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

Firma/organisation: _____

Telefon: _____

Postnr./By: _____

CVR-nr.: _____

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 kontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

Bestemmelserne udgør Datatilsynets standardkontraktbestemmelser (sort skrift) med de tilpasninger, som fremgår med blå skrift.

Dansk Psykologisk Forlag A/S, Januar 2025

Indhold

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af databehandlerens services, jf. 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 bestemmelser vedrørende andre aktiviteter, som ikke af 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.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

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

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a) Pseudonymisering og kryptering af personoplysninger

   b) Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

   c) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

   d) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med det varsel, der fremgår af bilag B.2 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.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a) Overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

   b) Overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

   c) Behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

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

9. Bistand til den dataansvarlige

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

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede

b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet i Danmark, 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 i Danmark, 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.

10. Underretning om brud på persondatasikkerheden

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

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

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

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

    b) de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige inden 3 måneder efter aftalens 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.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner,

der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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.

14. Ikrafttræden og ophør

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

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 kan enten:

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

   b. underskrives manuelt af den dataansvarlige og træder i kraft herefter, eller

c. træde i kraft automatisk ved bestilling af system uden indsigelse fra Kunden inden 14 dage.

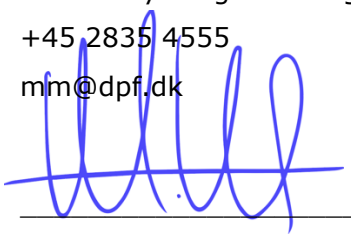
På vegne af den dataansvarlige

Navn _____
Stilling _____
Firma/organisation _____
Telefon _____
E-mail _____

Dato og underskrift _____

På vegne af databehandleren

Navn	Martin Første Montag
Stilling	Adm. Direktør / CEO
Firma	Dansk Psykologisk Forlag A/S
Telefon	+45 2835 4555
E-mail	mm@dpf.dk

Underskrift  _____

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via kontaktoplysningerne angivet nedenfor:

Dataansvarlige:

Navn _____
Stilling _____
Firma/organisation _____
Telefon _____
E-mail _____

Databehandleren:

Navn	Martin Første Montag
Stilling	Adm. Direktør / CEO
Firma	Dansk Psykologisk Forlag A/S
Telefon	+45 2835 4555
E-mail	mm@dpf.dk

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 vedhæftede Bilag A.

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

Beskrivelserne i Bilag A indgår automatisk i Bestemmelserne, når den dataansvarlige, 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
ADDvision ApS CVR-nr. 21356344 Lyskær 9 2 2730 Herlev Underdatabehandlere: Ingen	Hosting og support.	Databehandleraftale baseret på Datatilsynets standard. Udleveres på anmodning.	Danmark
Inizio Engage Nordic CVR-nr. 25784723 Rådhuspladsen 16 1550 København K Underdatabehandlere: Ingen	Support.	Databehandleraftale baseret på Datatilsynets standard. Udleveres på anmodning.	Danmark
Made This ApS CVR-nr. 38910914 Kochsgade 31D, 2. 5000 Odense C Underdatabehandlere: Ingen	Support.	Databehandleraftale baseret på Datatilsynets standard. Udleveres på anmodning.	Danmark
Anahoret SL at Calle Clara Campoamor, 12, BW 28, Alacant / Alicante, 03540, Spanien Underdatabehandlere: Ingen	Support.	EU Kommissionens standardaftale af 4. juni 2021, som udleveres på anmodning.	Spanien

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 aftalen, 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 herunder:

Bilag C.2 – Beskrivelse af behandlingssikkerhed

Teknisk sikkerhed	Beskrivelse
Antivirus	Alle enheder hos DPF, samt eksterne konsulenters enheder, er forsynet med antivirus. Enhederne opdateres og vedligeholdes automatisk.

