



Databehandlersaftale

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

mellem

Kunden

herefter "den dataansvarlige"

og

GAIS A/S

CVR 44574780

Klokhøjen 4

8200 Aarhus N

Danmark

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



1. 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 GAIS-plattformen iht. en aftale herom (**fremover 'hovedaftalen'**) 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, herunder de almindelige betingelser og vilkår for brug af GAIS-plattformen.
5. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.
6. Der hører tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
7. 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.
8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af ved indgåelse af nærværende aftale.
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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør hverken den dataansvarlige eller databehandleren fra forpligtelser, som parterne 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 Henvisninger 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 behandlingen er påkrævet 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 anses som i strid med databeskyttelsesforeningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

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. Behandlingsikkerhed

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 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 14 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
2. 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.

3. 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.

4. 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.
5. I tilfælde af databehandlerens konkurs, kan den dataansvarlige indtræde i databehandlernes rettigheder over for underdatabehandlere, således den dataansvarlige kan instruere underdatabehandlere i sletning eller tilbagelevering af personoplysningerne.

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

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. indsigtretten
- 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
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 5.3., 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 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 8.1. og 8.2.

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 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 8.2.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.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af virksomhedsoplysninger, er databehandleren forpligtet til at slette alle oplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne, eller andet er aftalt i Bilag C.
2. Personoplysninger afgivet af den dataansvarliges ansatte slettes ikke ved ophør af tjenester omfattet af hovedaftalen, såfremt disse har afgivet selvstændigt samtykke til behandlingen og den fortsatte opbevaring, medmindre andet aftales i Bilag C.

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 er nærmere angivet i Bilag C.7.
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. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for indgåelse af hovedaftalen.
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 i overensstemmelse med Bestemmelse 10.1 og Bilag C.4 anses Bestemmelserne som ophørt, medmindre andet følger af Bilag A.5.



13. 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.

Navn	Henrik Steuer Carlsen
Stilling	Head of Operations, GAIS
Telefonnummer	4140 6371
E-mail	henrik@gais.dk



Bilag A Oplysninger om behandlingen

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

At den dataansvarlige kan anvende GAIS-plattformen som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om egne medarbejdere, eventuelle frivillige og administratorer, med henblik på at gennemføre medarbejderundersøgelser og viderebehandle de indsamlede oplysninger .

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

At databehandleren stiller GAIS-plattformen til rådighed for den dataansvarlige og herigennem opbevarer, bearbejder og behandler personoplysninger om deltagere i GAIS-målinger hos den dataansvarlige.

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

Behandlingen omfatter altid som minimum registreredes navn, e-mail, alder, stilling, ansættelsesland, og køn.

Den dataansvarlige kan vælge at anvende GAIS-plattformen til behandling af andre oplysninger, såvel som de registrerede kan indgive fritekstkommentarer, der kan indeholde yderligere oplysninger, af både særlig og fortrolig karakter. Disse oplysninger er omfattet af behandlingen.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Ansatte, frivillige, kontaktpersoner og andre personer hos den dataansvarlige, hvis oplysninger, den dataansvarlige overgiver til behandling hos databehandleren.

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

Behandlingen er ikke tidsbegrænset og løber så længe, der eksisterer et aftalegrundlag mellem parterne, der fordrer, at databehandleren udfører databehandling på vegne af den dataansvarlige.

Den dataansvarlige kan til enhver tid og iht. betingelserne for opsigelse af datagrundlaget for databehandlingen herunder instruksen i bilag C, opsiges databehandlingen og bede databehandlerne slette den behandlede persondata.



Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

NAVN	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Irland	Leverer IT-systemer til databehandleren, der anvendes til følgende databehandlinger: <ul style="list-style-type: none"> • Hosting og behandling af personoplysninger på GAIS-plattformen via Azure • Udveksling af personoplysninger pr. mail igennem Outlook • Evt. databehandling i Office-programmer (excel/word) <p>AI databehandling foregår i EU. Underdatabehandleren er dog ejet af en amerikansk koncern, hvorfor dataoverførsler til USA jf. Schrems II kan ske utilsigtet. Af denne årsag har underdatabehandleren tiltrådt EU-U.S. Data Privacy Framework, og der er i aftalen implementeret yderligere foranstaltninger.</p>
MongoDB Limited	Building Two, Number One Ballsbridge Shelbourne Road, Ballsbridge Dublin, D04 Y3x9, Irland	Leverer databasesystem og hosting af GAIS-plattformens database via. Azure-servere. AI databehandling foregår i EU. Underdatabehandleren er dog ejet af en amerikansk koncern, hvorfor dataoverførsler til USA jf. Schrems II kan ske utilsigtet. Af denne årsag har underdatabehandleren tiltrådt EU-U.S. Data Privacy Framework, og der er i aftalen implementeret yderligere foranstaltninger.
SendInBlue	106 boulevard Hausmann, 75008 Paris, Frankrig	Leverer mailløsning til udsendelse af alle mails fra GAIS-plattformen, herunder invitationer til målinger, links til rapporter, mv. AI databehandling foregår i EU.
Pipedrive OÜ	Mustamäe tee 3a, 10615 Tallinn, Estland	Leverer CRM-system til GAIS, hvori kundedata kan blive behandlet. Dette omfatter alene oplysninger på kontaktpersoner hos kunden. AI databehandling foregår i EU. Underdatabehandleren er dog ejet af en amerikansk koncern, hvorfor dataoverførsler til USA jf. Schrems II kan ske utilsigtet. Af denne årsag har underdatabehandleren tiltrådt EU-U.S. Data Privacy Framework, og der er i aftalen implementeret yderligere foranstaltninger.
Freshworks Inc.	San Mateo, 2950 S Delaware St Suite 201, USA	Leverer supportsystem til GAIS, hvori persondata vil kunne blive behandlet i forbindelse med supportsager.



