Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Den dataansvarlige

og

INNOMATE a/s
CVR 15882271
Ørestads Boulevard 73
2300 København K
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 personers 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. 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 INNOMATE HR 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 3 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren 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 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.

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

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.

   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.

7. 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 skriftlig underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelser eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelser mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandlere. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af databehandleaftalens 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. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for 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 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.

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 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. 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.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet 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 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. 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 hermed, 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 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 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.

e. den dataansvarliges forpligtelse til at dokumentere, at en påtænkt overførsel af personoplysninger til et 3.land, hvor overførselsgrundlaget beror på reglerne om fornødne garantier, jf. Databeskyttelsesforordningens art. 46 og 47, kan gennemføres på en måde, der sikrer de registrerede et niveau af privatlivsbeskyttelse, der svarer til det europæiske.

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.

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 få 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. Databehandleren skal, om muligt, senest 24 timer efter bruddet er konstateret, udarbejde og fremsende en foreløbig redegørelse om bruddet. Databehandleren skal seneste 48 timer efter bruddet er konstateret udarbejde en endelig underretning om bruddet til den dataansvarlige.

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.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette/tilbagelevere alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte overfor den dataansvarlige, at oplysningerne er slettet/tilbageleveret.

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger, f.eks. men ikke begrænset til:

    a. Bogføringslovens bestemmelser om opbevaringspligt i 5 år, at dokumentation for løn- og ansættelsesvilkår skal opbevares sammen med de basale personoplysninger i mindst 5 år fra udgangen af det regnskabsår, hvor medarbejderen er fratrådt.
    b. Opbevaring af jobansøgninger med legitimt formål i 6-12 måneder efter modtagelsen af ansøgningen (kundetilpasses)

    Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

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

13. Parternes aftale om andre forhold

- 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.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på ved underskrift eller anden accept 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. Hvis levering af tjenesterne 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.

5. Underskrift

   På vegne af den dataansvarlige

   Navn
   Stilling
   Telefonnummer
   E-mail
   Underskrift

   På vegne af databehandleren

Navn	Karsten Jørgensen
Stilling	Adm. direktør
Telefonnummer	+45 22808158
E-mail	kj@innomate.com
Underskrift	

Bilag A Oplysninger om behandlingen

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

At databehandleren stiller systemet INNOMATE HR, som ejes af databehandleren, til rådighed for den dataansvarlige så:

- den dataansvarlige gennem anvendelse af INNOMATE HR, som ejes af databehandleren, får adgang til en tidssvarende, brugervenlig og sikker digital platform til understøttelse af effektive arbejdsgange i relation til den dataansvarliges HR-arbejde, herunder rekruttering, on-boarding, administration, medarbejdersamtaler, kompetenceudvikling.
- den dataansvarlige kan anvende databehandlerens kapaciteter, herunder tekniske og fysiske kapaciteter, processer, kompetencer og erfaring med drift-, support- og vedligehold af applikationer og de hertil knyttede IT-miljøer til at sikre en stabil og sikkerhedsmæssig forsvarlig drift og forvaltning af INNOMATE HR, som er en kritisk forretningsapplikation for den dataansvarlige.

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

Databehandlerens behandling drejer sig primært om indlæsning, registrering, lagring, systematisering og bearbejdning af den dataansvarliges persondata samt at sikre at den dataansvarlige håndtering af dennes persondata sker i overensstemmelse med GDPR-forordning.

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

Databehandleren behandler følgende kategorier af personoplysninger om den dataansvarlige og dennes ansatte/slutbrugere:

Almindelige personlige oplysninger

- Navn, telefonnummer, adresse, mail, medarbejderfoto, stilling, CPR nr., nærmeste pårørende, Jobansøgning, CV, Ansættelseskontrakt, Lønoplysninger/trækprocent og skattefradrag, kurser/uddannelser, kompetencer, sygedage, tjenstlige forhold, aftaler og lignende.

Følsomme personoplysninger

- Fagforeningsmæssigt tilhørsforhold, helbredsoplysninger.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Medarbejdere som er eller har været ansat hos den dataansvarlige
- Personer som ansøger eller tidligere har ansøgt en stilling hos den dataansvarlige
- Andre personer, uden ansættelse, men som bistår den dataansvarlige.
- Den dataansvarlige – i forbindelse med administration og håndtering af økonomiske mellemværender samt kundepleje.

