

DATABASEHANDLERAFTALE

Standardkontraktsbestemmelser

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

mellem

Kunden (som angivet i Hovedaftalen)

herefter ”den Dataansvarlige”

og

EPONA A/S

Boulevarden 19E

7100 Vejle

Danmark

CVR 45275027

herefter ”Databehandleren”

der hver især er en ”Part” og sammen udgør ”Parterne”

Har aftalt følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde Databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

Indhold

Præambel.....	3
Den Dataansvarliges rettigheder og forpligtelser	4
Databehandleren handler efter instruks	4
Fortrolighed	5
Behandlingssikkerhed	5
Anvendelse af underdatabehandlere	6
Overførsel til tredjelande eller internationale organisationer	7
Bistand til den dataansvarlige	8
Underretning om brud på persondatasikkerheden	10
Sletning og returnering af oplysninger	10
Revision, herunder inspektion	11
Parternes aftale om andre forhold.....	11
Ikrafttræden og ophør	11
Kontaktpersoner databehandleren	12
Bilag A Oplysninger om behandlingen	13
Bilag B Underdatabehandlere	17
Bilag C Instruks vedrørende behandling af personoplysninger	18
Bilag D Parternes regulering af andre forhold	26

Præambel

1. Disse Bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den Dataansvarlige. Bestemmelserne er indgået i tillæg til Parternes hovedaftale ("Aftalen")
2. Disse bestemmelser er udformet med henblik på Parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (Databeskyttelsesforordningen).
3. I forbindelse med leveringen af de af **Bilag A** angivne tjenesteydelser og leverancer behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den Dataansvarliges betingelser for Databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den Dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den Dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med Databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter Databeskyttelsesforordningen eller enhver anden lovgivning.

Den Dataansvarliges rettigheder og forpligtelser

1. Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den Dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den Dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som Databehandleren instrueres i at foretage.

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. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den Dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

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

Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den Dataansvarlige og Databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den Dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger
- b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
- c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

- d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal Databehandleren – uafhængigt af den Dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den Dataansvarlige stille den nødvendige information til rådighed for Databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
3. Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den Dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den Dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den Dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i Databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse

med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den Dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når Databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den Dataansvarlige, skal Databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og Databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter disse Bestemmelser og Databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den Dataansvarliges anmodning herom – i kopi til den Dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.
6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af Databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Databehandleren på baggrund af dokumenteret instruks herom fra den Dataansvarlige og skal altid ske i overensstemmelse med Databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Databehandleren ikke er blevet instrueret i at foretage af den Dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt, skal Databehandleren underrette den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - b. behandle personoplysningerne i et tredjeland
4. Den Dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i Databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i Databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i Databeskyttelsesforordningens kapitel V.

Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i Databeskyttelsesforordningens kapitel III.

Dette indebærer, at Databehandleren så vidt muligt skal bistå den Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
- b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
- c. indsigtssretten

- d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til Bestemmelse 6.3., bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:
- a. den Dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den Dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - c. den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d. den Dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed Databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. Databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den Dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som Databehandleren skal tilvejebringe i forbindelse med sin bistand til den Dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den Dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Ønsker den Dataansvarlige tilbagelevering af personoplysninger henvises der til Bilag C, pkt. C.4.

Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige.
2. Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den Dataansvarliges eller Databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af Databeskyttelsesforordningen.

Ikrafttræden og ophør

1. Bestemmelserne træder i kraft ved indgåelse af Aftalen.
2. Begge Parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af løsningen vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af løsningen vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

Kontaktpersoner hos databehandleren

1. Den Dataansvarlige kan kontakte Databehandleren via. nedenstående kontaktpersoner
2. Databehandleren er forpligtet til løbende at orientere den Dataansvarlige vedrørende kontaktpersoner

På vegne af Epona

Complianceafdelingen: Compliance@epona.com

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen af personoplysninger, på vegne af den Dataansvarlige, er at sikre levering af ydelser og leverancer i forbindelse med Parternes indgåelse af Aftalen om levering af:

Unik Advosys CE / JustiCase / JustiFinance /JustiBusiness: Programsuite ("Løsningerne") til udøvelse af advokatvirksomhed herunder primært sagsjournalisering

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

Hosting af Unik Advosys CE

Behandlingen sker primært i form af opbevaring, oprettelse, redigering, vedligeholdelse og lignende af de personoplysninger om klienter hos den Dataansvarlige som den Dataansvarlige administrerer ved hjælp af Løsningerne samt oplysninger om den Dataansvarliges medarbejdere efter den Dataansvarliges instruks.

