KOMBIT
Kommunernes it-fællesskab

Versionshistorik

Versionsnr.	Dato	Beskrivelse
0.8	25.11.2016	Høringsudkast til kombit.dk

DATABEHANDLERAFTALE

Mellem

[XXXX Kommune
adresse
postnr. og by
CVR. nr.: XXXX]
(herefter "Kommunen")

og

[Leverandørens navn
adresse
postnr. og by
CVR. nr.: XXXX]
(herefter "Leverandøren")

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

1. Generelt

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

(i) Bekendtgørelse nr. 528 af 15/06/2000 med senere ændringer (Sikkerhedsbekendtgørelsen).

(ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15/06/2000 (Sikkerhedsvejledningen).

(iii) [Principperne og anbefalingerne i ISO 27001 med senere ændringer, som på alle relevante områder vil finde anvendelse i det omfang andet ikke fremgår af Aftalen eller anden eller andre med relevans for Aftalen tilhørende aftale(r) mellem Kommunen og Leverandøren.] *[Punktet udtages hvis ikke relevant]*

1.2 Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen), således at Aftalens punkt 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen samt den øvrige nationale persondataretlige regulering, der indtræder som følge af ikrafttræden af Databeskyttelsesforordningen.

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

1.4 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger, og personoplysninger må alene behandles til formål, som er nødvendige for opfyldelsen af Aftalen.

2. Formål og baggrund

[Hvis Aftalen indgår som en del af en hovedaftale mellem Kommunen og Leverandøren, og hvis formålet og baggrunden er beskrevet her, da kan bilag 3 - Instruks udgå af Aftalen.]

[Hvis bilag 3 udgår, da skal det sikres, at punkt 6 indeholder en beskrivelse af formålet med behandlingerne samt en beskrivelse af instruksen.]

2.1 Leverandøren behandler personoplysninger for Kommunen jf. kontrakt af [titel og dato eller anden éntydig identifikation] hvor Leverandørens behandlinger og formålet med behandlingerne er beskrevet.

3. Kommunens forpligtelser

3.1 Kommunen har ansvaret for, at de personoplysninger, som Kommunen instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Kommunens opgavevaretagelse.

3.2 Kommunen har ansvaret for at overholde de forpligtelser, som lovgivningen jf. Aftalens punkt 1.1 og punkt 1.2 har pålagt dataansvarlig i forhold til blandt andet den registreredes rettigheder i forhold til fx krav om oplysningspligt, registreredes indsigtsret og i forhold til Sikkerhedsbekendtgørelsen.

3.3 Kommunen er forpligtet til at orientere Leverandøren i tilfælde af Kommunens eventuelle skærpede it-sikkerhedsregler, som Leverandøren ligeledes er forpligtet til at underrette underleverandører om. Leverandøren er berettiget til særskilt betaling for dokumenterede udgifter, der vil følge af sådanne skærpede tilpasninger som følge af ændringer i Kommunens eventuelle uddybende it-sikkerhedsregler, der går ud over hvad gældende lovgivning kræver, [samt hvad anbefalinger og principper for ISO-sikkerhedsstandarder eller lignende foreskriver.] *[Sætningen udtages hvis ikke relevant]*

4. Leverandørens forpligtelser

4.1 Leverandøren er databehandler for de personoplysninger, som Kommunen som dataansvarlig overlader til Leverandøren til behandling på vegne af Kommunen jf. punkt 6 og bilag 3 [eller alternativt jf. punkt 6.2].

4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks jf. punkt 6 og bilag 3 [eller alternativt jf. punkt 6.2] fra Kommunen og alene med henblik på opfyldelse af denne Aftale.

4.3 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske foranstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og bilag 1 – Sikkerhed [samt i hovedaftale jf. titel og dato eller anden éntydig identifikation mellem Leverandøren og Kommunen eller anden eller andre med relevans for Aftalen tilhørende aftale(r) jf. [titel og dato eller anden éntydig identifikation] mellem Kommunen og Leverandøren.]

4.4 Leverandøren forpligter sig herudover til at gøre sig bekendt med Kommunens it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de eventuelle dertil hørende uddybende it-sikkerhedsregler, som vedlægges Aftalen som bilag.

4.5 Leverandøren skal på opfordring fra Kommunen hjælpe Kommunen med at tilvejebringe oplysninger til brug for Kommunens besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, retning og sletning af oplysninger samt begrænsning af behandling af borgerens oplysninger.

4.6 Leverandøren skal hjælpe Kommunen med at efterleve dennes forpligtelser i medfør af Databeskyttelsesforordningens artikel 32-36, jf. artikel 28, stk. 3, litra f.