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

Varighed og ophør af abonnement
Der henvises til databehandlerens gældende abonnementsbetingelser.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Scannet	CVR: 29412006	Højvangen 4, 8660 Skanderborg	Hosting af databaser m.m.
Microsoft, Azure	IE8256796U	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Hosting af filer (herunder vedhæftede filer fra Rekruttering og medarbejderes filarkiv)
Jobnet	CVR: 34616939	Værkmestergade 5, 8000 Aarhus C	Jobopslag
KMD/Charlie Tango	CVR: 21029807	Rosenvængets Allé 11, 2100 København	E-boks
Lunaweb Ltd., Germany branch	UVAT ID: DE316913979	Nördliche Münchner Str. 14A, 82031 Grünwald, Tyskland	Konvertering af dokumenter til pdf-format.
Visma Addo	CVR: 29973334	Nørgaardsvej 32, 2800 Kongens Lyngby	Digital Signatur

Tilføjelse af nye Underdatabehandler er reguleret af pkt. 7 i Databehandleraftalen: 'Anvendelse af underdatabehandlere'.
En opdateret liste over underdatabehandlere er tilgængelig på siden https://www.innomate.com/index.php/da/support/GDPR

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 stiller den cloud-baserede HR-løsning 'INNOMATE HR' til rådighed for den dataansvarlige og herigennem opsamler, registrerer og organiserer personoplysninger om den dataansvarliges medarbejdere. Databehandlingen omfatter ligeledes ændringer og sletning af personoplysninger samt løbende transmission af personoplysningerne mellem den dataansvarlige, databehandleren og dennes underdatabehandlere.

Databehandling kan foregå automatiseret ved hjælp af programmerede workflows. Den dataansvarlige har adgang til at tilpasse og aktivere disse gennem de såkaldte Handlinger, hvortil dokumentation er fuld tilgængelig.

Databehandlerens løsninger er udviklet med åbent API, som gør det muligt at udveksle oplysninger på tværs af andre leverandørers løsninger. I det omfang den dataansvarlige vælger at installere og gøre brug af Tredjeparts-løsninger, der skal integrere med INNOMATE HR, anses det for at udgøre en instruktion til databehandleren om, at der kan ske overførsel mellem INNOMATE HR og tredjeparts løsningen.

Al adgang til kundens personoplysninger sker i henhold til kundens dokumenterede instruks. Den dokumenterede instruks udgøres dels af parternes aftalegrundlag, så de behandlinger der er nødvendige for at databehandleren kan opfylde indgåede aftaler med den dataansvarlige, kan udføres, og dels af de særskilte instrukser, som den dataansvarlige måtte give databehandleren. Databehandleren skal som nævnt i aftalens pkt. 4 efterleve den dataansvarliges dokumenterede instrukser. Denne aftale udgør en del af denne instruks.

Instruksen er generel i forhold udførelsen af de opgaver, der er aftalt med den enkelte kunde om levering og drift af INNOMATE HR, og omfatter således også almindeligt systemvedligehold, der skal sikre konsistens og driftssikkerhed.

Løsning af opgaver skal bestilles og/eller bekræftes af den dataansvarlige som hovedregel via databehandlerens servicesystem. Nye systemansvarlige ved kunden skal bemyndiges af aftaleansvarlig via servicesystemet.

Behandlingen af personoplysninger sker med de formål, og omfatter de kategorier af personoplysninger og registrerede, der er nævnt i bilag A.

Databehandleren må ikke behandle de af aftalen omfattede personoplysninger til egne formål, men alene til formål fastsat af den dataansvarlige.

Databehandleren skal i øvrigt medvirke til at sikre, at behandlingen sker i henhold til Databeskyttelsesforordningen og Databeskyttelsesloven.

Databehandleren skal som nævnt i aftales pkt. 4 efterleve den dataansvarliges dokumenterede instrukser. Denne aftale udgør en del af denne instruks.

.

