Databehandleraftale

Mellem

København Kommune
Beskæftigelses-, Integrations-
og Erhvervsforvaltning

Og

XX



Changelog

Version	DATO	ændringer
1.0	November 2026	

Standardkontraktsbestemmelser

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

mellem

Københavns Kommune
Beskæftigelses- Integrations- og Erhvervsforvaltningen
CVR 64942212
Gammel Køge Landevej 43
2500 Valby
Danmark

herefter "den dataansvarlige"

og

[NAVN]
CVR [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

Kommenterede [HF1]: Udfyldes af STU-skole.

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 og frihedsrettigheder

1. Indhold

2. Præambel 5
3. Den dataansvarliges rettigheder og forpligtelser 5
4. Databehandleren handler efter instruks 6
5. Fortrolighed 6
6. Behandlingssikkerhed 6
7. Anvendelse af underdatabehandlere 7
8. Overførsel til tredjelande eller internationale organisationer 8
9. Bistand til den dataansvarlige 9
10. Underretning om brud på persondatasikkerheden 10
11. Sletning og returnering af oplysninger 10
12. Revision, herunder inspektion 11
13. Parternes aftale om andre forhold 11
14. Ikrafttræden og ophør 11
15. Kontaktpersoner hos den dataansvarlige og databehandleren 12
Bilag A Oplysninger om behandlingen 13
Bilag B Underdatabehandlere 14
Bilag C Instruks vedrørende behandling af personoplysninger 15
Bilag D Parternes regulering af andre forhold 24

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 **ydelser under kvalitetsaftale for særligt tilrettelagt ungdomsuddannelse** 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.

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

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

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

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.

3. Når den Dataansvarlige er blevet underrettet om, at Databehandleren vurderer, at en instruks er ulovlig, skal Databehandleren ophøre med behandlingen indtil en nærmere dialog med Dataansvarlige har fundet sted.

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. 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 specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler, jf. bilag B.2. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.1.

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. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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, 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.

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 og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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 heraf.

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

På vegne af den dataansvarlige

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Dato og underskrift

Kommenterede [HF2]: Se proces for underskrift af Databehandleraftaler.

På vegne af databehandleren

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Dato og underskrift

Kommenterede [HF3]: Udfyldes af Databehandler.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Dataansvarlig:

Navn	Iwona Teresa Wozninska
Stilling	Chefkonsulent, Københavns Kommune
Telefonnummer	30512473
E-mail	dk9l@kk.dk

Navn	Hans Erik Praëm Fussing
Stilling	Fuldmægtig, Københavns Kommune
Telefonnummer	21627441
E-mail	G633@kk.dk

Databehandler:

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Kommenterede [HF4]: Udfyldes af Databehandler.

Bilag A Oplysninger om behandlingen

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

Dataansvarlig og databehandleren udveksler oplysninger om den unge med henblik på, at den unge kan gennemføre en STU i overensstemmelse med den unges forløbsplan.

Dataansvarlig og databehandleren behandler hver især oplysningerne til brug for de opgaver, som STU-loven tillægger dem. Dataansvarlig anvender oplysningerne til sine myndighedsopgaver, herunder afgørelse om optagelse, uddannelsesplan og valg af uddannelsessted samt opfølgning på uddannelsesplanen. Databehandleren anvender oplysningerne til at tilrettelægge og gennemføre undervisningen og til at give input til kommunens opfølgning.

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

Databehandlerens behandling drejer sig primært om opbevaring, brug, formidling, indsamling, registrering og sletning.

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

- Almindelige personoplysninger i form af
  - Kontakts- og identifikationsoplysninger
  - Fraværsregistrering
- Fortrolige personoplysninger i form af
  - CPR.nr
  - Straffeattest, samt evt. oplysninger om strafbare forhold
  - Sociale forhold
  - Økonomiske forhold
- Følsomme personoplysninger i form af
  - Helbredsoplysninger, herunder diagnoser og lægelig dokumentation

A.4. Behandlingen omfatter følgende kategorier af registrerede

Unge, der er visiteret til STU.

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

Databehandleraftalen følger kontraktsperioden.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Kommenterede [HF5]: Udfyldes af STU-skolen.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

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

Varslingsperioden for godkendelse af nye underdatabehandlere er på minimum 60 dage, jf. punkt 7.3.

