Databehandleraftale

Mellem

Den dataansvarlige:

Styrelsen for International Rekruttering og Integration

CVR 36997427

Njalsgade 72 A

2300 København S

Danmark

og

Databehandleren:

[Navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og by]

[Land]

1 Indhold

2 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Aftalen 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)*, som stiller specifikke krav til indholdet af en databehandleraftale.

3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes "hovedaftale": [Navn på hovedaftalen/ydelsen], som er indgået den [dato].

4. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".

6. Til denne aftale hører seks bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

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

8. Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger i forhold til persondatabehandling, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".

11. Databehandleraftalens Bilag E indeholder hvilke yderligere sikkerhedsforanstaltninger, der som minimum skal iagttages.

12. Databehandleraftalens Bilag F indeholder en tavshedspligtserklæring, der skal underskrives af alle de medarbejdere hos databehandleren, der skal deltage i opfyldelsen af hovedaftalen.

13. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

14. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, 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; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

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

5 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

3. **Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.**

4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6 Behandlingssikkerhed

1. **Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32**, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

    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

3. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C og E.

4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

7 Anvendelse af underdatabehandlere

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

2. **Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.**

3. **I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.**

4. Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

5. Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.

6. **Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.**

   Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

7. Underdatabehandleraftalen og eventuelle senere ændringer skal databehandleren sende af egen drift i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

8. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for

underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

9. **Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.**

8 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. **Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel** (overladelse, videregivelse samt intern anvendelse) **af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.**

2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – indenfor rammerne af databehandleraftalen - derfor bl.a. ikke;

    a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
    b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

3. Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

9 Bistand til den dataansvarlige

1. **Databehandleren bistår, under hensyntagen til behandlingens karakter, 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 3.**

    Dette indebærer, at databehandleren 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. den registreredes indsigtsret
d. retten til berigtigelse
e. retten til sletning (»retten til at blive glemt«)
f. retten til begrænsning af behandling
g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. **Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.**

   Dette indebærer, at databehandleren under hensynstagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
   b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
   c. forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
   d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
   e. forpligtelsen til at høre tilsynsmyndigheden (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. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

10 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 9.2., litra b, skal databehandleren - under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det betyder, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

   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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
   c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Den dataansvarlige kan træffe beslutning om, at undersøgelsen af hændelsen skal foretages af den dataansvarlige, databehandleren eller af en kompetent ekstern tredjepart. Databehandleren skal på den dataansvarliges anmodning udlevere en redegørelse for databehandlerens proces for håndtering af sikkerhedshændelser.

11 Sletning og tilbagelevering af oplysninger

1. **Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.**

12 Tilsyn og revision

1. **Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.

3. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.

4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgår af parternes "hovedaftale" eller af denne aftales Bilag D.

2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.

14 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.

2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.

4. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "hovedaftalen".

5. Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

6. Underskrift

På vegne af den dataansvarlige	På vegne af databehandleren
Navn:	Navn:
Stilling:	Stilling:
Dato:	Dato:
Underskrift:	Underskrift:

15 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter:

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Kontaktperson hos den dataansvarlige	Kontaktperson hos databehandleren
Navn:	Navn:
Stilling:	Stilling:
Telefonnummer:	Telefonnummer:
Email:	Email:

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

- [Udfyldes]

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

- [Udfyldes]

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- [Udfyldes]

Behandlingen omfatter følgende kategorier af registrerede:

- [Udfyldes]

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

- [Udfyldes]

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

[Udfyldes af den dataansvarlige]

B.2 Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
[Navn]	[CVR-nr]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]
[Navn]	[CVR-nr]	[Adresse]	[Overordnet beskrivelse af behandlingen hos underdatabehandleren]

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling end aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

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:

- [Udfyldes]

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- [Udfyldes]

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

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

C.2.1 Generelt

Sikkerhedsforanstaltningerne skal fastsættes i databehandlerens interne retningslinjer, herunder ved passende databeskyttelsespolitikker. Disse retningslinjer skal udleveres til den dataansvarlige på dennes anmodning.

Databehandleren skal påse overholdelsen af de interne retningslinjer. Retningslinjerne skal revideres mindst en gang årligt for at sikre deres fortsatte relevans og tilstrækkelighed.

Databehandleren etablerer procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

C.2.2 Databehandlerens medarbejdere

De af databehandlerens medarbejdere, der er autoriseret til at behandle data omfattet af denne aftale, skal underskrive en erklæring om tavshedspligt, som pålægger medarbejderen et straferetligt ansvar under dansk ret.

Databehandleren skal sikre, at personoplysninger omfattet af denne aftale ikke kan behandles af personer, som ikke er autoriserede hertil.

Databehandlerens medarbejdere kan ikke autoriseres til at behandle personoplysninger omfattet af denne aftale uden sikkerhedsgodkendelse efter Udlændinge- og Integrationsministeriets procedure herfor.

Databehandleren skal udarbejde og vedligeholde en udtømmende liste over medarbejdere, som er autoriseret til at behandle personoplysninger omfattet af denne aftale. Listen skal stilles til rådighed for den dataansvarlige på dennes anmodning.