JustiCase / JustiBusiness

Behandlingen i JustiCase / JustiFinance / JustiBusiness sker i form af opbevaring m.v. af den Dataansvarliges data i en SaaS-løsning (Software-as-a-Service).

Datakonvertering

Behandlingen i form af datakonvertering består i, at der i den gradvise overgang fra Unik Advosys CE til JustiCase, JustiFinance eller til JustiBusiness vil ske konvertering af den Dataansvarliges data på instruks fra den Dataansvarlige. Nærmere beskrivelse af den gradvise overgang findes i Aftalen.

I det omfang den Dataansvarlige i øvrigt instruerer Databehandleren i foretage datakonvertering af den Dataansvarliges data vil en sådan form for behandling også være omfattet af disse Bestemmelser.

Support

Bestemmelserne omfatter også behandling af den Dataansvarliges personoplysninger, som sker i forbindelse med, at den Dataansvarlige modtager programsupport og/eller teknisk support, der kan gives telefonisk, online gennem Connect eller on-site hos den Dataansvarlig, hvor Databehandlerens medarbejdere har adgang til at se, redigere, slette, m.v. i personoplysninger, og hvor dette sker under instruks fra den Dataansvarlige.

Konsulentytelser i form af implementering, opsætning, undervisning med brug af den Dataansvarliges data og lign.

I det omfang den Dataansvarlige instruerer Databehandleren til at foretage behandling af den Dataansvarliges personoplysninger som led i udførelse af konsulentopgaver i form af implementering, opsætning og undervisning, gælder behandlingen tillige for denne form for behandling. Det kan være alle former for behandling, som den Dataansvarlige instruerer Databehandleren om, herunder men ikke begrænset til organisering, systematisering, tilpasning eller ændring, genfindning, søgning, brug, formidling, samkøring, begrænsning og sletning. Behandling i form af konsulentytelser vil dog aldrig omfatte opbevaring af den Dataansvarliges personoplysninger.

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

Almindelige personoplysninger

- Navne og adresseoplysninger
- Registreringsoplysninger, herunder civilstatus
- Kommunikationsoplysninger (telefon, mobil, mail, fax, etc.)

- Kopi af legitimation (fx pas) til hvidvask
- Saldo- og betalingsoplysninger, herunder kontooplysninger
- Inkassooplysninger, herunder RKI-status via. integration til RKI Data og KreditVagt
- Oplysninger vedrørende gældssanering
- CVR-numre

Følsomme personoplysninger

- Det er muligt at angive følsomme personoplysninger i fritekstfelter og dokumenter (fotos, mails, sagsakter mv.), men Databehandleren har ikke designet felter i systemet til at indeholde følsomme personoplysninger.

Der vil ske opbevaring af disse oplysninger, hvor den Dataansvarlige under Unik Advosys CE er hostet hos Epona og ved anvendelse af SaaS-løsningerne JustiCase og JustiBusiness.

Fortrolige personoplysninger

- Personnumre (CPR-numre), jf. Databeskyttelsesloven

A.4 Behandlingen omfatter følgende kategorier af registrerede

Databehandleren behandler personoplysninger om følgende kategorier af registrerede på vegne af den Dataansvarlige:

- Dataansvarliges ansatte, tidligere ansatte, jobansøgere
- Klienter, sagspartner, sagsmodparter (tredjemand), vidner
- Leverandører, samarbejdspartnere

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige påbegyndes ved indgåelse af Aftalen og ophører samtidig med ophør af Aftalen, jf. dog afsnittet umiddelbart nedenfor og punkt C.4.

