DATABEHANDLERAFTALE version 1.3.2b

Mellem

Xxx Kommune
CVR. nr.: xxxx
(herefter ”Kommunen”)

og

WEBTJENESTEN LÆRIT.DK ApS
Ellehammersvej 93
7500 Holstebro
CVR: 35862056
(herefter ”Leverandøren”)

er der indgået nedenstående databehandleraftale (herefter ”Aftalen”) om Leverandørens behandling af personoplysninger på vegne af Kommunen:

1. Generelt

1.1 Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:

(i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).

(ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).

1.2 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.

1.3 I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

1.4 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

1.5 Leverandøren forpligter sig herudover til at gøre sig bekendt med Kommunens it-sikkerhedsregulativ og it-sikkerhedspolitik, såfremt disse er fremsendt til leverandøren.

2. Formål

2.1 Leverandøren behandler i medfør af aftale med Kommunen kontrakt vedrørende leverance af Børnetubeabonnement, (herefter ”Hovedaftalen”) personoplysninger for Kommunen, hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Kommunens rettigheder og forpligtelser

3.1 Kommunen er dataansvarlig for de personoplysninger, som Kommunen instruerer Leverandøren om at behandle.

3.2 Kommunen har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

4. Leverandørens forpligtelser

4.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kommunen, jf. pkt. 6 og bilag 3.

4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kommunen, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.

4.3 Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.

4.4 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.

4.5 Leverandøren skal på opfordring fra Kommunen hjælpe med at opfylde Kommunens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Kommunens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

4.6 Leverandøren skal fra 25. maj 2018 hjælpe Kommunen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.

4.7 Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kommunens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

4.8 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Kommunens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kommunen ved enhver ændring.

4.9 Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

5. Underleverandør (underdatabehandler)

5.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kommunen.

5.2 Leverandøren må anvende andre underdatabehandlere end dem, der er angivet i bilag 2, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Kommunen har overladt til Leverandøren i medfør af Hovedaftalen. Kommunen kan gøre indsigelse overfor tilføjelse eller udskiftning af en underdatabehandler, og nægte at godkende ændringen, såfremt der foreligger en konkret saglig begrundelse herfor. Leverandøren skal ajourføre oplysningerne over for Kommunen ved enhver ændring.

5.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Kommunen er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.

5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Kommunen er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kommunen ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.

5.6 Kommunen kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kommunen.

5.7 Al kommunikation mellem Kommunen og underdatabehandleren sker via Leverandøren.

6. Instrukser

6.1 Leverandørens behandling af personoplysninger på vegne af Kommunen sker udelukkende efter dokumenteret instruks, jf. bilag 3.

6.2 Leverandøren giver fra 25. maj 2018 omgående besked til Kommunen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

(i) tilintetgøres, mistes, ændres eller forringes,
(ii) kommer til uvedkommendes kendskab eller misbruges, eller
(iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1.

7.2 Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

7.3 Leverandøren skal mindst en gang årligt gennemgå sine interne sikkerheds-forskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 og 7.2, samt bilag 1.

7.4 Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.

7.5 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kommunens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.

7.6 Leverandøren er forpligtet til straks at underrette Kommunen om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

7.7 Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.6, uden forudgående skriftlig aftale med Kommunen om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

8.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kommunens instruks herfor, jf. bilag 3.

8.2 Hvis Kommunens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

8.3 Leverandøren er forpligtet til at holde sig ajour med Tilsynsmyndighedens fortegnelse over godkendte 3. lande, samt uden unødigt ophold at give Kommunen meddelelse om ændringer heri samt foretage foranstaltninger for lovliggørelse når ændringer i fortegnelsen har betydning for Leverandørens lovlige behandling af Kommunens oplysninger.

9. Tavshedspligt og fortrolighed

9.1 Leverandøren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.

9.2 Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

10.1 Leverandøren er forpligtet til at give Kommunen nødvendige oplysninger til, at Kommunen kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.

10.2 Kommunen, en repræsentant for Kommunen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.

10.3 Leverandøren skal én gang årligt vederlagsfrit til Kommunen fremsende en erklæring om overholdelse af denne Aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandleres databehandling. Den første erklæring skal foreligge senest 12 måneder efter Hovedaftalens indgåelse.

10.4 I tilfælde af, at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en uanmeldt fysisk inspektion af de ovennævnte foranstaltninger, forpligter Databehandleren sig til at stille tid og ressourcer til rådighed herfor.

11. Ændringer i Aftalen

11.1 I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Kommunen med et varsel på 60 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

12. Sletning af data

12.1 Kommunen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.

12.2 Kommunen skal senest 90 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kommunens meddelelse.

12.3 Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

13. Misligholdelse og tvistigheder

13.1 Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

14. Erstatning og forsikring

14.1 Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen.

