. pkt. 7.5, uden forudgående skriftlig aftale med den Dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

8.1 Databehandlerens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f. eks. via. en cloudløsning eller en underdatabehandler skal ske i overensstemmelse med Databehandlerens instruks herfor.

8.2 Ved overførsel af persondata til underdatabehandlere i lande, der ikke er medlem af EU, er Databehandleren ansvarlig for kontraktligt at aftale med underdatabehandleren, at sikkerhedsniveauet som er gældende inden for EU's grænser skal iagttages.

8.3 Ved overførsel af persondata til tredjelande er Databehandleren og den Dataansvarlige i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

9. Tavshedspligt og fortrolighed

9.1 Databehandleren er – under og efter Hovedaftalens ophør – pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f jf. straffelovens § 152a finder anvendelse.

9.2 Databehandleren skal sikre, at alle, der behandler oplysninger omfattet af aftalen, herunder ansatte, tredjeparter og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1 Databehandleren er forpligtet til uden ugrundet ophold at give den Dataansvarlige nødvendige oplysninger til, at den Dataansvarlige til enhver tid kan sikre sig, at Databehandleren overholder de krav, der følger af denne aftale.

10.2 Databehandleren skal én gang årligt vederlagsfrit fremsende en erklæring til den Dataansvarlige om overholdelse af denne aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende anerkendte branchestandarder på området og skal omfatte både Databehandlerens og eventuelle underdatabehandleres databehandling. Den første erklæring skal foreligge 12 måneder efter Aftalens indgåelse.

10.3 I tilfælde af, at Datatilsynet ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Databehandleren og Databehandlerens underdatabehandlere sig til at stille tid og ressourcer til rådighed herfor. Databehandleren har ret til en rimelig kompensation for omkostningerne herved. Kompensationen aftales skriftligt mellem Databehandleren og den Dataansvarlige med afsæt den tid og de ressourcer, Databehandleren har brugt.

11. Ændringer i Aftalen

11.1 Den Dataansvarlige kan til enhver tid med et forudgående varsel på mindst 30 dage foretage ændringer i Aftalen. Ændringsprocessen og omkostningerne aftales skriftligt mellem den Dataansvarlige og Databehandleren i Hovedaftalen. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.

11.2 Hvis ændringer i lovgivningen jf. pkt. 1.1 og 1.2 eller dertilhørende praksis giver anledning til dette, er den Dataansvarlige med et varsel på 14 dage og uden at dette medfører krav om betaling fra Databehandleren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

12.1 Den Dataansvarlige træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.

12.2 Den Dataansvarlige skal senest 14 dage inden Hovedaftalens ophør skriftligt meddele Databehandleren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til den Dataansvarlige. I det tilfælde, hvor personoplysningerne tilbageleveres til den Dataansvarlige, skal Databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever den Dataansvarliges meddelelse.

12.3 Databehandleren skal fremsende dokumentation for, at den påkrævede sletning jf. pkt. 12.2, er foretaget.

12.4 Ved bortskaffelse af Databehandlerens eget IT-udstyr eller hvis Databehandleren er ansvarlig for at bortskaffe den Dataansvarliges IT-udstyr, er det Databehandlerens ansvar, at de personoplysninger, der er lagret på udstyret slettes.

13. Misligholdelse og tvister

13.1 Misligholdelse og tvister er reguleret i Hovedaftalen.

14. Erstatning og forsikring

14.1 Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen.

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parters underskrift og løber indtil ophør af Hovedaftalen.

15.2 Aftalen har virkning fra d. 24. maj 2018.

16. Formkrav

16.1 Aftalen skal foreligge skriftligt, herunder elektronisk hos Databehandleren og den Dataansvarlige.

For IT-Operators
Dato 16/5/2018

Kim Gregersen

For Wax Facility Service ApS
Dato 16/5/2018

Camillo Krog

Art. 30-dokumentation for behandlingsaktiviteter som databehandler

I det følgende vil de behandlingsaktiviteter, IT Operators foretager som databehandler blive gennemgået.

Dokumentationskravene for databehandlere omfatter jf. art. 30, stk. 2, litra a-d følgende:

a) Navn på og kontaktoplysninger for databehandleren og den dataansvarlige, på hvis vegne, databehandleren handler, samt hvis det er relevant, den dataansvarliges eller databehandlerens repræsentant og databeskyttelsesrådgiveren.
b) De kategorier af behandling, der foretages på vegne af den enkelte dataansvarlige.
c) Hvor det er relevant overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland eller organisationen, og i tilfælde af overførsler til lande, der er omfattet af art. 49, dokumentation for passende garantier.
d) Generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

Behandlingsaktiviteterne vil nedenfor blive gennemgået efter samme systematik, som angivet i bestemmelsen. Dokumentation vil blive udformet for hver enkelt kunde og gemt som bilag til denne rapport jf. nedenfor anførte skabeloner:

Webhosting

a) Navn og oplysninger
Databehandler: IT Operators ApS, Jættevej 50b, 4100 Ringsted, CVR: 33255535
Dataansvarlig: Wax Facility Service ApS, Københavnsvej 11, 4800 Nykøbing Falster, CVR: 32102018

b) Ved webhosting oprettes dedikerede dataområder individuelt til virksomhedens drift af det enkelte website. Data lagres på IT Operators egne servere gennem softwaren på IT Operators Microsoft og Linux-servere. Dataene gemmes lokalt på IT Operators egne servere.

c) Der foregår ikke overførsel af personoplysninger til tredjelande ved webhosting

d) Microsoft og Linux har ikke selv adgang til eller indblik i de oplysninger, der behandles i deres software.
IT Operators har som databehandler ved kontrakt med den dataansvarlige forpligtet sig til lovmæssig behandling af data for den dataansvarlige.
IT Operators sikrer sine systemer med opdateret antivirussoftware, firewall og lign. foranstaltninger. Efter IT Operators opfattelse frembyder det anvendte software den sikkerhed, der med rette kan forventes af en IT-virksomhed.

IT Operators har organisatorisk sikret sig, at adgangen til de fysiske serverrum er begrænset således, at alene direktøren og én navngiven medarbejder har nøgler og koder til disse rum.

IT Recovery

a) Navn og oplysninger
Databehandler: IT Operators ApS, Jættevej 50b, 4100 Ringsted, CVR: 33255535
Dataansvarlig: Wax Facility Service ApS, Københavnsvej 11, 4800 Nykøbing Falster, CVR: 32102018

b) Afhængigt af opgavens art, genskabes enkelte filer eller hele harddiskens indhold. I tilfælde, hvor en fil er slettet og der ikke foreligger back-up gennem et stykke software, benyttes der tredjeparts fil-recovery-software til manuelt at lokalisere og gendanne den slettede fil på enheden. I tilfælde, hvor større dele af harddiskens indhold skal genskabes til en ny disk, kan der afhængigt af situationen enten udføres en komplet diskkloning af den gamle harddisk til en ny fuldt funktionel harddisk. I andre tilfælde udføres der en manuel lokalisering og udtrækning af dataene fra den gamle harddisk til den nye harddisk. I visse tilfælde er det nødvendigt at opbevare de udtrukne data midlertidigt på et af IT Operators diskmedier, indtil den nye harddisk er tilgængelig, eksempelvis i forbindelse med bestilling af ny hardware til kunden.

I tilfælde, hvor det er selve computeren, der er defekt, men harddisken er fuldt funktionel, flyttes harddisken blot over i en ny computer. I en sådan recovery-proces, er der således ingen behandling af dataene.

c) Data overføres ikke til tredjelande. I visse meget særlige omstændigheder, afsendes disken til en specialist placeret i England til dataudtræk. I disse tilfælde informeres kunden dog særligt herom.

d) IT Operators har som databehandler ved kontrakt med den dataansvarlige forpligtet sig til lovmæssig behandling af data for den dataansvarlige.
IT Operators sikrer sine systemer med opdateret antivirussoftware, firewall og lign. foranstaltninger. Efter IT Operators opfattelse frembyder det anvendte software den sikkerhed, der med rette kan forventes af en IT-virksomhed.
IT Operators har organisatorisk sikret sig, at adgangen til de fysiske serverrum er begrænset således, at alene direktøren og én navngiven medarbejder har nøgler og koder til disse rum.

Opgavetyper, hvor IT Operators ikke fungerer som databehandler eller dataansvarlig

IT support ved kunden

Ved denne opgavetype kører IT Operators konsulenter ud til kunden og løser problemer relateret til deres IT-systemer. Denne opgavetype kan i teorien indebære, at IT Operators

konsulenter kommer til at se personoplysninger i form af f. eks. mails, som kunden ikke har minimeret på sin computerskærm. Aftalen indgået med kunden går dog ud på problemløsning – ikke behandling af data, hvorfor IT Operators i denne sammenhæng ikke betragtes som databehandler jf. *Vejledning om Dataansvarlige og Databehandlere, november 2017, Datatilsynet og Justitsministeriet, s. 24.*

Fjernsupport

Denne opgavetype er sammenlignelig med IT Support, der foretages ved kunden, idet IT Operators konsulenter har til opgave at løse et IT problem ved kunden, men i stedet for fysisk at køre ud til kunden, løses problemet i stedet ved at IT Operators får adgang til kundens computer gennem fjernsupport.

Denne opgavetype kan i teorien indebære, at IT Operators konsulenter kommer til at se personoplysninger i form af f. eks. mails, som kunden ikke har minimeret på sin computerskærm. Aftalen indgået med kunden går dog ud på problemløsning – ikke behandling af data, hvorfor IT Operators i denne sammenhæng ikke betragtes som databehandler jf. *Vejledning om Dataansvarlige og Databehandlere, november 2017, Datatilsynet og Justitsministeriet, s. 24.*