Dansk Psykologisk Forlag
Knabrostræde 3, 1. sal
1210 København K

CVR 33255705
www.dpf.dk

Databehandleraftale

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

mellem

Kunden, jf. hovedaftalen mellem Parterne (herefter "Hovedaftalen")

herefter "den dataansvarlige"

og

Dansk Psykologisk Forlag A/S
Knabrostræde 3, 1. sal
1210 København K
CVR-nummer 33255705

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.

Bestemmelserne udgør Datatilsynets standardkontraktbestemmelser (sort skrift) med de tilpasninger, som fremgår med blå skrift og som er begrundet i skemaet på side 21-22. I skemaet fremgår den oprindelige bestemmelse tillige. Samme systematik (sort/blå skrift) følger i bilagene til Bestemmelserne, dog uden begrundelser for de tilpasninger, der er udarbejdet i bilagene.

Dansk Psykologisk Forlag A/S, 25. november 2021

Dansk Psykologisk Forlag

Indhold

Dansk Psykologisk Forlag

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 databehandlerens services, jf. nærmere i Hovedaftalen og Bilag A, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

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

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

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

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder databehandlerens faste takst for bistand til den dataansvarlige.

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 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.

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.

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,

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

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 generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med det varsel, der fremgår af bilag B.1 og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

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

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. SLETTET.

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.

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 standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

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 unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden 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.

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.

4. For sin bistand i medfør af nærværende punkt 9, er databehandleren berettiget til at modtage et rimeligt honorar. De til enhver tid gældende takster følger af Bilag D.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a) karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b) de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c) de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. 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.

5. For sin bistand udover tilvejebringelsen af den aftalte information i medfør af nærværende punkt 10, er databehandleren berettiget til at modtage et rimeligt honorar, medmindre sikkerhedsbruddet skyldes forhold, der kan tillægges data-behandleren som groft uagtsomt. De til enhver tid gældende takster følger af Bilag D.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige inden 3 måneder efter Hovedaftalens ophør og bekræfte over for den dataansvarlig, at oplysningerne er slettet, eller tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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

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. 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.

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 datoen for begge parters underskrift 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 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

   Aftalen underskrives eller accepteres elektronisk af den dataansvarlige og træder i kraft herefter.

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via de i Hovedaftalen specificerede kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Dansk
Psykologisk
Forlag

Bilag A

Oplysninger om behandlingen

Der henvises til det/de relevante beskrivelser, der fremgår af dokumentet Bilag A.1-A.12.

Her er databehandlerens produkter beskrevet med hver deres særskilte Bilag A i medfør af Datatilsynets model for nærværende bilag.

Beskrivelserne i Bilag A.1-A.12 indgår automatisk i Bestemmelserne, når den dataansvarlige, via Hovedaftalen, har tilvalgt et eller flere af produkterne.

Dansk Psykologisk Forlag

Bilag B

Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

Underdatabehandler	Service	Aftale	Serverland og evt. overførselsgrundlag
1stLevel ApS CVR-nr. 32148891 Baldershøj 17B 2635 Ishøj	Hosting og support	På anmodning.	Danmark
Ashfield Nordic ApS CVR-nr. 25784723 Rådhuspladsen 16 1550 København K	Support	På anmodning.	Danmark
Anahoret SL at Calle Clara Campoamor, 12, BW 28, Alacant / Alicante, 03540, Spanien	Support	På anmodning	Spanien og Ukraine, jf. GDPR, artikel 46(2)(c) og indgåelse af aftale om sikkerhedsforskrifter ved overførsel til Ukraine under anvendelse af supplerende foranstaltninger, som anført af EU-Kommissionen i: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

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.

B.2. Varsel for godkendelse af underdatabehandlere

2 måneder.

Dansk Psykologisk Forlag

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:

Databehandleren stiller en SaaS (Software as a Service) til rådighed. Det betyder, at databehandleren leverer et digitalt produkt på en licens med indbygget hosting.

De nærmere omstændigheder fremgår af Bilag A.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter personoplysninger omfattet af databeskyttelsesforordningens artikel 6 (almindelige personoplysninger).