Databehandleren skal instruere medarbejderne i reglerne for behandling af personoplysninger i denne aftale såvel som reglerne i persondatalovgivningen.

C.2.3 Kontrol med fysisk adgang til udstyret

Databehandleren skal sikre, at uautoriserede personer ikke kan få adgang til det behandlingsudstyr, der benyttes til behandling.

Databehandleren skal implementere og vedligeholde interne retningslinjer for anvendelse af hjemmearbejdspladser og databehandling uden for databehandlerens matrikler.

Der skal være fastsat instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af it-udstyr.

Ved reparation, service eller destruktion af udstyr, der benyttes til databehandling, skal der være foranstaltninger som sikrer, at uautoriserede personer ikke kan få adgang til data.

C.2.4 Kontrol med hjemme- og fjernarbejdspladser

Databehandleren skal sikre, at databehandlerens medarbejdere alene tilgår SIRIs personoplysninger og andre data via VPN-adgang til SIA-computer eller VIA-adgang til databehandlerens egne computere.

C.2.5 Kontrol med datamedier

Databehandleren skal sikre, at der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af datamedier.

Papirdokumenter som indeholder personoplysninger skal makuleres, når opbevaringsbehovet er ophørt.

C.2.6 Kontrol med opbevaring

Databehandleren skal sikre, at der ikke sker uautoriseret indlæsning af personoplysninger uautoriseret læsning, ændring eller sletning af opbevarede personoplysninger.

C.2.7 Brugerkontrol

Databehandleren skal sikre, at automatiske databehandlingssystemer ikke via datakommunikationsudstyr kan benyttes af uautoriserede personer.

Ved tilslutning til internettet eller andre åbne net skal der træffes foranstaltninger, som sikrer mod uvedkommende trafik og forhindrer adgang fra det åbne net til databehandlerens interne net.

C.2.8 Kontrol med dataadgangen

Databehandleren skal sikre, at personer med bemyndigelse til at anvende et automatisk databehandlingssystem kun har adgang til de personoplysninger, som er omfattet af deres adgangstilladelse.

Tildelingen af adgangsrettigheder skal være i overensstemmelse med de af databehandleren fastsatte retningslinjer herfor. Databehandleren skal på den dataansvarliges anmodning udlevere de fastsatte retningslinjer for tildeling af adgangsrettigheder.

Kun de personer hos databehandleren, der er autoriseret hertil, må have adgang til personoplysninger. Der må ikke gives adgangsrettigheder til personoplysninger i videre omfang end den pågældende bruger har et arbejdsmæssigt behov for.

Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang til persondatabehandling.

Der skal træffes særlige foranstaltninger for at sikre, at brugere med privilegerede adgangsrettigheder (herunder system- og driftsmedarbejdere) udelukkende anvender personoplysninger, som disse har et arbejdsbetinget behov for og for at sikre, at kun brugere, der har et arbejdsbetinget behov for privilegerede rettigheder, tildeles privilegerede rettigheder.

Brugeradgange skal revurderes halvårligt for at sikre, at autoriserede personer fortsat opfylder betingelserne for adgang.

Der skal føres kontrol med afviste adgangsforsøg, og der skal blokeres for yderligere forsøg efter flere på hinanden følgende afviste adgangsforsøg.

C.2.9 Kommunikationskontrol

Det skal sikres, at det er muligt at kontrollere og fastslå de modtagere, til hvilke der er blevet eller kan transmitteres eller stilles oplysninger til rådighed ved hjælp af datakommunikationsudstyr.

C.2.10 Kontrol med indlæsning og logning

Det skal sikres, at det er muligt efterfølgende at undersøge og fastslå, hvilke personoplysninger der er indlæst i automatiske behandlingssystemer, og hvornår og af hvem personoplysningerne blev indlæst.

Brugeradgange skal være personlige, og der må ikke anvendes fælleslogin til automatiske behandlingssystemer.

Databehandleren skal sikre, at følgende behandlingsaktiviteter i automatiske behandlingssystemer bliver logget:

- Indsamling
- Ændring
- Tilgang/opslag
- Videregivelse, herunder overførsel
- Samkøring

- Sletning

For så vidt angår behandlingstyperne tilgang/opslag og videregivelse, herunder overførsel, skal logningen gøre det muligt at fastlægge begrundelsen, datoen og tidspunktet for behandlingsaktiviteten og identifikation af den person, som har tilgået eller videregivet personoplysninger fra systemet, samt identiteten på modtageren af oplysningerne.

Loggene må alene anvendes til at kontrollere, om behandlingen er lovlig, til egenkontrol, til at sikre integriteten og sikkerheden af personoplysningerne.

C.2.11 Transportkontrol

Databehandleren skal sikre, at der ikke sker uautoriseret læsning, kopiering, ændring eller sletning af personoplysninger i forbindelse med overførsler af disse eller under transport af datamedier. Ved transmission over åbent net, herunder internet, tele- og faxnet, skal følgende minimumskrav overholdes:

- Data skal sikres ved passende kryptografiske kontroller. Der skal anvendes en stærk kryptering baseret på en anerkendt algoritme.
- Sikkerhed for afsenders og modtagers identitet (autenticitet) skal sikres i fornødent omfang ved anvendelse af f.eks. digital signatur eller individuelle, fortrolige adgangskoder.

