Bilag A. Oplysninger om behandlingen

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

Personkategori	Formål

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om de i Bilag D eller hovedaftalen beskrevne ydelser (karakteren af behandlingen)

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

Almindelige persondata (f.eks. navn, adresse, email, telefonnummer mv.).

Fortrolige persondata (CPR-nummer eller Væsentlige sociale problemer)

A.4. Behandlingen omfatter følgende kategorier af registrerede

Personkategori	Beskrivelse

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har den i Bilag D eller hovedaftalen anførte varighed

Bilag B. Underdatabehandlere

B.1. Godkendte underdatabehandlere

Leverandør	Land	Lovligt grundlag for processering uden for EU	Funktion
Lexoforms A/S	Danmark		Dokumentation
Uniconta	Danmark		Bogføring
Wolters Kluwer Danmark A/S	Danmark		Dokumentation
MD Soft ApS	Danmark		Dokumentation
Danske Lønsystemer A/S	Danmark		HR
PENNEO A/S	Danmark		Dokumentation
Visma e-conomic A/S	Danmark		Bogføring
Creditro A/S	Danmark		Dokumentation
Microsoft	Danmark		Backup
Microsoft Onedrive	Danmark		Backup

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Bilag C. Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand / instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører den i hovedaftalen/kontrakt eller i bilag D beskrevne behandling

C.2. Behandlingssikkerhed

Følgende sikkerhedsforanstaltninger er truffet:

Hvis der er tale om behandling af fortrolige, følsomme eller særlige kategorier af personoplysninger, skal der altid etableres et "højt" sikkerhedsniveau.

Tekniske sikkerhedsforanstaltninger (eksterne):

- SSL-krypteret forbindelse med klient og server
- 2-faktor validering ved eksternt login
- Adgangskode opbevares krypteret
- Passwords udskiftes regelmæssigt eller sikres på anden måde (eks. 2-faktor mv.).
- Løbende backup og logning.
- Underdatabehandlere er i EU eller i USA (alle med lovligt grundlag for processering)
- Driftsmiljøet er adskilt fra udviklings- og testmiljøer.

Tekniske sikkerhedsforanstaltninger (interne):

- Opdateret Antivirus på alle enheder der kan tilgå persondata.
- Opdateret Firewall på enheder der kan tilgå persondata samt på servere/driftscentre der måtte holde persondata.
- Passwords udskiftes regelmæssigt eller sikres på anden måde (eks. 2-faktor mv.).
- Løbende opdatering af operativsystemer og applikationer
- Løbende backup og logning.
- Ved overførsel af fortrolige, følsomme eller særlige personoplysninger benyttes kryptering

Organisatoriske sikkerhedsforanstaltninger:

- Alle medarbejdere er instrueret i beskyttelsen af personoplysninger og har underskrevet en medarbejderinstruks.

    - Medarbejderinstruksen opdateres og gennemgås mindst en gang årligt.
    - Medarbejderinstruksen gennemgås altid med nye medarbejdere i forbindelse med ansættelsen.
- Alle medarbejdere er pålagt tavshedspligt.
- Det overordnede ansvar for overholdelse af sikkerhedskravene, ligger ved databehandlerens ledelse, som typisk repræsenteres af IT-chefen.
- Persondata er kun tilgængelige for de medarbejdere der har en godkendelse og årsag til at skulle kunne tilgå disse data, og skal altid behandles fortroligt.
- Hvis der er tale om en stor mængde følsomme personoplysninger, så bør data adskilles hvor det er muligt, således at adgangen begrænses til absolut minimum.

Fysiske sikkerhedsforanstaltninger:

- Kontorer og bygninger aflåses, når de forlades.
- Sikre at driften kan fortsætte ved strømafbrydelser og evt. redundante kommunikationsforbindelser
- Arkiver med følsomme personoplysninger opbevares altid aflåst, hvor der ligeledes er alarm og overvågning etableret.
- Backup opbevares aflåst (både interne og eksterne), der laves en løbende genindlæsningstest, således at det sikres at backup'en virker og indeholder valide data.
- Alle fysiske medier (papir, USB drev mv.) destrueres på forsvarligvis, hvis de har været benyttet til at opbevare persondata.

Driftsmæssig sikkerhed.

- Udvikling, Test og Produktionsmiljøer er adskilte.
    - Udvikling og Test foretages af forskellige personer.
- Der tilpasses og kontrolleres løbende kapaciteter i forhold til opretholdelse af driften.
- Løbende password skift på både interne og eksterne systemer.
- Logning af afviste logon forsøg med automatisk alarmering.

C.3. Bistand til den dataansvarlige

Databehandleren skal så vidt muligt, bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre de i Bilag C.2 angivne tekniske og organisatoriske foranstaltninger.

C.4. Opbevaringsperiode / sletterutine

Personoplysninger opbevares i hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret, med mindre andet er aftalt i Bilag D / hovedaftalen eller i særlige vilkår.

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

C.5. Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske, på andre lokaliteter end databehandlerens eller underdatabehandlerens lokaliteter

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren overfører ikke personoplysninger til tredjelande, undtagen til de generelt godkendte underdatabehandlere listet i Bilag B

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

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

Databehandleren skal 1 gang årligt for egen regning indhente en erklæring/inspektionsrapport fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at der kan anvendes følgende type af erklæring

”Underskrevne uafhængige tredjepart (Navn, adresse, kontaktperson, telefon, email, evt. DPO med angivelse af navn, adresse, tlf og mail bekræfter at have gennemgået de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren har oplyst til den dataansvarlige i forbindelse med indgåelse af denne databehandleraftale.”

Erklæringen/inspektionsrapporten synliggøres/fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen/inspektionsrapporten og kan i sådanne tilfælde anmode om en ny erklæring/inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen/inspektionsrapporten, er den dataansvarlige berettiget til at

anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, af lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendig, Vurderingen skal bero på fakta og ikke fornemmelse. Fysisk inspektion kræver forudgående aftale med databehandlerne, og med et forudgående varsel på 3 uger, så databehandleren er forberedt på at kunne afsætte de nødvendige ressourcer til det."

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

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

Databehandlerens revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandleren sker på samme måde som den dataansvarliges revisioner hos databehandleren, se punkt C.7.

Bilag D. Parternes regulering af andre forhold, herunder instruks vedr. behandling af personoplysninger

Se den mellem parterne indgåede hovedaftale/kontrakt.

Brud på datasikkerheden:
Hvis der sker brud på datasikkerheden, skal databehandler medsende dokumentation for de faktiske omstændigheder ved bruddet, dets virkninger, de trufne afhjælpende foranstaltninger, og hvis

databehandleren har fået bemyndigelse til at foretage underretning til de registrerede, at oplyse om der er foretaget underretning til de registrerede og i givet fald hvorledes.