C.2. Behandlingssikkerhed

Behandlingen omfatter en større mængede personoplysninger omfattet af Databeskyttelsesforordningen artikel 9 om 'særlige kategorier af personoplysninger, hvorfor der skal etableres 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 gennemfører som minimum følgende foranstaltninger, som er aftalt med den dataansvarlige:

Eksterne tekniske sikkerhedsforanstaltninger:

- Kryptering - al overførsel af fortrolige data udenfor databehandlerens netværk foregår på en måde, så det ikke er muligt for uvedkommende at få adgang til data. Ved krypteret forsendelse, sker overførsel via en secure ftp serveradgang, o.l. Specifikt er det ikke tilladt at sende eller modtage fortrolige data over ikke-krypteret mail. Protokollerne på forbindelserne opdateres løbende.
- Der anvendes https og sftp. Der opdateres løbende sftp og tjekkes løbende op på sikkerheden af protokollerne.
- Firewall på enheder der kan tilgå persondata samt til servere/driftscentre der lagrer persondata.
- Login til INNOMATE HR logges. Brugeren lukkes ude ved gentagne loginforsøg. Ved mange gentagne loginforsøg blokeres hele IP-adressen. Der gennemføres desuden manuelle tjeks af adgangslogs to gange årligt.
  Data opbevares fysisk sikret hos underdatabehandler.

Interne tekniske sikkerhedsforanstaltninger:

- Antivirus på alle enheder hvorfra der tilgås persondata.
- Opdatering af operativsystemer og applikationer.
- Løbende backup. Tjek af backups og restore af data.
- Brugernes adgang til data er begrænset af specifikke opsatte rettigheder.
- Logning: Der føres log over tilgang og behandling af personoplysningerne. Det er muligt at se, hvilke personer, som har haft adgang og den behandling, som den enkelte har foretaget.
- Adskillelse af produktions-, udviklings- og testmiljø.

Organisatoriske sikkerhedsforanstaltninger

- Alle medarbejdere er pålagt tavshedspligt og har underskrevet tavshedserklæring.
- Persondata er kun tilgængelige for de medarbejdere, som har godkendelse og arbejdsbetinget behov for at tilgå persondata og sker efter 'least privilege' princippet. Der foretages faste kvalitetstjek af oversigt over medarbejdere med adgang samt deres tildelte adgange.

- Opgave tjekliste ved til- og fratrædelse af databehandlerens medarbejdere sikrer de nødvendige sikkerhedsmæssige foranstaltninger ift. databehandlerens medarbejders tildeling og lukning af systemadgange.
- Adgang til kundedatabaser er kun muligt med personligt login med et komplekst password, som kun autoriseret personale er i besiddelse af og som skiftes hver 3. mdr.
- Ved levering af remote-/on-sitesupport begrænses adgangen til den dataansvarliges data mest muligt og det påses, at der anvendes færrest mulige af den dataansvarliges data. Data må kun midlertidigt være til stede på databehandlerens arbejdsstationer og skal fjernes umiddelbart efter behandling. Ved udbedring og fejlrettelse anvendes så vidt muligt kun dummy- og anonymiserede data. Der må ikke foretages fysiske udskrifter af fortrolige data.
- Alt udstyr der bruges til at tilgå persondata, låses automatisk efter højst 15 minutters inaktivitet og sikres med virusscanning.
- Vedtaget beredskabs- og responsplan ved mistanke om brud på persondatasikkerheden, der afprøves årligt.
- Der foretages test af systemændringer inden de idriftsættes.
- Der foretages med faste intervaller risikovurderinger.
- Løbende awareness aktiviteter for medarbejdere om datasikkerhed.

Fysiske sikkerhedsforanstaltninger

- Data opbevares fysisk sikret på databehandlerens servere hostet hos Scannet A/S samt på Microsoft Azure servere i Amsterdam (West Europe).
- Kontorer og bygninger aflåses, når de forlades.
- Fysisk sikkerhed: Når udstyr og mobile enheder ikke anvendes, skal udstyret og enhederne være låst og/eller låst inde.
- Backup opbevares ved Scannet og Microsoft Azure. Der foretages en løbende genindlæsningstest, således at det sikres, at backup'en virker og indeholder valide data.
- Alle fysiske medier destrueres på forsvarlig vis, hvis de har været benyttet til at opbevare persondata.