	AI databehandling foregår i EU og USA. Underdatabehandleren har tiltrådt EU-U.S. Data Privacy Framework, og der er i aftalen implementeret yderligere foranstaltninger.
--	--

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke varsling iht. afsnit 6 gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.



Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

Databehandler stiller GAIS-plattformen til rådighed, hvori følgende data behandles: navn, e-mail, alder, stilling, ansættelsesland, køn og evt. andre oplysninger for den dataansvarlige. Hertil kommer oplysninger om virksomhed og virksomhedsmålinger hvori ovennævnte besvarelser indgår.

Databehandleren indsamler herefter oplysninger fra de registrerede i form af de registreredes udfyldelse af digitale spørgeskemaer. De indsamlede oplysninger udstilles for den dataansvarlige i anonymiseret form i rapporter og grafikker, hvor datatyper kan korreleres.

Databehandleren skal i forbindelse med behandlingen lave en anonymiseret kopi af GAIS-besvarelserne, ved GAIS-besvarelsernes afslutning, hvorefter databehandleren vederlagsfrit kan benytte de anonymiserede data til egne formål.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle at der som udgangspunkt ikke er tale om behandling af personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger". Sikkerhedsniveauet skal dog også afspejle, at de registrerede i egen kraft, kan tilføje oplysninger, der kan være omfattet af artikel 9, samt at flere oplysninger kan anses som fortrolige.

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

Databehandleren skal dog - i alle tilfælde og som minimum - gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige (på baggrund af den risikovurdering den dataansvarlige har foretaget):

- Al behandlet data er krypteret både ved udveksling, i transit og 'at rest'
- Der er etableret flere niveauer af backup, der sikrer at data kan genskabes op til 12 mdr. efter sletning
- Ved brugersletning skal brugers GAIS-besvarelser fuldt ud anonymiseres, samt at det skal sikres, at der ved reetablering af backup ikke genoprettelse af oplysningerne
- Tilgængelighed og reaktionstider indenfor 24 timer i hverdage
- Data skal tilgås SSL krypteret og kun tilladt via af databehandler godkendte IP-adresser
- Al administrativ adgang til databasen skal logges med login, tidspunkt og IP-adresse

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 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- Sletning af personoplysninger på dataansvarliges eller registreredes anmodning
- Mulighed for udtræk af registreredes oplysninger på dataansvarliges eller registreredes anmodning
- Nødvendige oplysninger til den dataansvarlige og registrerede for at overholde oplysningspligten

C.4 Opbevaringsperiode/sletterutine



Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret, eller hovedaftalen ophører, jf. Bilag A.5.

C.5 Lokaltet for behandling

Behandling sker som udgangspunkt på flere lokationer i Danmark og på underdatabehandleres lokationer i Europa. Behandling af de i aftalen omfattede personoplysninger kan ske på disse lokationer, såvel som øvrige lokationer under forudsætning af at data tilgås SSL krypteret og kun via en af databehandler godkendt IP-adresse.

C.6 Databehandling i tredjelande

Medmindre andet er aftalt mellem parterne i Bilag B, må databehandling ikke ske i tredjelande.

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 kan føre tilsyn med databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

Tilsyn føres som udgangspunkt skriftligt, og databehandleren deltager i tilsynet uden beregning, medmindre omfang eller frekvens ikke er proportionelt med databehandlingen.

Alle eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den medarbejdertid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.

C.8 Procedurer for databehandlerens revision, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til underdatabehandlere

Databehandleren eller en repræsentant for denne fører underdatabehandlere som udgangspunkt årligt tilsyn med underdatabehandlere.

Format afhænger af en konkret vurdering af den enkelte underdatabehandler, på baggrund af behandlingens karakter og omfang. Yderligere tilsyn kan finde sted, hvis der efter databehandlerens vurdering opstår et behov herfor.