C.2.12 Genopretning

Databehandleren skal sikre, at de anvendte systemer i tilfælde af teknisk uheld kan genetableres.

C.2.13 Pålidelighed og integritet

Databehandleren skal sikre, at systemet fungerer, at indtrufne fejl meldes, og at opbevarede personoplysninger ikke bliver ødelagt som følge af fejlfunktioner i systemet.

- [Udfyldes]

C.3 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

C.4 Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

- [Angiv, hvor behandlingen finder sted] [Angiv, hvilken databehandler eller underdatabehandler, der anvender adressen]
- [Angiv, hvor behandlingen finder sted] [Angiv, hvilken databehandler eller underdatabehandler, der anvender adressen]

C.5 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

- [Udfyldes – instruks og overførselsgrundlag]

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke indenfor rammerne af databehandleraftalen foretage en sådan overførsel.

C.6 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

- [Udfyldes med aftalt tilsyn, herunder tilsynets form, frekvens og evt. godkendte revisionserklæringer]

C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

- [Udfyldes med aftalt tilsyn, herunder tilsynets form, frekvens og evt. godkendte revisionserklæringer]

Bilag D Parternes regulering af andre forhold

D.1 Misligholdelse og erstatningsansvar samt administrative bøder

Den dataansvarlige og/eller databehandleren kan efter databeskyttelsesforordningens artikel 82 ifalde erstatningsansvar over for en registreret fysisk person.

Den dataansvarlige og/eller databehandleren kan efter databeskyttelsesforordningens artikel 83 blive pålagt en administrativ bøde af tilsynsmyndigheden.

For misligholdelse og erstatningsansvar i medfør af databehandleraftalen gælder dansk rets almindelige regler.

D.1.1 Der henvises til bestemmelserne om misligholdelse i hovedaftalen.

D.1.2 Der henvises til bestemmelserne om erstatning i hovedaftalen.

D.1.3 Uanset bestemmelsen i pkt. D.1.2, skal databehandleren skadesløsholde dataansvarlige, såfremt den dataansvarlige bliver mødt med krav fra tredjemand som følge af, at databehandleren i sin rolle som databehandler eller databehandlerens eventuelle underdatabehandlere i deres rolle som underdatabehandlere har overtrådt den til enhver tid gældende persondataretlige lovgivning. Databehandleren hæfter kun for skader, hvis databehandleren eller dennes eventuelle underdatabehandlere ikke har opfyldt sine forpligtelser som databehandler og/eller underdatabehandlere, som det følger af den til enhver tid gældende lovgivning, eller hvis databehandleren som databehandler eller dennes eventuelle underdatabehandlere som underdatabehandlere har undladt at følge eller handlet i strid med den dataansvarliges lovlige instruks. Forpligtelsen til at skadesløsholde den dataansvarlige er ikke omfattet af en eventuelt aftalt erstatningsmaksimering i hovedaftalen. Databehandlerens forpligtelse til at skadesløsholde den dataansvarlige efter nærværende afsnit gælder ikke for bøder pålagt den dataansvarlige i medfør af databeskyttelsesforordningens artikel 83 eller sanktioner fastlagt i Danmark i overensstemmelse med databeskyttelsesforordningens artikel 84.

D.1.4 Uanset bestemmelsen i pkt. D.1.2, skal den dataansvarlige skadesløsholde databehandleren, såfremt databehandleren bliver mødt med krav fra tredjemand som følge af, at den dataansvarlige i sin rolle som dataansvarlig har overtrådt den til enhver tid gældende persondataretlige lovgivning. Den dataansvarlige hæfter kun for skader, hvis den dataansvarlige ikke har op-

fyldt sine forpligtelser som dataansvarlig, som det følger af den til enhver tid gældende lovgivning. Forpligtelsen til at skadesløsholde databehandleren er ikke omfattet af en evt. aftalt erstatningsmaksimering i hovedaftalen. Den dataansvarliges forpligtelse til at skadesløsholde databehandleren efter nærværende afsnit gælder ikke for bøder pålagt databehandleren i medfør af databeskyttelsesforordningens artikel 83 eller sanktioner fastlagt i Danmark i overensstemmelse med databeskyttelsesforordningens artikel 84.

Bilag E Sikkerhedskrav i forbindelse med databehandling

E.1. Krav til databehandlerens sikkerhedsniveau

E.1.1 Overholdelse af relevant lovgivning

Databehandleren skal i hele aftaleperioden efterleve alle relevante sikkerhedsbestemmelser jf. såvel den dataansvarliges krav, som den til enhver tid gældende lovgivning, herunder databeskyttelsesforordningen (EU 2016/679 af 27. april 2017) samt danske love og bekendtgørelser udstedt i medfør heraf.