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 registrerer fremmøde og fravær og fører egen pædagogisk dokumentation, hvis form og indhold databehandleren selv fastlægger. Databehandleren udarbejder desuden praktikbeskrivelser ifm. virksomhedspraktikker

Forløbsplan og ressourcepapir udarbejdes i samarbejde mellem den unge, databehandleren og dataansvarlig. Dokumentationen tager udgangspunkt i den unges perspektiv og de mål, der arbejdes med i uddannelsen. Databehandleren giver input om den unges forløb og progression samt en vurdering af realistiske perspektiver efter uddannelsen. Dataansvarlig anvender inputtet i opfølgningen på uddannelsesplanen og i sine afgørelser.

Databehandleren deler oplysninger om fremmøde, fravær og den unges forløb med dataansvarlig. Oplysningerne deles i KUI og Uno STU.

C.2. a Behandlingssikkerhed

Kommenterede [HF6]: Nedenstående sikkerhedskrav tilpasses den enkelte kontrakt.

Databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige.

Det følger af databeskyttelsesforordningens artikel 24 og artikel 32, at dataansvarlige har ansvaret for at sikre sikkerhedsforanstaltninger, der er tilpasset det aktuelle risikoniveau. På baggrund heraf vurderer vi, at databehandleren skal foretage følgende foranstaltninger:

Emne:	Krav
ISO 27001	Databehandleren skal implementere relevante sikkerhedsforanstaltninger og kontrolprocedurer, herunder opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS), efter den til enhver tid gældende version af den internationale sikkerhedsstandard ISO/TEC 27001 eller tilsvarende national eller international anerkendt standard.
Netværkssikkerhed	Interne netværk skal segmenteres for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Databehandleren skal sikre, at netværk, systemer og applikationer overvåges for unormal adfærd, samt at der iværksættes passende handlinger for at evaluere potentielle informationssikkerhedshændelser og brud på persondatasikkerheden under hensyntagen til den til enhver tid gældende risikovurdering.
Adgangsstyring / privilegerede adgangsrettigheder / funktionsadskillelse	Databehandleren skal sikre, at tildelingen og anvendelsen af privilegerede adgangsrettigheder i relation til systemer, hvori der behandles personoplysninger, begrænses og styres.

	Brugeradministratorer dokumenterer udstedelse af adgangsrettigheder til sig selv eller andre. Der skal være funktionsadskillelse af øvrige arbejdsopgaver og tildeling af adgangsrettigheder således at en administrator ikke kan godkende egen adgang til et it-system.
Adgangsbegrænsning	Kun medarbejdere autoriseret hertil må have adgang til de personoplysninger, der behandles. Dette skal sikres både med organisatoriske og tekniske foranstaltninger.
Brugerstyring	Medarbejdere hos dataansvarlige skal alene kunne tilgå it-systemet via brugerstyringen på KK´s centrale brugersstyringsplatform (IGA). Hvis medarbejdere hos databehandleren har adgang til it-systemet uden om KK´s brugerstyringsplatform, skal der føres en opdateret oversigt over disse medarbejdere og deres rettigheder.
Logning	Databehandleren skal sikre, at der udarbejdes log af alle behandlinger af personoplysninger med henblik på undersøgelse af tidligere indtrufne hændelser i it-systemer. Databehandleren foretager relevant kontrol af log og udleverer efter anmodning logs uden udgifter for den dataansvarlige. Følgende logning skal etableres *vælg alt efter relevans*: • Hvem der har tilgået en personoplysning (bruger, enhed, system, terminalID og ip-adresse) • Hvornår der er tilgået en personoplysning (tidsstempling på sekundniveau) • Hvem der har ændret en personoplysning, herunder sletning. • Hvornår der er ændret i en personoplysning, herunder sletning. • Ændring af brugerrettigheder • Afviste adgangsforsøg • Afviste autentifikationsforsøg som følge af konto lockout udløst af adgangskontrol system • Forsøg på at øge adgangsprivilegier • Systemfejl • Alle anvendelser af personoplysninger foretaget af brugere, herunder læsning, tilføjelse, søgning (evt. søgekriterium), ændring, udtræk og sletning Der skal i øvrigt iværksættes *vælg alt efter relevans*: • Logning af ændringer i logopsætning, herunder deaktivering af logning • Automatiserede overvågnings- og alarmeringsprocesser *kan erstattes med manuelle overvågnings- og alarmeringsprocesser*. • Adgang til logs skal begrænses It-systemerne gemmer logdata i et specifikt tidsrum, [ANGIV TIDSPERIODE *fx de sidste 13 måneder*].

