Visma IMS

Databehandler-aftale

Standardkontraktsbestemmelser

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

mellem

Navn
CVR
Adresse
Postnummer
Danmark

herefter ”den dataansvarlige”

og

Visma IMS A/S
CVR: 25862015
Søren Frichs Vej 44D,
8230 Åbyhøj
Danmark

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 per- soners grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne 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 allerede indgåede aftale, "Abonnementsaftalen".

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.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmel- ser i andre aftaler mellem parterne, herunder i hovedaftalen.

6. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

7. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, her- under om behandlingens formål og karakter, typen af personoplysninger, kategori- erne af registrerede og varighed af behandlingen.

8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

9. 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.

10. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

11. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

12. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandle- ren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. 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 medlemsstaternes[1] 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.

4. 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.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktions- beføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbe- stemt 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 nødven- dig, 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.

6. 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.

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

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og friheds- rettigheder 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 personop- lysninger 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 ud- gør 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 alle- rede 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.

4. 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 Bilag 1 til hovedaftalen - Generelle leveringsbetingelser, eller af denne aftales bilag D.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelses forordningens 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 anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen 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 **90 dages** varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede under- databehandler(e). 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. 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 databe- skyttelsesforpligtelser 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 underdatabehandler aftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvar- lige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af under- databehandlerens 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.

8. 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 underret- ning 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. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. 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.

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 om- handlet i databeskyttelsesforordningens kapitel V.

9. 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 databeskyttelsesforordnin- gens 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 registre- rede

b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
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 unødig 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 in- debærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig 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 ana- lyse 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.

   Parternes eventuelle regulering/aftale om vederlag eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af denne aftales bilag D.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig 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 24 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. Er den dataansvarlige uden unødig forsinkelse blevet underrettet af databehandleren om et brud på persondatasikkerheden i overensstemmelse med Bestemmelse 10, og skyldes bruddet alene den dataansvarliges forhold, er databehandleren berettiget til særskilt vederlag for tid brugt på underretningen.

5. 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.

11. 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 dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver op- bevaring af personoplysningerne.

12. 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 lov-

givningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehand- lerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

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 tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Aftalen er gældende, så længe behandlingen består. Uanset den allerede indgåede aftale og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

5. Underskrift
   På vegne af den dataansvarlige

Navn	Navn
Stilling	xx
Telefonnummer	xx
E-mail	xx

På vegne af databehandleren

Navn	Maria Radmer
Stilling	Data protection manager

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.
   På vegne af den dataansvarlige

Navn	Navn
Stilling	xx
Telefonnummer	xx
E-mail	xx

På Vegne af databehandleren

Navn	Maria Radmer
Stilling	Data protection manager
Telefonnummer	24499972
E-mail	maria.radmer@visma.com

Bilag A Oplysninger om behandlingen

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

Behandlingen af den dataansvarliges personoplysninger sker med det formål at opfylde den indgåede aftale mellem databehandleren og den dataansvarlige om databehandlerens levering af dennes digitale løsning(er) jf. Abonnementsaftalen.

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

Databehandleren stiller dennes digitale løsning(er) til rådighed for den dataansvarliges brug og udfører løbende support og opdateringer af systemet som angivet nærmere i Abonnementsaftalen. Behandling indebærer desuden både teknisk- og brugersupport.

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

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

Navn, e-mailadresse, telefonnummer, adresse, medlemsnummer, uddannelse, ansættelsesforhold, samtykke. Vælg evt. andre typer herunder

Type medlemsskab
Medlemsnummer
Betalingskortoplysninger

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- ☐ Racemæssig eller etnisk baggrund
- ☐ Politisk overbevisning
- ☐ Religiøs overbevisning
- ☐ Filosofisk overbevisning
- ☐ Fagforeningsmæssige tilhørsforhold
- ☐ Helbredsforhold herunder misbrug af medicin, narkotika, alkohol m.v.
- ☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6, 9, 10, samt databeskyttelseslovens § 8):

- ☐ Strafbare forhold
- ☐ Væsentlige sociale problemer
- ☐ Andre rent private forhold, som ikke er nævnt ovenfor:

_____

_____

Oplysninger om cpr-nummer (jf. databeskyttelseslovens § 11, stk. 1)

☐ CPR-numre

A.4. Behandlingen omfatter følgende kategorier af registrerede

[BESKRIV KATEGORIERNE AF REGISTREREDE]

Kreditorer
Ansatte
Studerende/kursister/elever
Medlemmer
Borgere

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Der foretages opbevaring af personoplysninger, så længe den dataansvarlige selv ønsker at opbevare personoplysninger. Det er således op til den dataansvarlige selv at fastsætte kassation datoer og de endelige sletningsrutiner. Behandlingen er således ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne. Herunder hører også ophør af adgang til systemerne når Abonnementsaftalen ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Nedenfor fremgår en oversigt over databehandlerens underdatabehandlere på produktniveau. Afhængig at de tilvalg som er foretaget i Hovedaftalen gør nedenstående oversigt af underdatabehandlere sig gældende:

Underdatabehandlere for Visma Case			
NAVN	**CVR**	**ADRESSE**	**BESKRIVELSE AF BEHANDLING**
Cloud Factory	35393692	Vestergade 4, 6800 Varde	Cloud Factory stiller IT hostingmiljø til rådighed for Visma IMS A/S. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Acronis International GmbH GmbH	874459	Rheinweg 9, 8200 Schaffhausen, Switzerland	Acronis anvendes til hosting af løsningen, herunder lagring og processering af data. Denne behandling af data sker i henhold til deres standard underdatabehandleraf- tale.
Zendesk	26-4411091	1019 Market Street San Francisco, CA 94103, USA	Zendesk anvendes til at hoste support-ticket-system til afsendelse af beskeder fra løsningen. Denne behandling af data sker i henhold til deres standard underdatabehandleraf- tale.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3. Sal, 5000 Odense C, Danmark	Ubivox anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.

Compaya A/S	31375428	Palægade 4, 2. tv. 1261 Kbh. Danmark	Compaya anvendes som leverandør af SMS gateways til udsendelse af SMS'er. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale

Underdatabehandlere for IMS DigitalPost Cloud			
NAVN	**CVR**	**ADRESSE**	**BESKRIVELSE AF BEHANDLING**
Cloud Factory	35393692	Vestergade 4, 6800 Varde	Cloud Factory stiller IT hostingmiljø til rådighed for Visma IMS A/S. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Acronis International GmbH GmbH	874459	Rheinweg 9, 8200 Schaffhausen, Switzerland	Acronis anvendes til hosting af løsningen, herunder lagring og processering af data. Denne behandling af data sker i henhold til deres standard underdatabehandleraf- tale.
Zendesk	26-4411091	1019 Market Street San Francisco, CA 94103, USA	Zendesk anvendes til at hoste support-ticket-system til afsendelse af beskeder fra løsningen. Denne behandling af data sker i henhold til deres standard underdatabehandleraf- tale.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3. Sal, 5000 Odense C, Danmark	Ubivox anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.

Underdatabehandlere for IMS Faktura Flow

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Cloud Factory	35393692	Vestergade 4, 6800 Varde	Cloud Factory stiller IT hostingmiljø til rådighed for Visma IMS A/S. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Zendesk	26-4411091	1019 Market Street San Francisco, CA 94103, USA	Zendesk anvendes til at hoste support-ticket-system til afsendelse af beskeder fra løsningen. Denne behandling af data sker i henhold til deres standard underdatabehandleraf- tale.
Heysender ApS	31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Danmark	Heysender anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3. Sal, 5000 Odense C, Danmark	Ubivox anvendes til at hoste SMTP-service til udsendelse af e-mails. Denne behandling af data sker i henhold til deres standard underdatabehandleraftale.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke foruden 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.

Databehandleren skal opretholde en til enhver tid gældende liste over underdatabehandlere på databehandlerens hjemmeside, som dermed udgør gældende bilag B. Underdatabehandleraftalerne rekvireres via hjemmesiden eller ved skriftlig anmodning til databehandleren.