E.1.2 Risikovurdering

Den dataansvarlige gennemfører løbende risikovurderinger af informationssikkerheden og databeskyttelsen i den dataansvarliges projekter, processer og it-systemer og justerer på baggrund heraf løbende informationssikkerhedskravene til organisatoriske og tekniske sikkerhedskontroller til den dataansvarliges aktuelle trusselsniveau, hvorfor databehandlere må forvente at krav til informationssikkerheden og databeskyttelsen kan ændre sig i forbindelse med kontraktindgåelse i rammeaftalens periode. Ændringer af krav i relation til informationssikkerheden og databeskyttelsen til databehandleren vil bliver håndteret i overensstemmelse med databehandleraftalen.

Databehandleren er forpligtet til at deltage og afgive oplysninger i forbindelse med den dataansvarliges informationssikkerhedsmæssige risikovurdering af databehandlingen og databehandleren samt i forbindelse med privatlivsvurderinger og konsekvensanalyser for den registreredes rettigheder (PIA og DPIA). I den forbindelse er databehandleren forpligtet til i rimeligt omfang at stille ressourcer og oplysninger til rådighed for den dataansvarlige. Databehandleren er berettiget til særskilt vederlag baseret på det faktiske timeforbrug med udgangspunkt i de timepriser, der er anført i [prislisten eller hovedaftalen, angiv evt. bilagsnr.].

Databehandleren skal generelt agere proaktivt i samarbejdet med den dataansvarlige om efterlevelse af sikkerhedskravene i forbindelse med databehandlingen. Den proaktive adfærd omfatter i forhold til indeværende bilag:

- At gøre den dataansvarlige opmærksom på relevante forebyggende sikkerhedskontroller og
- At gøre den dataansvarlige opmærksom på sårbarheder i forbindelse med databehandlingen og kontroller, som databehandleren vurderer at trusler kan udnytte og dermed potentielt medføre brud på fortroligheden, integriteten og tilgængeligheden af data.

E.2. Databehandlerens styring af informationssikkerheden

E.2.1 Efterlevelse af ISO 27001:2013 eller tilsvarende

Den dataansvarlige er underlagt Statens krav om, at alle statslige institutioner skal efterleve ISO27001:2013.

Databehandleren skal derfor også efterleve ISO27001:2013 eller tilsvarende international anerkendt standard som fælles rammeværk for databehandlerens sikkerhedsstyring af informationssikkerhed. Dokumentation for dette skal udleveres til den dataansvarlige i afklaringsfasen. Så-

fremt databehandleren efterlever en tilsvarende standard skal denne redegøre for hvorledes denne tilsvarer ISO27001:2013.

E.2.2 Databehandlerens organisering af informationssikkerheden

Databehandleren skal iværksætte og opretholde de organisatoriske, administrative og tekniske it-sikkerhedskontroller til sikring af, at data ikke hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab eller misbruges. Databehandleren forpligter sig til løbende og for egne midler at holde sig opdateret om best practice inden for informationssikkerhed.

Databehandleren skal fastsætte og gennemføre interne retningslinjer for informationssikkerhed. Databehandleren skal have retningslinjer for organisatoriske forhold, logisk og fysisk sikring, herunder administration af adgangskontrolanordninger og autorisationsordninger samt kontrol af autorisationer.

E.2.3 Databehandlerens tavshedspligt

Medarbejdere hos databehandleren har tavshedspligt om den dataansvarliges information og data, som de får adgang til, og information og data må ikke videregives til uvedkommende eller anvendes til uvedkommende formål. Alle databehandlerens medarbejdere, som arbejder inden for rammerne af denne hovedaftale, skal underskrive en strafsanktioneret tavshedspligterklæring, som opfylder den dataansvarliges krav hertil.

Denne erklæring er vedlagt som bilag F til denne databehandleraftale.

E.2.4 Databehandlerens informationssikkerhedsansvarlige

Databehandleren skal udpege en ansvarlig hos databehandleren for databehandlerens informationssikkerhed i forbindelse med databehandling under hovedaftalen. Databehandleren vedlægger CV på den informationssikkerhedsansvarlige som bilag til denne databehandleraftale. Den informationssikkerhedsansvarlige skal være den dataansvarliges kontaktperson i forbindelse med dette bilags sikkerhedskrav.

E.3. Krav til sikker behandling af data

Databehandleren skal aktivt medvirke til at sikre mod uautoriseret og uvedkommende adgang til den dataansvarliges data – såvel fysisk adgang som logisk adgang, herunder også beskyttelse mod skadelig software – i henhold til internationalt anerkendte metoder og teknikker for adgangskontrol og personlig identifikation. Det skal som minimum omfatte etablering og vedligeholdelse af anti-malware, firewalls og opsætning af sikkerhedsindstillinger i systemmiljøer.

Databehandleren og dennes ansatte må ikke tilgå eller gives adgang til den dataansvarliges it-miljøer uden forudgående skriftlig aftale med den dataansvarlige.

Databehandleren er ansvarlig for at give den fornødne instruktion til medarbejdere i behandling af data.

Databehandleren skal sikre, at der er fastsat instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af it-udstyr, som behandler den dataansvarliges informationer. Instrukserne skal svare til informationernes klassifikation.