Hvis Aftalen mellem Databehandler og Dataansvarlig indeholder bestemmelser om, at Databehandleren kan varetage afgrænsede databehandleropgaver efter ophør af Aftalen, sker den fortsatte databehandling efter de retningslinjer, der var gældende ved Aftalens ophør.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere, der måtte være relevant for den Dataansvarlige:

NAVN OG ADRESSE	BESKRIVELSE AF BEHANDLING	BEHANDLINGSAKTIVITET
Vipre Adresse: Sportorno Allé 12 2630 Taastrup CVR nr.: 22117833	Vipre leverer scanning af ind- og udgående mails for spam og vira. Uønskede mails sættes i karantæne. Mails opbevares som udgangspunkt i 14 dage eller længere Vipre håndterer endvidere signering, kryptering og dekryptering af mails, når det er valgt.	Unik Advosys CE (Sikker mail-løsning)
Charlie Tango (KMD) Adresse: Lautrupparken 40 2750 Ballerup CVR nr.: 26911745	Alle leverancer til e-Boks skal gå igennem en dokumentleverandør. På modulet til e-Boks levering er Charlie Tango er dokumentleverandør via modtagers cpr nr..	Unik Advosys C (E-boks integration)
Penneo Adresse: Enghavevej 40, 4. Sal 1674 København V CVR nr.: 35633766	Penneo anvendes til digital underskrift via MitID. De underskrevne dokumenter er tilgængelige via Penneos løsning. Dokumenter sendes via modtagers mailadresse og ved sikker mail anvendes cpr. nr. også. Afsender er oprettet hos Penneo med navn og mailadresse.	Unik Advosys CE (Digital underskrift)
CIM Mobility Adresse:	CIM Mobility leverer på baggrund af tilsendt mobiltelefonnummer SMS-beskeder til modtager.	Unik Advosys CE (Advosys SMS-modul)

NAVN OG ADRESSE	BESKRIVELSE AF BEHANDLING	BEHANDLINGSAKTIVITET
Fælledvej 17 7600 Struer CVR nr.: 27913334		
Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18, Ireland	Microsoft leverer via Microsoft Azure en B2C log-in-løsning. Denne løsning anvendes, når den Dataansvarlige logger ind på JustiCase eller JustiBusiness. Det er alene den Dataansvarliges log-in oplysninger, der opbevares.	JustiCase JustiFinance JustiBusiness
Unik System Design A/S Adresse: Boulevarden 19E 7100 Vejle CVR nr.: 17512692	Unik leverer, drifter og supporterer den fysiske infrastruktur for den platform, hvor Løsningerne afvikles, herunder servere, netværk, storage system, firewall, internetforbindelse, strømforsyninger, brandslukningsudstyr og køling. Samtidig leverer Unik også backup samt opbevaring af off-site immutable backup.	Unik Advosys CE JustiCase JustiBusiness JustiFinance

B.2. Varsel for godkendelse af underdatabehandlere

Bestemmelsernes pkt. 7.3 beskriver proceduren for varsling af underdatabehandlere.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker som led i, at Databehandleren udfører følgende:

Levering af ydelser og leverancer i forbindelse med Parternes indgåelse af Aftalen om levering af: Unik Advosys CE / JustiCase / JustiFinance / JustiBusiness: Programsuite til udøvelse af advokatvirksomhed herunder primært sagsjournalisering (Løsningerne), jf. Bilag A.1.

Databehandleren må alene behandle den Dataansvarliges personoplysninger i det omfang dette er nødvendigt for at levere de ovenfor beskrevne ydelser og leverancer til den Dataansvarlige.

Såfremt den Dataansvarlige fastholder en instruks på trods af en indsigelse fra Databehandleren, har Databehandleren ret til at kontakte Datatilsynet med henblik på at afprøve parternes forskellige fortolkninger. Parterne er enige om at afvente Datatilsynets svar, inden der tages beslutninger om instruksens opretholdelse.

C.2. Behandlingssikkerhed

Fysisk sikkerhed

2.1 Brand, strømafbrydelser, oversvømmelser m.v.

Den Dataansvarliges data i Løsningerne er sikret på sædvanlig vis mod brand og således, at driften kan fortsætte, også ved strømafbrydelser af en vis varighed, ligesom der er beskyttet på sædvanlig vis mod oversvømmelse.

Hostingcentre er udstyret med redundante strømforsyninger og køleanlæg, brandsikringer og UPS'er. Faciliteterne overvåges dertil af en lang række tekniske alarmer og sensorer.

2.2 Adgangskontrol

Den Dataansvarliges data i Løsningerne er beskyttet med sædvanlige indbruds- og tyverialarmer på alle Databehandlerens lokationer, herunder hosingcentre. Det er udelukkende relevante personer, der har adgang til Databehandlerens faciliteter, og der er fysisk adgangskontrol til alle lokationer.