Firewall	Enhver adgang er sikret med firewall, som vedligeholdes løbende. Administrativ adgang er begrænset til bestemte IP-adresser for de enkelte brugere. Firewalls opdateres løbende til den nyeste version for at lukke for eventuelle sårbarheder. Overvågning af sårbarhed er indbygget i databehandlerens software. Switche opdateres sammen med firewalls og indgår i denne overvågning.
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.
Kryptering ved transmission via web og mail	Der anvendes webkryptering https:// med gyldigt certifikat TLS 1048-bit på de online platforme, som stilles til rådighed af databehandleren. Hvis der i forbindelse med en særskilt instruks eller supportcase sendes personoplysninger uden for platformene, sker det som minimum med TLS 1.2-kryptering. Sendes der personoplysninger, der efter konkret vurdering kræver yderligere sikkerhedsforanstaltninger end TLS 1.2, sker dette med IRM-beskyttet mail. Alle ansattes daglige arbejde foregår via VPN.
Logning	Logning foretages på login, som opbevares løbende i 180 dage. Derudover foretages der på STAV, SK og SEF fejllogning, dvs. hvis systemet fejler. Da det ikke er muligt at manipulere data, foretages der ikke yderligere logning på produktplatformene.
Logbeskyttelse	Der er logbeskyttelse i form af autoriseret adgang til logdatabasen. Dette hidrører kun få betroede personer. Loggen gennemgås løbende.
Testmiljø	Alt data der benyttes i eventuelle testmiljøer, er fuldt anonymiseret, og indeholder ikke personoplysninger tilhørende den dataansvarlige. Implementeringen af evt. udviklingsmoduler sker direkte på produktionsserveren hos databehandleren.
Sårbarhedstest	Hosting-leverandøren foretager løbende test.

Opdateringer, patches, mv.	Ændringer i 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 henvises til beskrivelser under de enkelte systemer i Bilag A.

Fysisk sikkerhed	**Beskrivelse**
Adgangsforhold	I arbejdstiden sker adgangen til kontoret først gennem en port, som er åben indenfor almindelig kontortid (porten er aflåst om natten og almindeligvis på helligdage), og dernæst gennem en opgangsdør som altid er aflåst. Døren åbnes enten med nøgle eller nøglebrik. Adgangsdøren til kontorlejemålet er aflåst med en systemnøgle og sikret med et moderne alarmanlæg med videoovervågning, der aktiveres udenfor åbningstiden. Hvis alarmen aktiveres, sendes der besked til alarm-selskabet, samt en SMS til den ansvarlige på forlaget. I forlagets åbningstid er døren ulåst, således ansatte og besøgende har fri adgang til kontorlejemålet. Receptionen, som altid er bemandet med én til to medarbejdere, er placeret ved indgangen til kontorlejemålet, hvorfor ingen besøgende kan træde ubemærket ind på forlaget. Forlagets ansatte har nøgler og kodebrik til alle døre. Udover alle ansatte har forlagets rengøringsfirma også adgang til kontoret uden for åbningstiden. Alle ansatte er instrueret i, at fortrolige og følsomme persondata altid skal opbevares utilgængeligt for uvedkommende. Udover Dansk Psykologisk Forlag huser ejendommen også andre selskaber, der driver erhvervsvirksomhed inden for liberale erhverv.

Organisatorisk sikkerhed	Beskrivelse
Informationssikkerhedspolitik	DPF har udarbejdet en it-sikkerhedspolitik der bl.a. indeholder en beskrivelse af korrekt databehandling. Sikkerhedspolitikken er dels udleveret og dels overdraget gennem oplæring til alle ansatte.
Medarbejdertillid	Der er en generel procedure for efterprøvning af ansatte i forbindelse med ansættelse.
Fortrolighed	Alle databehandlerens ansatte er underlagt en tavshedspligts- og fortrolighedserklæring. Det samme gælder hos underleverandører.
Fratrædelsesprocedurer	Fratræder en ansat overleveres data til en kollega, som har autoritet til at varetage disse i en overgangsfase. Den ansattes adgang til terminalserven lukkes straks efter fratrædelsen, hvilket håndteres i samarbejde med alle relevante aktører.
Awareness-træning	Alle ansatte hos databehandleren har fået udtrykkelig instruks angående opbevaring, behandling, sletning og sikkerhed vedrørende behandling af personoplysninger. Instruksen opdateres løbende. Der afholdes endvidere et seminar hvert halve år om relevante databeskyttelsesretlige aspekter.

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.

Bistand til overholdelse af de registreredes rettigheder:

Databehandler skal indrette løsningerne således, at de understøtter den Dataansvarliges pligt til at overholde reglerne om registreredes rettigheder.