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 følgende:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren opbevarer data for den dataansvarlige i systemet og udfører løbende support og backup.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandlerens digitale løsning omfatter behandling af personoplysninger som følger af nærværende bilag A. Derfor har databehandleren valgt at implementere et højt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog under alle omstændigheder og som minimum gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Informationssikkerhed

Databehandleren 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 databehandlerens 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.

Instruks

Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende og mindst en gang årligt en vurdering af, om procedurerne skal opdateres.
Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.

Fysisk sikring og miljøsikring

Databehandlerenen skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger herunder opbevaring af personoplysninger omfattet af databehandleraftalen mod uvedkommende adgang og manipulation.
Databehandleren har passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang til lokaler, hvor der behandles personoplysninger. Databehandleren skal

desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler.

Databehandleren sikrer, at niveauet for den fysiske sikkerhed til enhver tid er afstemt med det aktuelle trusselbillede samt den følsomhed og mængde af personoplysninger, som databehandleraftalen omfatter.

Kommunikationsforbindelser og kryptering
Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk herunder beskytte data under transmission og adgang via internettet samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

Databehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingsskik.

I det omfang det er et krav i medfør af gældende national og international lovgivning, standarder vedrørende kryptering af klassificeret information eller god databehandlingsskik anvender databehandler krypteringsteknologier og andre tilsvarende foranstaltninger.

Firewall eller lignende tekniske foranstaltninger
Alle databehandlerens servere er placeret og beskyttet bag en passende firewall. Al trafik fra kunde til hostede systemer foretages på krypterede forbindelser. Databehandleren sikrer at firewall trafik logges og operativsystemer har aktiveret lokale firewalls.

Antivirus
Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.

Sikkerhedskopiering
Databehandleren skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen.

Sikkerhedskopiering af konfigurationsfiler og data skal finde sted i et ubrudt forløb, således at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Sikkerhedskopierne skal opbevares fysisk adskilt fra primære data og i et sikkerhedsgodkendt datacenter.

Anvendelse af hjemme/fjernarbejdspladser
Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikre databehandleren at disse lever op til de sikkerhedsmæssige krav i denne databehandleraftale med bilag og lovgivning i øvrigt.

Databehandler skal blandt andet opfylde følgende:

- At der anvendes krypteret forbindelse mellem ad hoc arbejdspladsen og databehandlerens/dataansvarliges netværk

- Databehandlerens har en intern instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal databehandleren, hvis det er teknisk muligt, anvende 2-faktor-autentifikation.

Instruktion af medarbejdere

Databehandleren sikrer, at ansatte til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker og arbejdsgange og om deres tavshedspligt.

Der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt, inden for det seneste år. Informationssikkerhedspolitikken er kommunikeret til relevante interessenter herunder databehandlerens medarbejdere.

Informationssikkerhedspolitikken lever generelt op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.
Der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.

Medarbejdere har underskrevet en fortrolighedsaftale. Medarbejdere er blevet introduceret til:
- Informationssikkerhedspolitikken
- Procedurer vedrørende databehandling, samt anden relevant information

Der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. inddrages.
Der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samar- bejde.

Databehandleren udbyder awareness-træning til medarbejderne, der omfatter generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.

Der foreligger dokumentation for, at alle medarbejdere, som enten har adgang til eller behand- ler personoplysninger, har gennemført den udbudte awareness-træning.

Bortskaffelse af udstyr

Databehandleren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

Logning

Databehandlerens systemer indeholder mulighed for adgang til log, som kan tilgås af dataansvarlig selv fra brugergrænsefladen. Derudover sikrer databehandleren følgende:

1. Sikrer logning på alle miljøer, hvor personoplysninger behandles
2. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder
3. Ændringer i systemrettigheder til brugere
4. Sikrer, at sikkerhedsloggens omfang er defineret ud fra en af Databehandleren udført risikovurdering
5. Sikrer, at der er plads nok til at sikkerhedsloggene kan gemmes for perioden
6. Sikrer, at der gennemføres løbende stikprøvekontroller, af, at sikkerhedsloggene indeholder det forventede

7. Afvejer løbende sikkerhedsloggens slettefrister imellem muligheden for at analysere cyberangreb, understøtte efterforskning og hensynet til beskyttelses af fysiske perso- ners rettigheder og frihedsrettigheder
8. Sikrer opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Registreredes rettigheder, jf. pkt. 9.1.