Den dataansvarlige efterlever Udlændige- og Integrationsministeriets dataklassifikationsmodel, jf. politik for klassifikation af information, og databehandleren må ikke klassificere data og informationer på en måde der medfører et lavere sikkerhedsniveau end den dataansvarliges klassifikationsmodel foreskriver. Databehandleren skal i afklaringsfasen redegøre for overensstemmelse mellem dennes klassifikationsmodel og den dataansvarliges.

E.3.1 Brug af testdata

Test på persondata må ikke ske uden den dataansvarliges forudgående skriftlige accept. Såfremt den dataansvarlige giver tilladelse til, at testdata må indeholde persondata, skal de anvendte it-miljøer hertil have etableret sikkerhedskontroller svarende til den dataansvarliges krav til produktionsmiljøer (jf. databehandleraftalen).

E.3.2 Sikring af databehandlerens udstyr

I forbindelse med reparation, service eller destruktion af udstyr og medier, der måtte indeholde overførte data tilhørende den dataansvarlige, herunder kildekode og persondata, skal databehandleren sikre, at disse ikke kommer til uvedkommendes kendskab.

E.3.3 Transmission af oplysninger

Databehandleren skal til enhver tid overholde de retningslinjer, som Datatilsynet har fastsat for transmission af persondata over internettet (Datatilsynets it-sikkerhedstekst ST4). Databehandleren skal overholde retningslinjerne for persondata såvel som for øvrige data.

Ved tilslutning til internet eller andre åbne net (som fx telefon- eller faxnet), skal databehandleren implementere foranstaltninger som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til databehandlerens interne net.

For transmission af data over åbne net skal følgende opfyldes af databehandleren:

- Transmission af data klassificeret til JM fortrolig jf. Justitsministeriets dataklassifikationsmodel skal sikres ved stærk kryptering baseret på en anerkendt algoritme.
- Sikkerhed for afsenders og modtagers identitet (autenticitet) skal sikres i fornødent omfang ved anvendelse af fx digital signatur eller individuelle, fortrolige adgangskoder.

E.3.4 Sletning af data

Databehandleren er forpligtet til at slette eller tilbagelevere data når databehandleren ikke længere har et arbejdsmæssigt behov for fortsat behandling.

Alle den dataansvarliges data skal slettes eller tilbageleveres ved hovedaftalens ophør efter nærmere aftale med den dataansvarlige.

Papirdokumentation skal makuleres, når der ikke længere er behov for at opbevare data.

Data, der opbevares digitalt, skal slettes på anerkendt måde straks efter behandlingsbehovet er ophørt. Dette gælder ikke data, som er nødvendige at opbevare for at opfylde lovgivningsmæssige krav vedrørende regnskabsaflæggelse og revision. Disse oplysninger skal opbevares i overensstemmelse med gældende lovgivning for bogføring mm.

Databehandleren forpligter sig til at sikre, at data, der skal slettes, rent faktisk bliver slettet på forsvarlig vis. Sletning skal ske i overensstemmelse med Datatilsynets it-sikkerhedstekst ST3.

Digitale databærende medier, som har været anvendt i forbindelse med databehandlerens opfyldelse af hovedaftalen, skal destrueres efter best practice. Databehandleren kan opfylde kravet ved at indhente en erklæring fra ansvarlige underleverandører, som benytte databærende medier, om at destruktion af alle databærende medier finder sted og opfylder dansk lovgivning. Relevante forhold omkring destruktionen skal fremgå af erklæringen.

Den dataansvarlige kan til en hver tid i hovedaftalens løbetid og indtil 5 år efter hovedaftalens ophør kræve dokumentation for at retmæssig sletning eller destruktion er forekommet i hovedaftalens løbetid.

E.3.5 Backup og restore

Databehandleren skal have faste retningslinjer for backup og restore. Retningslinjerne skal sikre at systemer og data kan genetableres i tilfælde af teknisk uheld eller skadevoldende handlinger. Databehandleren skal i afklaringsfasen redegøre for dennes interne retningslinjer for backup og restore. Databehandlerens retningslinjer skal understøtte at der i tilfælde af systemnedbrud mv. ikke sker tab eller forringelse af data.

E.3.6 Beredskabs- og forretningsnødplaner

Databehandleren skal have nedskrevne og efterprøvede beredskabs og forretningsnødplaner, der omfatter den dataansvarliges data. Planerne skal inkludere den dataansvarliges rettidige involvering i tilfælde af aktivering af beredskab- og forretningsnødplaner.

E.4. Adgangsstyring

E.4.1 Databehandlerens adgangsstyring

Databehandleren skal have fastsatte retningslinjer for tildeling af adgangsrettigheder. Tildeling af adgangsrettigheder skal være i overensstemmelse med databehandlerens fastsatte retningslinjer herfor. Den dataansvarlige kan til en hver tid bede om en kopi af databehandlerens fastsatte retningslinjer for tildeling af adgangsrettigheder. Følgende krav skal som minimum overholdes i forbindelse med databehandlerens interne adgangsstyring:

Kun de personer hos databehandleren, som er autoriseret hertil af den dataansvarlige, må have adgang til den dataansvarliges data. Der må ikke gives adgangsrettigheder til data i videre omfang, end den pågældende bruger har et arbejdsbetinget behov for.