Underretning af den Dataansvarlige om anmodninger fra den registrerede

Databehandler skal have faste procedurer, der sikrer, at den Dataansvarlige uden unødig forsinkelse skriftligt bliver underrettet om

- *enhver anmodning rettet til Databehandler eller dennes eventuelle Underdatabehandlere fra en registreret om udøvelse af den registreredes rettigheder. Den Dataansvarlige besvarer sådanne henvendelser.*

- *enhver henvendelse rettet til Databehandler eller dennes eventuelle underdatabehandlere fra Datatilsynet vedrørende behandling af personoplysninger omfattet af databehandleraftalen. Den Dataansvarlige besvarer sådanne henvendelser.*
- *enhver henvendelse om tilsyn rettet til Databehandler eller dennes eventuelle underdatabehandlere fra øvrige myndigheder*
- *videregivelse af de personoplysninger, som er omfattet af databehandleraftalen, medmindre orienteringen er forbudt i henhold til EU-retten eller lovgivningen i en medlemsstat. Hvis videregivelsen finder sted som følge af præceptiv lov i et ikke sikkert tredjeland og orienteringen er forbudt i henhold til dette lands lovgivning, skal den pågældende Databehandler straks oplyse den Dataansvarlige om, at aftalen misligholdes.*

Bistand ved sikkerhedsbrud

Databehandler bistår den Dataansvarlige i tilfælde af sikkerhedsbrud.

Databehandler skal indsamle og dokumentere informationer om sikkerhedshændelser hos Databehandler og Underdatabehandlere, og underrette den Dataansvarlige om sikkerhedsbrud, uden ugrundet ophold og senest indenfor det antal timer som fremgår af punkt 10.2. Oplysningerne skal i sidste ende have et omfang og en detaljeringsgrad, som den Dataansvarlige i det konkrete tilfælde finder tilstrækkeligt. Databehandler oplyser så vidt muligt følgende indenfor den angivne tidsramme i punkt 10.2:

Dato og tid	*Brud på persondatasikkerheden er konstateret den [DATO] klokken [KLOKKESLET]*
Karakteren af bruddet	*Hændelsen skyldes [BESKRIV ÅRSAGEN/KARAKTEREN AF BRUDDET].*
Kategorierne og det omtrentlige antal berørte registrerede	*Typen af berørte registrerede er [ANGIV TYPEN AF BERØRTE REGISTRERede] og antal berørte er [ANGIV ANTAL BERØRTE FOR HVER TYPE REGISTRERede. EVT. DET OMTRENTELIGE ANTAL, HVIS EN NÆRMERE SPECIFICERING IKKE ER MULIG]*
Typen af personoplysninger	*[ANGIV TYPEN AF PERSONOPLYSNINGER]*
Varigheden af bruddet	*[ANGIV START- OG SLUTTIDSPUNKT]*
De sandsynlige konsekvenser af bruddet	*[BESKRIV SANDSYNLIGE KONSEKVENSER AF BRUDDET]*
Andre oplysninger inkl. umiddelbar persondataretlig vurdering af bruddet	*[ANGIV ANDRE OPLYSNINGER OM BRUDDET, DER KAN VÆRE BRUGBARE FOR DEN DATAANSVARLIGES VURDERING AF BRUDDETS INDVIRKNING]*

Foranstaltninger truffet	*[BESKRIV DE FORANSTALTNINGER, DER ER TRUFFET, ELLER SOM VIL BLIVE TRUFFET SOM LED I HÅNDTERINGEN AF BRUDDET OG DETS MULIGE SKADEVIRKNINGER]*
Kontaktoplysninger	*[NAVN OG KONTAKTOPLYSNINGER TIL KONTAKTPUNKT, HVOR YDERLIGERE OPLYSNINGER KAN INDHENTES]*

Databehandlerens bistand til den Dataansvarlige er lovpligtig, jf. art 28 stk. 3 litra e. og dermed påregnelig. Ovenstående og lignende ydelser honoreres ikke. Det er udelukkende ekstraordinære indsatser der honoreres.

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.

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

Databehandleren skal årligt for egen regning levere en inspektionsrapport som dokumentation for, at der er udført tilsyn med databehandlerens opfyldelse af sine forpligtelser iht. denne databehandleraftale.

Inspektionsrapporter fremsendes uden unødig forsinkelse til den Dataansvarlige ved forespørgsel. Den Dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny revisions-erklæring eller inspektionsrapporter under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen eller rapporten 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 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).

Og/eller

Den dataansvarlige eller en repræsentant for den dataansvarlige foretager en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt. Den dataansvarliges 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

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

Databehandleren skal årligt for egen regning udføre tilsyn hos underdatabehandlere baseret på Datatilsynets vejledning om tilsyn. Valget af tilsyn afhænger af den årlige risikovurdering.

Revisionserklæringer eller inspektionsrapporter fremsendes uden unødig forsinkelse til den Dataansvarlige ved forespørgsel. Den Dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny revisions-erklæring eller inspektionsrapporter under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen eller rapporten 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.

Bilag D - Parternes regulering af andre forhold

N/A