Adgangskode	Adgangskoder skal følge Københavns Kommunes passwordpolitik:
	
	• Adgangskoden skal have **minimum 15 karakterer**
	• Adgangskoden skal indeholde:
	  ○ små bogstaver
	  ○ STORE BOGSTAVER
	  ○ tal (fra 0 til 9) eller specialtegn (!#%^-&*)

Multifaktor-autentifikation	Adgang til systemer, databaser og øvrige konti hvori der sker behandling af personoplysninger på vegne af den dataansvarlige, skal som minimum ske ved anvendelse af to-faktor-autentifikation. Adgangen til konti, der er tildelt privilegerede rettigheder, skal beskyttes med multifaktor-autentifikation. Det gælder også konti, der anvendes i forbindelse med ekstern eller fjernadgang adgang til organisationens systemer.
Automatisk lås ved ineffektivitet	Arbejde med dataansvarliges personoplysninger skal ske på devices, der er sat op til at låse automatisk efter [ANGIV TIDSPERIODE *fx 5/ 10 minutter*.]
Beskyttelse mod malware	Databehandleren skal sikre, at systemer og databaser der anvendes til behandling af personoplysninger, er beskyttet mod malware. Beskyttelsen sker i overensstemmelse med den til enhver tid gældende risikovurdering. Databehandleren skal have en procedure for at holde øje med offentliggjorte sårbarheder og patches, og have en procedure for at patche disse sårbarheder. Databehandleren må ikke anvende software, programmel og hardwarekonfigurationer med kendte svagheder og sårbarheder, som kan udnyttes til at få adgang til personoplysningerne.
Backup / gendannelse/sikkerhedskopiering	Databehandleren skal sikre, at der foretages sikkerhedskopiering af information, programmel og systemer, der anvendes til behandling af personoplysninger, samt at disse vedligeholdes og testes regelmæssigt. Sikkerhedskopiering skal finde sted så relevante data kan reetableres. Sikkerhedskopierne skal opbevares så de ikke hændeligt eller ulovligt kan tilintetgøres, forringes eller fortabes eller kommer til uvedkommendes kendskab, misbruges eller behandles i strid med retningslinjer og regler for behandling af personoplysninger. Aftalte slettefrister gælder også sikkerhedskopier. Databehandleren er forpligtet til at sikre rettidig genoprettelse af tilgængelighed til personoplysningerne i tilfælde af fysiske hændelser (fx strømafbrydelse, brand, oversvømmelse, lynnedslag mv.) og/eller tekniske hændelser (systemnedbrud, DoS, DDoS mv.), herunder i form af beredskabsplaner og procedurer.

	Databehandleren skal udfærdige en proces der sikrer, at personoplysninger, der skal gendannes, gendannes til en tilstand, hvor integriteten af oplysningerne kan sikres, urigtige eller ufuldstændige personoplysninger kan identificeres, og en proces for en afklaring heraf.
Kryptering	Databehandleren skal anvende effektiv kryptering af personoplysninger under transport (in transit) og i hvile (at rest). Niveauet af kryptering skal på baggrund af risikovurderingen være passende for at effektivt forhindre uvedkommende i at få adgang til personoplysninger. Kryptering af transportlaget (TLS) skal minimum være TLS 1.2 med opdaterede cyber suites. Alle ældre TLS-protokoller skal være slået fra. Databehandleren skal definere og implementere regler for effektiv anvendelse af kryptografi, herunder administration af krypteringsnøgler. Ved anvendelse af hjemme- og fjerarbejdspladser anvendes kryptering af kommunikationsforbindelser.
VPN	Ved anvendelse af hjemme- og fjerarbejdspladser anvendes kryptering af kommunikationsforbindelser og autentifikation af personer der gives adgang. Der logges på databehandlerens netværk via VPN med flerfaktorautentifikation.
Firewall	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, skal ske gennem en firewall med relevant og korrekt konfiguration i forhold til det vurderede risikoniveau.
Test	Personoplysninger må ikke anvendes til testbrug, medmindre udførelsen af tests derved umuliggøres. Er det ikke muligt at undgå at anvende personoplysninger til testbrug, skal personoplysningerne, hvis muligt, pseudonymiseres. Anvendelse må alene ske for at varetage den dataansvarliges formål i henhold til aftale og på den dataansvarliges vegne. Anvendes pseudonymiserede oplysninger, eller, rent undtagelsesvist, personoplysninger der hverken er pseudonymiserede eller anonymiserede, aftales proceduren for anvendelsen af personoplysningerne på forhånd med den dataansvarlige. Leverandøren skal adskille og sikre udviklings-, test- og produktionsmiljøer, der anvendes i forbindelse med Kontraktens opfyldelse.
Sletning	Der skal kunne opsættes sletterutiner (automatisk håndtering af sletning af personoplysninger) efter lovgivningens regler eller de administrativt fastsatte slettefriser således, at data kan slettes på bestemte tidspunkter efter de opsatte regler.