Teknisk sikkerhed

3.1 Firewalls og antivirus

Alle arbejdsmaskiner og servere er udstyret med antivirussoftware med henblik på at blokere vira, malware m.v. Netværket er placeret bag firewalls for at kunne beskytte mod uautoriseret adgang.

3.2 Kryptering

Der er etableret kryptering, hvor dette er en del af Aftalen.

3.3 Lagring af data og backup

Den Dataansvarliges data lagres enten alene i den Dataansvarliges egne systemer eller Databehandlerens hostingcenter.

Der foretages løbende og daglig backup af alle de lagrede data, således at det sikres, at tabte data så vidt muligt kan genetableres.

Organisatorisk sikkerhed

4.1 Adgangsrettigheder

Medarbejdere hos Databehandleren har alene adgang til de systemer, der er relevante for den enkelte medarbejder.

Ved fjernadgang til den Dataansvarliges udstyr, udfører medarbejdere hos Databehandleren arbejdet efter instruks fra den Dataansvarlige. I den forbindelse kan medarbejdere hos Databehandleren tilfældigt få adgang til persondata hos den Dataansvarlige og er i den forbindelse underlagt fortrolighedsaftaler.

Alle ansatte har unikke brugernavne og passwords. Brugernavne og passwords oprettes og ændres efter alment anerkendte principper. Der foretages registrering af alle afviste adgangsforsøg. Efter gentagne afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, blokeres der for yderligere forsøg.

4.2 Fortrolighed

Alle medarbejdere hos Databehandleren, der har adgang til personoplysninger, er underlagt fortrolighedsaftaler.

4.3 Logning

Der sker normal logning af alle tilgange til tjenester nævnt i bilag A.2. Sådan logning registrerer tidspunktet, hvilken medarbejder, der tilgår tjenesterne samt varigheden af tilgangen. Logen gemmes i minimum 6 måneder.

Sker adgangen vha. fx Teamviewer eller tilsvarende tjeneste, hvor Databehandleren bliver inviteret ind i den Dataansvarliges system via en bruger hos den Dataansvarlige, vil der ikke ske automatisk logning af adgang hos Databehandleren.

Sletning og kassation

5.1 IT-lagermedier

Data slettes efter instruks fra den Dataansvarlige. Harddiske og øvrige lagermedier, der udgår fra driften, bliver destrueret på en måde, så det ikke er muligt at genetablere data. Alle genbrugte diske bliver formateret i overensstemmelse med gældende branchestandarder.

C.3 Bistand til den Dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger i henhold til C.2.

Den Dataansvarlige skal dække alle Databehandlerens omkostninger ved bistand i henhold til Bestemmelse 9.1, herunder til eventuelt involverede underdatabehandlere. Databehandlerens bistand afregnes til Databehandlerens til enhver tid gældende timetakt for sådant arbejde

C.4 Opbevaringsperiode/sletterutine

I tilfælde af Aftalens ophør, uanset årsag, skal Databehandleren enten slette eller tilbagelevere alle personoplysninger til den Dataansvarlige. Sletning omfatter alle personoplysninger og eksisterende kopier heraf, medmindre EU-retten eller dansk national lovgivning foreskriver opbevaring af personoplysningerne. Tilbagelevering omfatter alle personoplysninger omfattet af Aftalen, som den Dataansvarlige ikke allerede er i besiddelse af. Den Dataansvarlige afholder alle omkostninger, såfremt denne vælger tilbagelevering af oplysningerne, og Databehandleren er berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al arbejdstid, som en sådan anmodning måtte medføre Databehandleren.

Databehandleren skal slette alle personoplysninger, som Databehandleren behandler på vegne af den Dataansvarlige, senest 90 dage efter Aftalens ophør, såfremt den Dataansvarlige ikke senest 30 dage efter Aftalens ophør instruerer Databehandleren i at tilbagelevere personoplysningerne.

Uanset det foranstående er Databehandleren berettiget til, i det omfang det er nødvendigt for at kunne dokumentere levering af ydelserne omfattet af Aftalen eller forsvare sig mod retskrav, at gemme en kopi af den Dataansvarlige personoplysninger. Personoplysningerne må i så fald udelukkende behandles til de anførte formål.