Databehandleren skal sikre, at al adgang for databehandlerens medarbejdere til den dataansvarliges data og de systemer, hvor data lagres, er personhenførbar, blandt andet vha. personlige brugernavne og password. Passwords skal konstrueres i overensstemmelse med god praksis og skal være personlige og fortrolige. Databehandleren skal tilse, at adgangskontrollens sværhedsgrad afstemmes med fortroligheden og følsomheden af den dataansvarliges data.

Databehandleren skal implementere formelle procedurer for registrering og afmelding af brugere. I forbindelse med ophør, fratrædelse og omplacering til anden funktion skal databehandleren sikre, at brugernes adgange blokeres. Databehandleren skal til enhver tid kunne dokumentere,

hvem der er autoriseret til at have adgang til data, og hvilke rettigheder medarbejderne har i forhold til systemer.

E.5. Rapportering af sikkerhedshændelser

Databehandleren skal aktivt kunne medvirke til at håndhæve informationssikkerheden - tilgængelighed, integritet, fortrolighed og sporbarhed, herunder sikre at alle sikkerhedsrelaterede hændelser optegnes på en sådan form, at det kan anvendes til sikkerhedshåndhævelse.

Ved konstateret sikkerhedshændelser på informationssikkerheden eller ved mistanke herom skal databehandleren rapportere dette til den dataansvarlige. Dette gælder for sikkerhedshændelser, som påvirker informationssikkerheden for systemer der anvendes til behandling af den dataansvarliges data eller vurderes at vil have konsekvenser for disse systemer. Dokumentation af et eventuelt sikkerhedsbrud skal være uafviseligt og forelægges for den dataansvarlige.

Sikkerhedshændelser defineres som utilsigtede hændelser eller ulovlige eller ondsindede handlinger, som kompromitterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af den dataansvarliges data.

I tilfælde af, at databehandleren registrerer sikkerhedshændelser i standardprogrammel anvendt ved opfyldelse af indeværende aftale, i leverancer til andre kunder, skal den dataansvarlige informeres. Det skal ske i det omfang information om hændelsen kan bidrage til at undgå, at noget lignende sker for den dataansvarlige. Hændelsen skal anonymiseres før den formidles til den dataansvarlige.

Sikkerhedshændelser rapporteres til den dataansvarliges It-og informationssikkerhedsleder.

E.6. Revision og audit af databehandlerens informationssikkerhedskontroller

Databehandleren skal føre kontrol med, at kravene i dette bilag overholdes. Retningslinjerne skal revideres årligt for at sikre, at de stadig er tilstrækkelige og relevante.

Den dataansvarlige kan til enhver tid kræve at få indblik i databehandlerens interne retningslinjer for informationssikkerheden.

Databehandleren skal i rimelig omfang deltage i møder med den dataansvarlige om databehandlerens efterlevelse af indeværende krav til informationssikkerhed. Databehandleren er berettiget til særskilt vederlag baseret på det faktiske timeforbrug med udgangspunkt i de timepriser, der er anført i [prislisten eller hovedaftalen, angiv evt. bilagsnr.].

Databehandleren skal, på den dataansvarliges anmodning, bistå med revisionserklæringer om det samlede informationssikkerhedsniveau hos databehandleren fra en ekstern statsautoriseret revisor, baseret på internationalt anerkendt revisionsstandard ISAE3000 og/eller ISAE3402 eller tilsvarende. Den dataansvarlige forbeholder sig ret til at anmode databehandleren om at bistå med revisionserklæringer i henhold til indeværende bilag 1 gang årligt.

Omkostningerne til den eksterne statsautoriserede revisor afholdes af den dataansvarlige. Databehandleren skal vederlagsfrit yde auditor den bistand, der er nødvendig til gennemførelse af audit, herunder oplysninger om brugernavn, passwords, dokumentation, kildekode mv.

Den dataansvarlige definerer omfanget af erklæringen, som vil dække it-kontroller i relation til databehandlerens overholdelse af aftalens krav til sikkerhed, herunder til enhver tid gældende persondatalovgivning og Sikkerhedsbekendtgørelse samt ISO 27001:2013 og dennes nyeste udgave. Anvender databehandleren underleverandører til udførelse af leverancer, vil it-revision og erklæringer i relevant omfang også inkludere disse.

Den dataansvarlige er forpligtet til at varsle databehandleren om it-revisionen 10 arbejdsdage forud for opstart.

Databehandleren er forpligtet til at orientere den dataansvarlige om resultater fra databehandlerens egne interne og eksterne it-revisioner, it-audits og sikkerhedstest, hvor disse resultater omfatter systemer der anvendes til behandling af den dataansvarliges data eller kan have en konsekvens for disse systemer. Databehandleren afholder alle omkostninger til databehandlerens egne interne og eksterne it-revision og audits. Databehandleren skal vederlagsfrit udlevere generelle it-revisionserklæringer til den dataansvarlige.

Bilag F Tavshedspligterklæring

Erklæring om tavshedspligt i forbindelse med: **[INDSÆT titel og dato for hovedaftalen/opgaven]**

Undertegnede erklærer herved, at jeg er indforstået med at iagttage ubetinget tavshed med hensyn til de forhold, som jeg måtte blive bekendt med, og hvis hemmeligholdelse ifølge lovgivningen eller sagens natur er påkrævet eller bliver foreskrevet.

