

Standardkontraktbestemmelser

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

mellem

Kunden

som angivet i aftalen vedr. nærværende rådgivningsopgave (Opgaveaftalen).

herefter "den dataansvarlige"

og

Human House A/S

CVR 61896813

Dynamovej 11

2860 Søborg

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingsikkerhed	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger.....	8
12. Revision, herunder inspektion	8
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør.....	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	9
Bilag A Oplysninger om behandlingen	10
Bilag B Underdatabehandlere	11
Bilag C Instruks vedrørende behandling af personoplysninger.....	12
Bilag D Parternes regulering af andre forhold.....	15

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 rådgivningsydelse, indsamles personoplysninger fra de Registrerede, og disse behandles af databehandleren 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 er 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.

2. 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.

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

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.

3. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. 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.
3. Er den dataansvarliges instruks i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, er parterne forpligtet til i fællesskab at finde en lovlig løsning. Hvis parterne ikke kan finde en løsning uden, at den er unødvendig byrdefuld for databehandleren, har hver part mulighed for at opsige databehandleraftalen med 1 måneds varsel.

4. 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.

5. 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.

6. 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 specifik skriftlig godkendelse fra den dataansvarlige.
3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 3 mdr. varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B. Ved ophør af brugen af

en underdatabehandler skal databehandleren give den dataansvarlige skriftlig meddelelse herom.

Side 6 af 15

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.

7. 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 standardkontraktbestemmelser 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.

8. Bistand til den dataansvarlige

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

9. 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.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, skal databehandleren slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige, og skal ved den dataansvarliges anmodning bekræfte at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. 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. Procedurene 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.

12. 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.

13. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på ikrafttrædelsesdatoen for Opgaveaftalen.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder 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 skriftlig varsel af begge parter.

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via Opgaveaftalens kontaktpersoner/ opgaveansvarlige.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner/ opgaveansvarlige.

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

Databehandlingen har til formål at indsamle personoplysninger fra de Registrerede med henblik på at yde rådgivning med feedback ved deling af resultater med den dataansvarlige. *[Deling kun relevant hvis aftalt i Opgaveaftalen]*

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

Behandlingen består af:

1. Modtagelse af kontaktinformation på de Registrerede
2. Indsamling af personoplysninger fra de Registrerede
3. Rådgivning med feedback på baggrund af indsamlede personoplysninger *[Kun relevant hvis aftalt i Opgaveaftalen]*
4. Deling af resultater med den dataansvarlige. *[Kun relevant hvis aftalt i Opgaveaftalen]*

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

Der behandles følgende almindelige personoplysninger jf. databeskyttelsesforordningens art. 6 om de Registreredes:

- E-mailadresse
- Telefonnummer
- Navn
- Afdeling
- Stilling/titel

[Som aftalt i Opgaveaftalen]

Følgende personoplysninger jf. databeskyttelsesforordningens art. 9 kan behandles:

- Helbredsoplysninger
- Seksuelle forhold

[Som aftalt i Opgaveaftalen]

Personoplysninger jf. databeskyttelsesforordningens art. 9 behandles alene på den Registreredes eget initiativ, hvis den Registrerede oplyser herom under rådgivning.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Medarbejdere ansat hos den dataansvarlige, samt evt. arbejdsgiver, andre medarbejdere og andre Registrerede, hvis aftalt i Opgaveaftalen (samlet, de Registrerede).

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

Kontaktoplysninger indeholdende personoplysninger delt af den dataansvarlige samt personoplysninger indsamlet af databehandleren slettes senest 6 mdr. efter afslutning af opgaveaftale.

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft EU Ireland Operations Ltd	IE256796	South County Business Park, Leopardstown, Dublin 18, D18 DH6k	Microsoft 365 dataopbevaring.
NHL Data ApS	25575555	Gammel Køge Landevej 55, 2500 Valby, Danmark	IT-drift og support herunder backup og restore.

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

C.1. Behandlingens genstand/instruks

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

Den dataansvarlige giver databehandleren instruks til at kontakte og indsamle personoplysninger fra de Registrerede med henblik på at yde rådgivning. Herunder instrueres databehandleren til at dele resultater med den dataansvarlige. *[Deling kun relevant hvis aftalt i Opgaveaftalen]*

C.2. Behandlingssikkerhed

Det høje sikkerhedsniveau afspejler, at behandlingen i særlige tilfælde omfatter følsomme personoplysninger omfattet af forordningens artikel 9 samt fortrolige oplysninger.

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:

- Personoplysninger opbevares hos de under punkt B.1 nævnte underdatabehandlere og slettes senest 6 mdr. efter afslutning af opgaveaftale. De konkrete tekniske og organisatoriske foranstaltninger er dokumenteret i underdatabehandlerens årlige ISAE-3000 erklæring for gennemførte IT-kontroller.
- Det aftalte sikkerhedsniveau er etableret med nødvendig fysisk, logisk sikkerhed, herunder sikring af adgangsforhold, brugerkonti og databeskyttelse.
- Alle medarbejdere hos databehandleren er underlagt en generel tavshedspligt indeholdt i deres ansættelseskontrakt, ligesom forskellige faggrupper som sygeplejersker, læger og psykologer derudover er underlagt yderligere lovgivning om tavshedspligt.