Det er ikke formålet med Hovedaftalen, at databehandleren skal behandle personoplysninger omfattet af databeskyttelsesforordningens artikel 9 (særlige kategorier af oplysninger). Den dataansvarliges anvendelse af databehandlerens produkter kan imidlertid medføre, at de hostede oplysninger lægger sig tæt op ad diagnoser på fx ADHD eller autisme. Det vil afhænge af produktvalget (jf. Bilag A for nærmere beskrivelse), omstændighederne for den dataansvarliges årsag til anvendelsen af testen, samt resultaterne af de tests, som den dataansvarlige gennemfører. Til brug for fastlæggelse af sikkerhedsforanstaltningerne betragtes denne del af behandlingen som behandling af oplysninger om "andre beskyttelsesværdige personoplysninger", jf. Datatilsynets kategorisering i "*Vejledning om tilsyn med databehandlere, Pointskala og seks tilsynskoncepter, oktober 2021*". Disse oplysninger behandles sikkerhedsmæssigt på samme måde, som hvis der var tale om "særlige kategorier af personoplysninger" i direkte forstand.

Databehandleren skal ikke behandle oplysninger om strafbare handlinger eller undladelser efter databeskyttelsesforordningens artikel 10.

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.

En beskrivelse af sikkerhedstiltag er tilgængelig som **Bilag C.2**.

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:

Dansk Psykologisk Forlag

Sende hændelseslog over konstaterede sikkerhedsbrud hos databehandleren samt bistå efter nærmere aftale i tilfælde af sikkerhedsbrud.

C.4 Opbevaringsperiode/sletterutine

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og 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 følgende:

Databehandlerens hjemsted, samt lokaliteterne hos underdatabehandlerne, fremgår af Bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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.

De i Bilag B angivne tredjelandsoverførsler betragtes som en godkendt instruks i forbindelse med indgåelsen af Hovedaftalen og Bestemmelserne.

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

Med henvisning til Datatilsynets *"Vejledning om tilsyn med databehandlere, Pointskala og seks tilsynskoncepter, oktober 2021"*, følger Databehandleren som udgangspunkt tilsynskoncept 3 og 5. Koncepterne kan anvendes i kombination.

Koncept 3:

Databehandleren skal årligt – enten direkte eller via sin hjemmeside – give en skriftlig status på forhold, der er omfattet af Bestemmelserne, og andre relevante områder (f.eks. organisatoriske eller produktmæssige ændringer).

Koncept 5:

Databehandleren skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af erklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- Advokaterklæring
- ISAE 3000 revisionserklæring
- ISAE 3402 revisionserklæring
- ISO 27001 revisionserklæring

Revisionserklæringen gøres tilgængelig for den dataansvarlige på anmodning. Databehandleren er altid berettiget til at fremvise en erklæring, der ikke er dateret mere end 12 måneder tilbage.

Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode. I så fald indhentes erklæringen på den dataansvarliges regning.

Baseret på resultaterne af erklæringen, 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. Databehandleren er berettiget til at modtage et rimeligt honorar for implementeringen af yderligere foranstaltninger, som den dataansvarlige specifikt har bedt om.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, 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 det nødvendigt. Den dataansvarliges og databehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den data-ansvarlige 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.

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

Databehandleren er ansvarlig for at indhente revisionserklæringer mv. fra underdatabehandlere efter samme principper som beskrevet i punkt C.7. Databehandleren vurderer hvilket koncept der vil være hensigtsmæssigt at anvende ved revisionen. Revisionsmaterialet fremsendes til den dataansvarlige på anmodning.