15. Ikrafttræden og varighed

15.1 Aftalen indgås ved begge parters underskrift og løber indtil ophør af Hovedaftalen.

For Kommunen	For Leverandøren
Dato	Dato
_____	_____

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

Bilag 3 – Instruks

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

Generelle sikkerhedsforanstaltninger
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om interne sikkerhedsbestemmelser, instrukser, retningslinjer for Leverandørens tilsyn og ajourføring, instruktion, fysisk sikring samt sikkerhed ved reparation, service, kassation af medier mv.]

Fysisk sikkerhed:
Leverandørens datacenter er fysisk placeret (co-location) hos Nianet.
Datacenteret er tier 2 klassificeret, og har en ISAE 3402 type 2 erklæring.
Datacenteret er skalsikret, og datacenterenes døre og vinduer er således sikret imod indtrængen. Datacenteret er forsynet med sensorer til detektering af indbrud og indbrudsforsøg.

Datacenteret er under konstant overvågning med overvågningskameraer, udvendigt ved indgangsdøre og indvendigt med kameraer i udvalgte områder/vinkler.
Til Leverandørens datascenter, hvori løsningen er placeret, er der kun adgang for udvalgt personale fra Leverandøren.
Det installerede adgangskontrolsystem sikrer, at det kun er muligt at komme ind i datacenteret ved hjælp af nøglebrik og personlig kode.

Leverandørens udstyr er monteret i serverracks, der er tilsluttet 2 separate strøm sikringsgrupper. Gulvene i maskinstuerne er forsynet med en antistatisk belægning.
Strøm til serverracks har UPS anlæg, batterier og dieselgeneratorer.

Datacenteret er tilsluttet køleanlæg.
Maskinstuerne er inddelt i kold og varm zone.
Køleanlægget sikrer en rumtemperatur i maskinstuerne på max 25° C.

I maskinstuerne er installeret et brandalarmeringssystem. Til brandbekæmpelse er installeret et inergenanlæg, som minimerer indholdet af ilt i luften og således kvæler ilden uden at beskadige infrastrukturen.

Databærende mediaer (hardiske/bånd), som ikke længere tjener et formål, destrueres/ødelægges med hammer.

Logisk sikkerhed:
Datacenteret er beskyttet af firewall teknologi baseret på Cisco. Leverandøren forbeholder sig retten til at vælge anden teknologileverandør.

Backupdata opbevares på selvstændig hardware, placeret i et andet datacenter.

Organisatoriske sikkerhedsforanstaltninger:
Leverandøren tillader udelukkende særlige medarbejdere adgang til datacenteret. Således er adgangen begrænset til de personer, som har en reel funktion i datacenteret.

Enhver medarbejder hos Leverandøren er underlagt tavshedspligt, hvilket indebærer, at medarbejderen også efter ansættelsesforholdets ophør har tavshedspligt med hensyn til alt, hvad vedkommende har erfaret i ansættelsesforholdet. Denne tavshedspligt dækker både over interne og kunderelaterede oplysninger samt forretningshemmeligheder.

Autorisation og adgangskontrol
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2, samt hvis relevant kap. 3, om autorisationer og adgangskontrol]

Brugere af platformen (lærere, elever osv.):
Autorisation og adgangskontrol er integreret med STIL Uni-login. Det er således den ansvarlige hos kommunen/institutionen, der administrerer og vedligeholder, hvilke brugere som har adgang.

Leverandørens medarbejdere:
Adgang til databaser med udvidede rettigheder er begrænset til få udvalgte medarbejdere.
Adgang til det fysiske datacenter er begrænset til få udvalgte medarbejdere og underlagt separat adgangskontrol med ID kort og nøgler samt videoovervågning.

Inddatamateriale som indeholder personoplysninger
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om håndtering af inddatamateriale]

Ikke relevant, idet der ikke håndteres inddatamateriale jf. Sikkerhedsbekendtgørelsens kap. 2 om inddatamateriale.

Uddatamateriale som indeholder personoplysninger
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om håndtering af uddatamateriale]

Ikke relevant, idet der ikke håndteres uddatamateriale jf. Sikkerhedsbekendtgørelsens kap. 2 om uddatamateriale.

Eksterne kommunikationsforbindelser
[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om eksterne kommunikationsforbindelser. Hjælp til udfyldelse kan findes i Datatilsynets it-sikkerhedstekster: https://www.datatilsynet.dk/vejledninger/it-sikkerhedstekster/]

Alle data er krypterede, når de sendes over Internettet, enten via VPN-forbindelser eller via HTTPS protokollen.