Databehandleren kontrollerer og vurderer tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed hos underdatabehandler regelmæssigt.

Databehandlerens ansatte har modtaget instruktion om korrekt og sikker håndtering af personoplysningerne.

Databehandleren anvender underdatabehandlere, der er certificeret efter ISO 27001 suppleret med ISAE baserede revisorerklæringer. Databehandleren har outsourcet alle tekniske services til certificerede og kontrollerede underdatabehandlere, som har den fornødne erfaring og de fornødne garantier til at bistå med business continuity aktiviteter og de medfølgende foranstaltninger.

Databehandleren er under opbygning af et tilsvarende højt niveau efter et ISO 27001 baseret Statement of Applicability, der skal sikre modning af alle behandlingssystemer og -tjenester.

Personalehåndbog og awareness kampagner skaber grundlaget for at alle databehandlerens medarbejdere er bevidste om deres pligter ift. databeskyttelse.

Generelt, anvender databehandleren MFA og VPN samt Bitlocker-beskyttede enheder og brugerkonti. Alle aktiviteter omkring livscyklus for dokumenter, emails og persondatabærende systemer logges.

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 efter nærmere aftale med den dataansvarlige, så vidt muligt, bistå den dataansvarlige med at sikre overholdelse af aftalens forpligtelser, herunder i forordningens artikel 32 (gennemførelse af passende tekniske og organisatoriske foranstaltninger), 35 (foretagelse af konsekvensanalyse vedrørende databeskyttelse) og 36 (forudgående høring).

Den dataansvarliges udgifter i forbindelse med revisioner, inspektioner o.lign., afholdes af den dataansvarlige selv. Databehandleren er berettiget til at fakturere den dataansvarlige for nødvendige udgifter og medgået tid, herunder omkostninger til underdatabehandlere og tredjeparts assistance ifm. revisioner, inspektioner o.lign., som måtte følge af enhver anmodning, instruks eller bistand i medfør af denne aftale, ligesom den dataansvarlige vil blive faktureret for eventuelle betalinger til underdatabehandlere og for anden tredjeparts assistance.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger tilbageleveres ikke til den dataansvarlige, men slettes af databehandleren efter ophør af tjenesterne eller senest 6 mdr. efter afslutning af opgaveaftale.

C.5 Lokalt for behandling

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

Personoplysninger opbevares i datacenter hos Microsoft med adresse: South County Business Park, Leopardstown, Dublin 18, D18 DH6k i Irland, samt NHL Data ApS med adresse: Gammel Køge Landevej 55, 2500 Valby i Danmark.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den behandling af persondata, som Databehandleren foretager efter aftale med den Dataansvarlige, må alene foretages af Databehandleren eller underdatabehandlere, indenfor EU/EØS-grænser.

Databehandleren er ikke berettiget til at lade databehandling foregå udenfor EU/EØS-grænser uden den Dataansvarliges skriftlige samtykke.

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.

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

Den dataansvarlige eller en repræsentant for den dataansvarlige har adgang til at foretage inspektioner, herunder fysiske inspektioner, af de lokaliteter og systemer, hvorfra databehandleren foretager behandling af personoplysninger. Inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt, så længe tjenesterne vedrørende behandling af personoplysninger ikke er ophørt jf. Bestemmelse 14.4 f.eks. ved sletning jf. Bilag A.5, og databehandleren kan ikke afvise eller begrænse den dataansvarliges ret hertil. Inspektioner skal dog gennemføres efter forudgående anmodning efter rimelig frist, således at databehandleren kan tilrettelægge adgang og afsætte de nødvendige ressourcer til gennemførelse af inspektionen.

Databehandleren stiller på anmodning den dokumentation til rådighed, som er nødvendig for, at den dataansvarlige kan vurdere databehandlerens overholdelse af databeskyttelsesforordningen og disse Bestemmelser, herunder interne politikker, procedurer, relevante kontroller og samt eventuelle erklæringer jf. punkt C.8.

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

Databehandleren fører årligt tilsyn med underdatabehandlere ved indhentning af underdatabehandlerens seneste revisionserklæring vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Den dataansvarlige kan til enhver tid anmode databehandleren om at få en kopi af underdatabehandlerens seneste revisionserklæring.

Databehandleren eller en repræsentant for Databehandleren kan anmode om adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra Underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen.

I tilfælde af at sådan inspektion gennemføres kan dokumentation af resultaterne heraf fremsendes herfor til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode mod betaling af udgifter og medgået tid.

Bilag D Parternes regulering af andre forhold

Der er ikke aftalt regulering af andre forhold mellem parterne, end som angivet i Opgaveaftalen.