- Databehandleren skal bistå med at iagttage de registreredes rettigheder ved bl.a. at kunne give indsigt i, slette, begrænse og berigtige oplysninger samt sørge for at dette også sker hos underdatabehandlerne
- Databehandleren skal bistå med at opfylde de registreredes rettigheder uden unødig forsinkelse
- Databehandleren skal have udarbejdet en procedure for, hvordan de behandler anmodninger fra en registreret om deres rettigheder

Brud og hændelser, jf. pkt. 9.2.

Informationer som skal sendes:

- Fakta om det konstaterede brud (tid, sted, årsag)
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
- Kategorierne og det omtrentlige antal berørte registrerede hvis dette er muligt
- Kategorierne af personoplysninger hvis dette er muligt
- Navn og kontaktoplysninger til kontaktpunkt hvor yderligere oplysninger kan indhentes
- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet eller foreslået truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

C.4 Opbevaringsperiode/sletterutine

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 opbeva- res skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slette eller tilbageleveret, dette sker i forbindelse med ophør af Abonnementsaftalen.

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 de, som følger af nærværende databehandleraftale.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser, at foretage sådanne overførsler, medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere nævnt i bilag B. Overførselsgrundlag anvendes i henhold til Databeskyttelsesforordningens Kapitel V om over- førsler af personoplysninger til tredjelande eller internationale organisationer. De specifikke overførselsgrundlag følger af gældende bilag B.

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

Databehandleren skal inden for en periode af 12 måneder for egen regning indhente en ISAE 3000 revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret samt disse Bestemmelser.

Revisorerklæringen vil være tilgængelig for den dataansvarlige på databehandlerens hjemmeside.

Den dataansvarlige kan mod betaling anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæring 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 samt disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover – mod betaling – adgang til at foretage inspektioner herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt og efter passende forudgående vars- ling.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv.

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

Databehandleren skal årligt for egen regning indhente en revisorerklæring fra en uafhængig tredjepart eller en kontrolrapport vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstater- nes nationale ret.

Dokumentation for sådanne inspektioner fremsendes ved anmodning herom til den dataansvarlige til orientering.

Bilag D Parternes regulering af andre forhold

D.1 Ansvar og misligholdelse

En eventuel misligholdelse af Bestemmelserne reguleres og behandles i overensstemmelse med parternes aftale vedrørende levering af tjenesterne.

I tilfælde hvor databehandleren har udredt beløb til registrerede i overensstemmelse med Databeskyttelses Forordningens artikel 82 eller erstatningsansvarsloven § 26, har databehandleren fuld regres mod den dataansvarlige for det udredte beløb, som beløbsmæssigt overstiger den aftalte ansvarsbegrænsning i parternes aftale vedrørende levering af tjenesterne.

Parterne har hermed aftalemæssigt fraveget Databeskyttelsesforordningens artikel 82, stk. 5, og erstatningsansvarsloven § 26.

Uanset databeskyttelsesforordningen art 82, stk. 5 kan en part, der har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres efter princippet i art. 82, stk. 5.

I forhold til anden godtgørelse for ikke-økonomiske tab til de registrerede skal princippet i art. 82 ligeledes finde anvendelse, for så vidt angår den interne endelige ansvarsfordeling mellem databehandleren og den dataansvarlige.

Parterne kan ikke gøre regres eller erstatningskrav gældende overfor den anden part for bøder eller anden straf, der er pålagt i medfør af databeskyttelsesloven § 41 samt for bødeforelæg accepteret efter databeskyttelsesloven § 42.

D.2 Vederlag for bistand til den dataansvarlige

Alle aktiviteter beskrevet i afsnit 9 er ydelser, databehandleren er berettiget til særskilt betaling for, medmindre de pågældende aktiviteter skyldes, at databehandleren ikke har levet op til sine forpligtelser.