Kontrol med afviste adgangsforsøg
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 3 om kontrol med afviste adgangsforsøg]

Leverandøren behandler ikke personoplysninger, der er anmeldelsespligtige efter lov nr. 429 om behandling af personoplysninger af 31/5 2000, og er derfor ikke omfattet af kravet om kontrol med afviste adgangsforsøg efter kapitel 3 i Sikkerhedsbekendtgørelsen (bekg. nr. 528 af 15/6 2000).

Logning
[Her beskriver Leverandøren, hvis relevant, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 3 om logning]

Leverandøren behandler ikke personoplysninger, der er anmeldelsespligtige efter lov nr. 429 om behandling af personoplysninger af 31/5 2000, og er derfor ikke omfattet af kravet om logning i kapitel 3 i Sikkerhedsbekendtgørelsen (bekg. nr. 528 af 15/6 2000).

Hjemmearbejdspladser
Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser:

✓ Ja

☐ Nej

[Her beskriver Leverandøren, hvordan Leverandøren overholder kravene i Sikkerhedsbekendtgørelsens kap. 2 om retningslinjer for hjemmearbejdspladser mv.]

Leverandørens medarbejdere har adgang til personoplysninger fra pc-arbejdspladser uden for Leverandørens lokationer, der er opkoblet via VPN forbindelser.
Pc-arbejdspladserne er til enhver tid opdaterede og beskyttet med antivirusprogrammel.

Sikkerhedskrav fra 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk

2. Implementeringsomkostningerne

3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)

4. Konsekvenserne for borgerne ved et sikkerhedsbrud

5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:

    a) tilintetgørelse af oplysningerne

    b) tab af oplysningerne

    c) ændring af oplysningerne

    d) uautoriseret videregivelse af oplysningerne

    e) uautoriseret adgang til oplysningerne

De allerede beskrevne og implementerede tekniske og organisatoriske foranstaltninger vil efter 25. maj 2018 blive suppleret af en pseudonymisering af personoplysningerne ved brug til underdatabehandlere.

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. **Lokation(er) for behandlingen** *[Her opregner Leverandøren, de steder, hvor Kommunens personoplysninger opbevares/behandles.]*

   Webtjenesten LÆRIT.DK ApS
   c/o Nianet A/S
   Hørskætten 6C
   2630 Taastrup

   Webtjenesten LÆRIT.DK ApS
   c/o Nianet A/S
   Egeskovvej 2
   2665 Vallensbæk Strand

2. **Underdatabehandlere**

   Book Creator
   Red Jumper Limited
   31-34 High Street
   Bristol, BS1 2AW
   UK

   Explain Everything sp. z o.o.
   Orzechowa 4,
   55-002 Kamieniec Wroclawski
   Poland
   UE Tax-ID: PL 8961543036

   MeisterLabs GmbH
   Valentin-Linhof- Str. 8
   81829 München
   Deutschland
   Ust-IdNr/VAT.: DE 247 139 684

   WeVideo Inc.
   149 Commonwealth Dr.
   Ste.2118
   Menlo Park, CA 94025
   USA

Bilag 3 – Instruks

Instruks
Kommunen instruerer hermed Leverandøren om at foretage behandling af Kommunens oplysninger til brug for levering af Børnetubeabonnement, jf. Hovedaftale.

1.1 Behandlingens formål

Behandling af Kommunens oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Kommunen.

1.2 Generel beskrivelse af behandlingen

Via Uniloginkald modtages brugerens fornavn, efternavn, uniloginbrugernavn, institutionsnr og funktion (fx pæd, lærer). Med disse data oprettes en personlig profil på Børnetube, hvor brugeren beskyttet kan opbevare sine uploadede medieproduktioner.
Ovenstående oplysninger bruges desuden, hvis brugeren ønsker, at benytte en af Børnetubes underleverandører. En profil oprettes ved underleverandøren via sikker API. (fra 1/7-2017 benytter nye brugere ikke ovenstående persondata i sammenhæng med underleverandører. Her bruges nu pseudonymiserede profildata).

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):

☐ Racemæssig eller etnisk baggrund
☐ Politisk overbevisning
☐ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssige tilhørsforhold
☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):

☐ Strafbare forhold
☐ Væsentlige sociale problemer
☐ Andre rent private forhold, som ikke er nævnt ovenfor:

_____

_____

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

☐ CPR-numre

1.4 Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):

A) Institutions børn

B) Pædagogisk personale

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren må overføre personoplysninger til følgende tredjelande:

USA (EU-US Privacy Shield)
USA (EU Kommissionens standardkontrakt)

Gyldigt overførselsgrundlag for overførslerne er:

A) EU-US Privacy Shield
B) EU KOMMISSIONENS AFGØRELSE af 5. februar 2010 om standardkontrakt-bestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (meddelt under nummer K(2010) 593) (EØS-relevant tekst) (2010/87/EU)