Dansk
Psykologisk
Forlag

Bilag C.2

Behandlingssikkerhed, beskrivelse

Teknisk sikkerhed	Beskrivelse
Antivirus	Alle enheder i DPF, samt eksterne konsulenters enheder er forsynet med antivirus. Enhederne bliver automatisk opdateret og vedligeholdt.
Firewall	Enhver adgang er sikret igennem en firewall, som løbende bliver vedligeholdt. Administrativ adgang er begrænset til bestemte IP-adresser for de enkelte brugere. Alle medarbejdernes daglige arbejde foregår via VPN.
Netværkssegmentering	Alle netværk er segmenteret. Segmenteringen sker således både i forbindelse med hosting-netværket for databasen med tests mv., og i forbindelse med databehandlerens kontornetværk.
Brugeradgang	Alle systemer er opdelt på brugerniveau. Der er tilknyttet adgangsbegrænsninger på de forskellige brugerniveauer.
Systemovervågning	Der er overvågning på alle systemer, hvor der behandles personoplysninger. Der foretages logning af alle aktiviteter i Microsoft Office365 i en periode på 180 dage.
Kryptering ved transmission via web og mail	Alle brugere har adgang til kryptering, når de sender personoplysninger ud af systemet. Alt mailtransmission sker igennem Microsoft Office365. Transmission sker som minimum med sikkerhedsprotokol TLS 1.2-kryptering. Sendes der personoplysninger, som efter en konkret vurdering kræver yderligere sikkerhedsforanstaltninger, sker dette med IRM-beskyttet mail.
Logning	Der foretages logning af alle aktiviteter i Microsoft Office365 i en periode på 180 dage.
Logbeskyttelse	Alle Microsoft-systemer kører efter den nyeste standard, og de er beskyttet mod manipulation og tekniske fejl i deres logs. Loggen bliver løbende gennemgået.

Testmiljø	Alt data der benyttes i eventuelle testmiljøer, er fuldt anonymiseret og vil ikke udgøre personoplysninger tilhørende den datansvarlige. Implementeringen af evt. udviklingsmoduler sker direkte på produktionsserveren hos databehandleren.
Sårbarhedstest	Der er installeret firewalls, som løbende bliver opdateret til den nyeste version for at lukke for sårbarheder. Overvågning af sårbarhed er indbygget i databehandlerens software. Switche bliver opdateret sammen med firewalls og indgår i denne overvågning. Hostingleverandøren foretager løbende test.
Opdateringer, patches, mv.	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.
Forretningsgang for brugeradgang	Alle brugeradgange tildeles ud fra et arbejdsbetinget behov. Dette er en fast procedure ved on- og off-boarding af medarbejdere og underleverandører og opdelt i henhold til den opgave, som den enkelte bruger skal varetage.
To-faktor-adgang	Der er implementeret to-faktor-adgang på alle de systemer hvor der behandles personoplysninger.

Fysisk sikkerhed	**Beskrivelse**
Adgangsforhold	Selve tilgangen til kontoret sker i almindelig arbejdstid via en port som er åben, porten lukkes og låses om natten. Efter porten skal man igennem en låst dør ind til en opgang, hvor der ligeledes ligger andre firmaer. Denne dør kan enten åbnes via nøgle eller med en nøglebrik. Der er bemandet reception i åbningstiden. Udenfor forlagets åbningstid er døren låst med to låse. Medarbejderne har nøgler til alle døre, og hvis alle indgange er låst, kræves det 1 nøgle at få adgang til forlaget. Endvidere er kontoret udstyret med en alarm, med videoovervågning, sættes alarmen i gang sendes der direkte besked til alarmselskabet, og de kan tænde

	kameraet og se hvem der er på kontoret, de kontakter og den ansvarlige hos forlaget. Udover medarbejdere hos databehandleren, har et rengøringsfirma adgang til kontoret uden for åbningstiden. Alle medarbejdere er instrueret i at fortrolige og følsomme personoplysninger skal opbevares utilgængeligt for uvedkommende, som ikke skal have adgang til personoplysningerne.

Organisatorisk sikkerhed	**Beskrivelse**
Informationssikkerhedspolitik	DPF har udarbejdet en IT-sikkerhedspolitik. Denne er videregivet til medarbejder gennem oplæring, dagligvirke og ved udlevering af et dokument til medarbejder, med beskrivelse af hvordan de skal behandle data.
Medarbejdertillid	Der er en generel procedure for efterprøvning af medarbejdere i forbindelse med ansættelse.
Fortrolighed	Alle databehandlerens medarbejdere er dækket af en tavshedspligts- og fortrolighedserklæring. Det samme gælder hos underleverandører.
Fratrædelsesprocedurer	Fratræder en medarbejder, sikres det, at data overleveres til anden medarbejder, som har autoritet til at kunne overtage dem i overgangsfasen. Medarbejderen adgang til terminalserven lukkes straks efter medarbejderen fratræder, dette sker i samarbejde med alle relevante aktører.
Awareness-træning	Alle medarbejdere hos databehandleren har fået udtrykkelig instruks angående opbevaring, behandling, sletning og sikkerhed vedrørende behandling af personoplysninger. Instruksen opdateres løbende, senest i juli 2021. Der afholdes endvidere et seminar hvert halve år om relevante databeskyttelsesretlige aspekter.