Fysiske lagringsmedier	Databehandleren dokumenterer anskaffelse, brug, transport, returnering og bortskaffelse af lagringsmedier, herunder USB-nøgler, bærbare computere og mobiltelefoner. Hvis det er muligt også, om lagringsmediet indeholder personoplysninger. Ved reparation og service af udstyr, skal databehandleren, hvis ikke oplysningerne kan fjernes fra udstyret, sikre sig, at reparations- og servicepersonalet vil behandle oplysninger, som de måtte blive bekendt med under deres arbejde, som fortroligt materiale, der under ingen omstændigheder må videregives eller anvendes. Ved kassation af lagringsmedier og udstyr, som indeholder personoplysninger, skal lagringsmedierne destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet.
Fysisk adgangsstyring	Den fysiske adgang til lokaliteter, hvor der behandles personoplysninger, sikres mod uvedkommendes adgang til oplysningerne, og kan eksempelvis omfatte aflåsning af lokaler, brug af adgangskort, alarmsystemer og vagter, samt særlig begrænsning i adgangen til serverrum. Det er et krav at databehandleren kan fremvise dokumentation for, at adgangen er effektivt styret og begrænset mest muligt, herunder at der er etableret formelle procedurer for gennemgang af adgangen til lokaliteterne.
Databehandlerens interne tilsyn	Databehandleren skal årligt gennemføre tilsyn internt i egen virksomhed med, at medarbejdere har adgange i overensstemmelse med deres arbejdsbetingede behov og at behandling af personoplysninger alene sker efter og i overensstemmelse med den dataansvarliges instruks. Databehandlerens interne tilsyn vedrørende behandling af personoplysninger i egen virksomhed skal dokumenteres og efter anmodning udleveres til den dataansvarlige.
Risikovurdering	Der skal til enhver tid foreligge en aktuel risikovurdering for den dataansvarliges personoplysninger hos databehandleren. Databehandleren skal således løbende foretage risikoanalyse og risikobedømmelse af alle hændelser og handlinger, der potentielt kan påvirke den aktuelle risikovurdering. Databehandleren skal på baggrund af risikovurderingen identificere og vurdere mulighederne for risikohåndtering. Databehandleren skal opdatere risikovurderingen for de registreredes rettigheder løbende og som minimum én (1) gang årligt. Databehandleren sender den gældende risikovurdering således at dataansvarlig til enhver tid har databehandleren seneste risikovurdering.
Fortegnelse	Databehandleren skal udarbejde og vedligeholde en fortegnelse over behandlinger af personoplysninger, der foretages på vegne af den dataansvarlige.

Awareness	Databehandleren skal løbende gennemføre awareness-træning af medarbejderne i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger, herunder hvornår der er tale om en behandling af en personoplysning til et sagligt formål, registreredes rettigheder og brud på persondatasikkerheden.
Baggrundsverifikation af medarbejdere	Der skal udføres en baggrundsverifikation af alle databehandlerens medarbejdere, der behandler personoplysninger på vegne af den dataansvarlige. Dette sker inden tiltrædelse og løbende under hensyn til regler, klassifikationsniveau og den til enhver tid gældende risikovurdering. Baggrundsverifikationen omfatter: - Referencer fra tidligere ansættelser - Straffeattest
Procedure for formålsbegrænsning	Databehandleren skal udarbejde skriftlige procedurer, som indeholder krav om, at personoplysninger alene må tilgås af brugere med sagligt og arbejdsbetinget formål. Adgangen begrænses til arbejdsbetinget behov med henblik på at undgå unødig risiko for fejlhåndtering og misbrug af oplysninger fx i muligheder for at læse, tilføje, søge, ændre, udtrække eller slette data.
Tavshedspligt	Alle medarbejdere med adgang til personoplysninger skal være underlagt kontraktuel tavshedspligt med hensyn til alt, hvad medarbejderen under ansættelse erfarer om alle forretningsmæssige og fortrolige oplysninger, som vedrører parter som databehandleren arbejder med. Tavshedspligten skal være gældende efter ansættelsesforholdets ophør.
Procedure for håndtering af anmeldelse af databrud	Databehandleren skal have dokumenterede og fungerende procedurer for håndtering af og mistanke om brud på persondatasikkerheden. Databehandleren skal sikre, at medarbejdere og andre interessenter kan indrapportere observerede eller formodede brud på persondatasikkerheden rettidigt via passende kanaler.
Lukning/deaktivering af adgange	Databehandleren skal have en proces, som sikrer, at når en medarbejder fratræder, deaktiveres kontoen, kontoens password skiftes og muligheden for passwordgendannelse for den pågældende konto deaktiveres. Dette skal ske efter [indsæt] antal dage. Databehandleren skal sikre automatisk lukning af adgang, som ikke har været anvendt i en periode [Vælg tidsinterval *fx hvert kvartal*]. Dette kan ske automatisk eller manuelt.
Fortegnelse over brugere	Det skal være muligt for databehandleren at generere fortegnelser over brugere og tildelte rettigheder over brugere, der behandler den dataansvarliges oplysninger. Fortegnelsen skal udleveres til den dataansvarlige på den dataansvarliges forlangende.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