Jeg erklærer endvidere, at jeg er gjort bekendt med indholdet af forvaltningslovens § 27 og straffelovens §§ 144-145, §§ 147-152 f og §§ 155-157 af hvilke, der er udleveret mig et særtryk.

Jeg er indforstået med, at denne **tavshedspligt vedvarer**, uanset om den beskæftigelse, der har nødvendiggjort erklæringen, ophører.

Dato og sted:

Navn:

Underskrift:

Herved attesteres, at nærværende tavshedspligterklæring er underskrevet i min overværelse og efter, underskriveren overfor mig har udtalt, at vedkommende er gjort bekendt med indholdet af erklæringens fulde ordlyd.

Dato og sted:

Underskrift:

Forvaltningslov

§ 27. Den, der virker inden for den offentlige forvaltning, har tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til oplysninger om
1) enkeltpersoners private, herunder økonomiske, forhold og
2) tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den person eller virksomhed, oplysningerne angår, at oplysningerne ikke videregives.

Stk. 2. Den, der virker inden for den offentlige forvaltning, har desuden tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, når det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Det samme gælder, når en oplysning ved lov eller anden gyldig bestemmelse er betegnet som fortrolig, herunder når fortrolighed følger af en EU-retlig eller folkeretlig forpligtelse el.lign.

Stk. 3. Den, der virker inden for den offentlige forvaltning, har herudover tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, når det er nødvendigt at hemmeligholde en oplysning til beskyttelse af væsentlige hensyn til rigets udenrigspolitiske interesser, herunder forholdet til andre lande eller internationale organisationer.

Stk. 4. Den, der virker inden for den offentlige forvaltning, har endvidere tavshedspligt, jf. straffelovens § 152 og §§ 152 c-152 f, med hensyn til oplysninger, som det i øvrigt er nødvendigt at hemmelighol de for at varetage væsentlige hensyn til
1) forebyggelse, efterforskning og forfølgning af lovovertrædelser samt straffuldbyrdelse og beskyttelse af sigtede, vidner eller andre i sager om strafferetlig eller disciplinær forfølgning,
2) gennemførelse af offentlig kontrol-, regulerings- eller planlægningsvirksomhed eller af påtænkte foranstaltninger i henhold til skatte- og afgiftslovgivningen,
3) det offentliges økonomiske interesser, herunder udførelsen af det offentliges forretningsvirksomhed,
4) forskeres og kunstneres originale ideer samt foreløbige forskningsresultater og manuskripter eller
5) private og offentlige interesser, hvor hemmeligholdelse efter forholdets særlige karakter er påkrævet.

Stk. 5. Inden for den offentlige forvaltning kan der kun pålægges tavshedspligt med hensyn til en oplysning, når det er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til bestemte offentlige eller private interesser som nævnt i stk. 1-4.

Stk. 6. En forvaltningsmyndighed kan bestemme, at en person uden for den offentlige forvaltning har tavshedspligt med hensyn til fortrolige oplysninger, som myndigheden videregiver til den pågældende uden at være forpligtet hertil.

Stk. 7. Fastsættes der i henhold til § 1, stk. 3, regler om tavshedspligt, eller pålægges der tavshedspligt efter stk. 6, finder straffelovens § 152 og §§ 152 c-152 f tilsvarende anvendelse på overtrædelse af sådanne regler eller pålæg.

Borgerlig straffelov

§ 144. Den, der i udøvelse af dansk, udenlandsk eller international offentlig-tjeneste eller hverv uberettiget modtager, fordrer eller lader sig tilsige en gave eller anden fordel, straffes med bøde eller fængsel indtil 6 år.

§ 145. Kræver eller modtager nogen, som virker i offentlig tjeneste eller hverv, for privat vindings skyld kendelse for tjenestehandling, skat eller afgift, der ikke skyldes, straffes han med bøde eller fængsel indtil 6 år. Beholder han for privat vindings skyld sådan i god tro oppebåren ydelse efter at være blevet opmærksom på fejlen, straffes han med fængsel indtil 2 år.

§ 147. Når nogen, hvem det påhviler at virke til håndhævelse af statens straffemyndighed, derved anvender ulovlige midler for at opnå tilståelse eller forklaring eller foretager en lovstridig anholdelse, fængsling, ransagning eller beslaglæggelse, straffes han med bøde eller fængsel indtil 3 år.

§ 148. Når nogen, hvem domsmyndighed eller anden offentlig myndighed til at træffe afgørelse i retsforhold tilkommer, eller hvem det påhviler at virke for håndhævelse af statens straffemyndighed, forsætlig eller ved grov uagtsomhed undlader at iagttage den lovbestemte fremgangsmåde med hensyn til sagens eller enkelte retshandlingers behandling eller med hensyn til anholdelse, fængsling, ransagning, beslaglæggelse eller lignende forholdsregler, straffes han med bøde eller fængsel indtil 4 måneder.