C.5 Lokaltet for behandling

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

Databehandlerens lokationer:

Hjulmagervej 8B

7100 Vejle

Danmark

Underdatabehandlere:

Se lokationer under pkt. B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren er med disse Bestemmelser instrueret i at overføre Personoplysninger til underdatabehandlere i tredjelande, i det omfang sådanne underdatabehandlere er angivet med lokation i et tredjeland på listen i Bilag B ved indgåelsen af Bestemmelserne. Databehandleren er berettiget og bemyndiget til frit at vælge og etablere juridisk grundlag til overførelse.

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

Såfremt anvendelsen af en ny underdatabehandler, ændring i anvendelsen af en eksisterende godkendt underdatabehandler eller det i øvrigt vil være nødvendigt at overføre personoplysninger til et eller flere tredjelande eller organisationer udenfor EEA, skal

Databehandleren indhente Dataansvarliges specifikke godkendelse samt instruks hertil. Giver den Dataansvarlige i disse situationer ikke sit specifikke samtykke og/eller sin instruks, er Databehandleren berettiget til at opsige den del af Aftalen, der vedrører services, som ville have betydet en overførsel af personoplysninger til et eller flere tredjelande eller organisationer udenfor EEA. Den berørte del af Aftalen kan opsiges uden af den Dataansvarlige har ret til erstatning med effekt fra tidspunktet, hvor ændringerne relateret til overførslen er tiltænkt at skulle få effekt. Øvrige dele af Aftalen skal fortsat være gældende mellem Parterne.

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

Databehandleren skal stille rimelig og nødvendig information til rådighed for den Dataansvarlige med henblik på at dokumentere overholdelse af Databeskyttelsesforordningens artikel 28 og disse Bestemmelser, jf. Databeskyttelsesforordningens artikel 28, stk. litra h. Databehandleren skal på den Dataansvarliges anmodning levere en IT-sikkerhedsrapport dækkende forhold omfattet af Aftalen mellem den Dataansvarlige og Databehandleren. En revisionserklæring med høj grad af sikkerhed, herunder en ISAE 3000-erklæring, skal anses som tilstrækkelig dokumentation i dette henseende. Såfremt den Dataansvarlige anmoder om information og/eller dokumentation, som ligger ud over Databehandlerens egen interne standard dokumentation skal den Dataansvarlige dække alle Databehandlerens omkostninger til at levere den nødvendige dokumentation/information.

I det omfang at den Dataansvarlige anmoder om audit hos Databehandleren, stiller Databehandleren de for behandlingen relevante systemer og faciliteter hos Databehandleren til rådighed. Sådan auditering skal udføres af en uafhængig auditør på hverdage og indenfor almindelige kontortider med forudgående varsel på minimum 14 dage og under iagttagelse af almindelige fortrolighedsprocedurer og principper. Den uafhængige auditør må ikke være en repræsentant for en konkurrent til Databehandleren.

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

Databehandleren skal ved antagelse af en underdatabehandler, baseret på en konkret vurdering af risikoen ved behandlingen, tage stilling til hvordan og hvor ofte Databehandleren vil føre kontrol med underdatabehandleren. Databehandleren skal på den Dataansvarliges anfordring levere dokumentation på, at Databehandleren har overholdt sine forpligtelser til at kontrollere sine underdatabehandlere. En revisionserklæring, der stilles vederlagsfrit til rådighed for Dataansvarliges, skal anses som tilstrækkelig dokumentation i dette henseende.

Bilag D Parternes regulering af andre forhold

Databehandlerens totale ansvar overfor den Dataansvarlige i medfør af disse Bestemmelser er, uanset grundlaget herfor, herunder i form af videreførelse af krav fra de registrerede, begrænset til 500.000 kr.

I tillæg til Aftalen gælder følgende: Parterne er i intet tilfælde ansvarlig for indirekte tab og følgeskader, herunder driftstab, der måtte opstå i tilknytning til manglende overholdelse af Bestemmelserne. Rejses der krav fra tredjemand mod Databehandleren for forhold, der udspringer af Aftalen, herunder Bestemmelserne, skal den Dataansvarlige skadesløsholde Databehandleren for dele af sådanne krav, der sammen med et eventuelt krav fra den Dataansvarlige overstiger Databehandlerens samlede økonomiske ansvar som angivet ovenfor.