Dansk
Psykologisk
Forlag

Bilag D

Parternes regulering af andre forhold

Databehandlerens standardtakst for de særlige ydelser, der følger af Bestemmelsernes punkt 8.4 og 10.5, er dkr. 1.500 / timen.

Dansk Psykologisk Forlag

Bilag E

Begrundelser for afvigelser til Bestemmelserne

Oprindelig bestemmelse	Ny bestemmelse	Begrundelse for ændring
2.9 Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.	2.9 Bilag D indeholder databehandlerens faste takst for bistand til den dataansvarlige.	Tidsforbrug forbundet med GDPR-opgaver på Kundens vegne er ikke en del af Dansk Psykologisk Forlags licenspriser.
6.6 Databehandleren skal i sin aftale med underdata-behandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehand-lerens konkurs, således at den dataansvarlige kan indtræde i databehand-lerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den data-ansvarlige i stand til at instruere underdatabe-handleren i at slette eller tilbagelevere personoplysningerne.	Bestemmelsen udgår.	Bestemmelsen er ikke obligatorisk ifølge GDPR, artikel 28 og i kæden af underleverandører, er det ikke altid muligt at indføje et sådant vilkår. I tilfælde af en konkurs hos en underdatabehandler, vil Dansk Psykologisk Forlag naturligvis sørge for at varetage de interesser, der gør sig gældende for både Dansk Psykologisk Forlag og Kunden.
Ingen	9.4 For sin bistand i medfør af nærværende punkt 9, er databehandleren berettiget til at modtage et rimeligt honorar. De til enhver tid gældende takster følger af Bilag D.	Tidsforbrug forbundet med GDPR-opgaver på Kundens vegne er ikke en del af Dansk Psykologisk Forlags abonnementspriser, idet omfanget er ukendt.
Ingen	10.5 For sin bistand udover tilvejebringelsen af den aftalte information i medfør af nærværende punkt 10, er databehandleren berettiget til at modtage et rimeligt honorar, medmindre sikkerhedsbruddet skyldes forhold, der kan tillægges databehandleren som groft uagtsomt. De til enhver tid gældende takster følger af Bilag D.	Hvis Kunden stiller særlige krav eller spørgsmål, som går ud over det aftalte, er det rimeligt, at Dansk Psykologisk Forlag honoreres særskilt for denne indsats, da en sådan service ikke er en del af Dansk Psykologisk Forlags abonnementspriser og transaktionsomkostninger. Hvis Dansk Psykologisk Forlag har begået fejl ved

		grov uagtsomhed, er det tilsvarende rimeligt, at Dansk Psykologisk Forlag bistår Kunden i det omfang det måtte være relevant uden særskilt beregning.
11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.	11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige inden 3 måneder efter Hovedaftalens ophør og bekræfte over for den dataansvarlig, at oplysningerne er slettet, eller tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.	Der er indsat en tidsfrist for sletning på 30 dage.
14.1 Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.	14.1 Bestemmelserne træder i kraft på datoen for begge parters tiltrædelse af Hovedaftalen.	Aftaleindgåelse er mere smidig på denne måde.
14.5 Underskrift På vegne af den dataansvarlige Navn Stilling Telefonnummer E-mail Underskrift På vegne af databehandleren Navn Stilling Telefonnummer E-mail Underskrift	Bestemmelsen udgår.	Aftaleindgåelse er mere smidig på denne måde.
15.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.	15.1 Parterne kan kontakte hinanden via de i	Aftalen er mere smidig på denne måde.

	Hovedaftalen specificerede kontaktpersoner.	
14.5 Underskrift På vegne af den dataansvarlige Navn Stilling Telefonnummer E-mail Underskrift På vegne af databehandleren Navn Stilling Telefonnummer E-mail Underskrift	Bestemmelsen udgår.	Aftaleindgåelse er mere smidig på denne måde.