§ 149. Når nogen, hvem en fanges bevogtning eller fuldbyrdelse af domme i straffesager påhviler, lader en sigtet undvige, hindrer dommens fuldbyrdelse eller bevirker, at den fuldbyrdes på mildere måde end foreskrevet, straffes han med bøde eller fængsel indtil 3 år.

§ 150. Når nogen, som virker i offentlig tjeneste eller hverv, misbruger sin stilling til at tvinge nogen til at gøre, tåle eller undlade noget, straffes han med fængsel indtil 3 år.

§ 151. Den, som tilskynder eller medvirker til, at nogen, der er underordnet vedkommende i offentlig tjeneste eller hverv, forbryder sig i denne tjeneste, straffes, uden hensyn til om den underordnede kan straffes eller på grund af vildfarelse eller af andre grunde er straffri, efter den for den pågældende forbrydelse gældende bestemmelse.

§ 152. Den, som virker eller har virket i offentlig tjeneste eller hverv, og som uberettiget videregiver eller udnytter fortrolige oplysninger, hvortil den pågældende i den forbindelse har fået kendskab, straffes med bøde eller fængsel indtil 6 måneder.
Stk. 2. Begås det i stk. 1 nævnte forhold med forsæt til at skaffe sig eller andre uberettiget vinding, eller foreligger der i øvrigt særligt skærpende omstændigheder, kan straffen stige til fængsel indtil 2 år. Som særligt skærpende omstændighed anses navnlig tilfælde, hvor videregivelsen eller udnyttelsen er sket under sådanne omstændigheder, at det påfører andre en betydelig skade eller indebærer en særlig risiko herfor.
Stk. 3. En oplysning er fortrolig, når den ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser.

§ 152 a. Bestemmelsen i § 152 finder tilsvarende anvendelse på den, som i øvrigt er eller har været beskæftiget med opgaver, der udføres efter aftale med en offentlig myndighed. Det samme gælder den, som virker eller har virket ved telefonanlæg, der er anerkendt af det offentlige.

§ 152 b. Med samme straf som efter § 152 straffes den, som udøver eller har udøvet en virksomhed eller et erhverv i medfør af offentlig beskikkelse eller anerkendelse, og som uberettiget videregiver eller udnytter oplysninger, som er fortrolige af hensyn til private interesser, og hvortil den pågældende i den forbindelse har fået kendskab.
Stk. 2. Med samme straf som efter § 152 straffes endvidere den, som virker eller har virket som ansat ved De Europæiske Fællesskabers Statistiske Kontor, eller som arbejder eller har arbejdet i kontorets lokaler, og som uberettiget videregiver eller udnytter fortrolige statistiske oplysninger, hvortil den pågældende i den forbindelse har fået kendskab.

§ 152 c. Bestemmelserne i §§ 152-152 b gælder også for de pågældende personers medhjælpere.

§ 152 d. Bestemmelserne i §§ 152-152 c finder tilsvarende anvendelse på den, som uden at have medvirket til gerningen uberettiget skaffer sig eller udnytter oplysninger, der er fremkommet ved en sådan overtrædelse.
Stk. 2. Med samme straf straffes den, der uden at have medvirket til gerningen uberettiget videregiver oplysninger om enkeltpersoners rent private forhold, jf. forvaltningslovens § 28, stk. 1, som er fremkommet ved overtrædelse af §§ 152- 152 c.
Stk. 3. På samme måde straffes den, som uden at have medvirket til gerningen uberettiget videregiver oplysninger, der er fortrolige af hensyn til statens sikkerhed eller rigets forsvar.

§ 152 e. Bestemmelserne i §§ 152-152 d omfatter ikke tilfælde, hvor den pågældende:
1) er forpligtet til at videregive oplysningen eller
2) handler i berettiget varetagelse af åbenbar almeninteresse eller af eget ellerandres tarv.

§ 152 f. Overtrædelse af §§ 152 – 152 d, hvorved der alene er krænket private interesser, er undergivet privat påtale.
Stk. 2. Offentlig påtale kan dog ske, når den forurettede anmoder herom.

§ 155. Misbruger nogen, som virker i offentlig tjeneste eller hverv, sin stilling til at krænke privates eller det offentliges ret, straffes han med bøde eller fængsel indtil 4 måneder. Sker det for at skaffe sig eller andre uberettiget fordel, kan fængsel indtil 2 år anvendes.

§ 156. Når nogen, som virker i offentlig tjeneste eller hverv, nægter eller undlader at opfylde pligt, som tjenesten eller hvervet medfører, eller at efterkomme lovlig tjenstlig befaling, straffes han med bøde eller fængsel indtil 4 måneder. Uden for foranstående bestemmelse falder hverv, hvis udførelse hviler på offentlige valg.

§ 157. Når nogen, som virker i offentlig tjeneste eller hverv, gør sig skyldig i grov eller oftere gentagen forsømmelse eller skødesløshed i tjenestens eller hvervets udførelse eller i overholdelsen af de pligter, som tjenesten eller hvervet medfører, straffes den pågældende med bøde eller fængsel indtil 4 måneder. Uden for foranstående bestemmelse falder hverv, hvis udførelse hviler på offentlige valg.