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

• oplysningspligten ved indsamling af personoplysninger hos den registrerede
• oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
• indsigtsretten
• retten til berigtigelse
• retten til sletning (”retten til at blive glemt”)
• retten til begrænsning af behandling
• underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
• retten til dataportabilitet
• retten til indsigelse
• retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

Databehandleren skal ved anmodning herom give den dataansvarlige relevant information inden 7 dage.

Databehandleren skal bistå den dataansvarlige i tilfælde af informationssikkerhedsbrud eller brud på persondatasikkerheden og have dokumenterede og fungerende procedurer for håndtering af informationssikkerhedsbrud samt brud på persondatasikkerheden. Procedurerne skal sikre, at den dataansvarlige underrettes om eventuelle sikkerhedshændelser hos databehandleren og dennes eventuelle underdatabehandlere.

I tilfælde af brud på persondatasikkerheden eller mistanke om brud på persondatasikker-heden skal databehandleren uden unødig forsinkelse underrette den dataansvarlige på følgende mailadresse:

Bifsikkerhed@kk.dk

Databehandleren skal afgive en rapport til den dataansvarlige uden unødig forsinkelse, dog senest 24 timer efter bruddet på persondatasikkerheden eller mistanke herom. Rapporten skal som minimum indeholde følgende:

• en beskrivelse af 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
• en beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden
• en beskrivelse af 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.

Når og for så vidt som det ikke er muligt at give ovenstående oplysninger samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

Databehandleren må alene underrette tredjemand om et brud på persondatasikkerheden efter forudgående, skriftlig tilladelse fra den dataansvarlige.

C.4 Opbevaringsperiode/sletterutine

C.4.a: Sletning ved ophør af databehandleraftalen

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:

Se bilag B.1.

Medarbejderne hos databehandleren og/eller underdatabehandleren må arbejde udenfor databehandleren/underdatabehandlerens lokationer. Hvis medarbejder arbejder udenfor databehandleren/underdatabehandlerens lokationer, skal dette ske ved brug af VPN eller anden sikker forbindelse, og databehandleren/underdatabehandleren skal iværksætte en proces for godkendelse af denne mulighed for den enkelte medarbejder indeholdende awareness- og sikkerhedsforanstaltninger svarende til den vurderede risiko.

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande – Ikke instruks

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.

Der gives ikke en instruks til overførsel til et 3. land.

C.6.a Utilsigtede overførsler til 3. land

Der er ikke tale om at databehandler/underdatabehandler er underlagt lovgivning i usikkert 3. land.

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

På baggrund af den udarbejdede risikovurdering og øvrige relevante forhold, er det vurderingen, at tilsyn skal ske på følgende måde:

REVISIONSERKLÆRING

Databehandleren skal årlig 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 revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser: ISAE 3000 eller tilsvarende.

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring 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 vælger selv, hvordan tilsyn med underdatabehandlere skal foregå. Databehandleren skal efterfølgende betrygge den dataansvarlige i, at behandlingen af personoplysninger lever op til dataansvarliges krav.

Hvis dataansvarlige ikke er betrygget, kan dataansvarlige iværksætte andre foranstaltninger.

Bilag D Parternes regulering af andre forhold

Anvendelse af Kunstig Intelligens:
Databehandler (og eventuelle underdatabehandlere), må ikke anvende kunstig intelligens i forbindelse med behandling af de personoplysninger omfattet af nærværende databehandleraftale.

Hvis Databehandleren ønsker at anvende kunstig intelligens, skal det godkendes af Dataansvarlig, før sådan behandling påbegyndes.