Driftsmæssige sikkerhedsforanstaltninger

- Personoplysninger sikkerhedskopieres automatisk. Kopierne opbevares adskilt og forsvarligt, således at personoplysningerne kan genskabes. Restore af data kan gennemføres til en given måned et år tilbage.
- Som dokumentation på, at kun autoriseret personale har adgang til persondata i INNOMATE HR og at adgang kun sker efter instruks fra dataansvarlige, foretages logning af al tilgang og behandling af personoplysninger. Logs, der indeholder persondata slettes efter højst følgende periode: Hvis loggen er relevant for at undersøge sikkerhedsbrud: 1 år. Alle andre tilfælde: 3 måneder.
- Systemovervågning med alarmering af oppetid for server samt systemfejl. Netværkstrafik overvåges ved underdatabehandlere. Der følges op på logning af tilgang til databaser.
- Der foretages sårbarhedsscanninger og penetrationstests.
- Der er er mulighed for at opsætte forskellige specifikke niveauer af adgange for brugere af INNOMATE HR.

Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden

Den øverste ledelse hos databehandleren er ansvarlig for behandlingssikkerheden og for at der til stadighed er etableret de nødvendige målsætninger, procedurer, systemer og politikker, herunder politik for privatlivsbeskyttelse og IT-sikkerhedspolitik, til understøttelse heraf. Ledelsen er repræsenteret i databehandlerens GDPR Gruppe og er driftsansvarlig for den løbende opdatering, kontrol og dokumentation til efterlevelse af behandlingssikkerheden. Arbejdet er organiseret og systematiseret omkring 'INNOMATE GDPR Årshjul' med månedlig kontrol, afprøvning og evaluering samt beslutning om specifikke indsatser til den fortløbende efterlevelse af databehandleraftalen.

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:

Databehandleren skal, mod databehandlerens til enhver tid gældende timetakst for sådant arbejde, bistå den dataansvarlige med opfyldelse af den dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder, herunder om indsigt, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af databehandleren.

Databehandleren skal endvidere stille oplysninger og nødvendig dokumentation til rådighed for den dataansvarlige, så denne kan føre tilsyn med databehandlerens overholdelse af kravene, herunder ved at give mulighed for- og bidrage til revision og audit.

I tilfælde af mistanke om brud på persondatasikkerheden igangsættes beredskab med beskrevne procedurer for håndtering herunder også evt. kommunikation med Datatilsynet. Disse evalueres årligt.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares hos databehandleren indtil den dataansvarlige anmoder om at få data slettet eller tilbageleveret medmindre andet er aftalt i 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 de som er angivet i bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren er berettiget til at anvende underdatabehandlere beliggende i tredjelande til opfyldelse af databehandlerens forpligtelser overfor den dataansvarlige.

Anvendelse af underdatabehandlere beliggende i tredjelande kan alene ske, hvis (i) overførslen er baseret på en afgørelse fra EU Kommissionen om tilstrækkelighed af beskyttelsesniveau, herunder f.eks. at det pågældende tredjeland mv. har et tilstrækkeligt beskyttelsesniveau, eller (ii) overførslen er omfattet af fornødne garantier, som f.eks. EU Kommissionens Standardkontraktsbestemmelser.

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.

INNOMATE overfører ikke personoplysninger til 3. lande. Grundet brug af underdatabehandleren Microsoft Azure Irland, der er et moderselskabs europæisk baseret datterselskab med modtagerland i EU og moderselskab i USA, er der udarbejdet nedenstående Transfer Impact Assesment (TIA). Denne TIA er udelukkende udarbejdet for at sikre den højest mulige grad af tillid i overholdelse af de intereuropæiske overførsler mellem parterne.

Virksomhed	Modtager-land	Moder-selskab	Oplysninger	Overførsels-grundlag	Supplerende
Microsoft, Azure	Irland	USA	Hosting af filer, herunder vedhæftede filer fra Rekruttering og medarbejderes filarkiv.	SCC	Transfer Impact Assessment (TIA) Se særligt afsnit 1.4.

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

Databehandleren indhenter én gang årligt en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen er tilgængelig på databehandlerens hjemmeside, Revision af Databehandleraftale. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan for egen regning og risiko anmode om en ny revisorerklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisorerklæringen, 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 fysisk inspektion, med 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 behov herfor og kræver forudgående aftale, så databehandleren er forberedt på at afsætte de nødvendige ressourcer.

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

Databehandleren fører tilsyn vedrørende overholdelsen af denne databehandleraftale hos underdatabehandleren. Dette foregår igennem indhentning af relevant dokumentation, erklæringer eller lignende.

Ud over det planlagte tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.