4.7 Leverandøren garanterer ved denne Aftales indgåelse at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de nødvendige tekniske og organisatoriske foranstaltninger, som på forespørgsel fra Kommunen skal kunne dokumenteres.

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

4.9 [Hvis Leverandøren opererer i en anden medlemsstat skal Leverandøren ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.] *[Punktet udtages hvis ikke relevant.]*

5. Underleverandør (underdatabehandler)

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

5.2 Leverandøren må ikke uden udtrykkeligt skriftligt samtykke fra Kommunen anvende en anden databehandler (underdatabehandler) til at behandle de personoplysninger, som Kommunen har overladt til Leverandøren i medfør af Aftalen. Leverandøren må heller ikke udskifte en underdatabehandler uden udtrykkeligt skriftligt samtykke fra Kommunen.

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

5.4 Underdatabehandleraftalen jf. punkt 5.3 skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som leverandøren er pålagt efter Aftalen, herunder at underdatabehandleren stiller garanti for at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de nødvendige tekniske og organisatoriske foranstaltninger.

5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Kommunen er dataansvarlig for, til underdatabehandlere, har Leverandøren ansvaret for underdatabehandlernes overholdelse af dennes forpligtelser.

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

5.7 Al kommunikation mellem Kommunen og underdatabehandleren sker via Leverandøren.

6. Instrukser

6.1 Leverandørens behandling af personoplysninger på vegne af Kommunen sker udelukkende efter dokumenteret instruks, jf. bilag 3 [eller alternativt jf. punkt 6.2]. Instruks fra Kommunen til en eventuel underdatabehandler jf. punkt 5.3 sker ved fremsendelse af instruksen via Leverandøren.

6.2 [*Indsæt instruks i dette punkt, herunder en beskrivelse af hvilke oplysninger Leverandøren skal behandle eller udfyld og henvis til instruks, jf. bilag 3. Hvis bilag 3 anvendes, vil punkt 6.2 udgå.]*

6.3 Leverandøren giver omgående besked til Kommunen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen jf. punkt 1.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

7.1 Leverandøren skal jf. bilag 1 træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

(i) tilintetgøres, mistes, ændres eller forringes,
(ii) kommer til uvedkommendes kendskab eller misbruges, eller
(iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1 og 1.2.

7.2 Leverandøren skal [mindst en gang årligt] [*Alt afhængig af en konkret vurdering af behandlingsrisikoen hos Leverandøren fastsættes et passende interval*] gennemgå sine interne sikkerhedsforskrifter og retningslinjer, for behandlingen

af personoplysninger, med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. punkt 7.1 samt bilag 1.

7.3 Leverandøren skal i sine retningslinjer fastsætte regler, der sikrer, at dennes ansatte kun har adgang til personoplysninger som er nødvendige for den ansattes udførelse af sine arbejdsopgaver.

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

7.5 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kommunens personoplysninger om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed jf. punkt 10.

7.6 Leverandøren er forpligtet til straks at underrette Kommunen om ethvert sikkerhedsbrud samt ved:

(i) Driftsforstyrrelser, hvis det har indflydelse på de personoplysninger, som Leverandøren behandler under denne aftale
(ii) Enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed medmindre orienteringen af Kommunen er eksplicit forbudt ved lov, fx i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,
(iii) Enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne, eller anden manglende overholdelse af Leverandørens, samt eventuelle Underdatabehandleres forpligtelser, eller enhver mistanke derom,
(iv) Øvrige hændelser jf. punkt 7.1

7.7 Underretningen jf. punkt 7.6 skal ske omgående efter konstateringen af tilfældet/tilfældene og uanset om konstateringen sker hos Leverandøren eller hos Underdatabehandleren jf. (i) – (iv).

7.8 Leverandøren må under ingen omstændigheder offentligt eller til tredjeparter kommunikere om sikkerhedsbrud jf. punkt 7.6 uden forudgående skriftlig aftale med Kommunen om indholdet af en sådan kommunikation.

8. Overførsler til tredjelande

8.1 Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande) fx via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kommunens instruks herfor jf. bilag 3 [eller alternativt punkt 6.2].

8.2 Overførsler, jf. pkt. 6.1, må kun ske med Kommunens godkendelse.

8.3 Hvis Kommunen har godkendt en overførsel, påhviler det Leverandøren at sikre, at der foreligger et gyldigt overførselsgrundlag fx Europa-Kommissionens standardkontrakter til overførsel af personoplysninger til tredjelande.

8.4 Det er Leverandørens ansvar, at de til enhver tid gældende sikkerhedsforanstaltninger, som er fastsat i lovgivningen i det land, hvor Kommunens personoplysninger overføres til, overholdes.

8.5 [*Hvis Krigsreglen jf. Persondatalovens § 41, stk. 4 finder anvendelse*: Leverandøren må ikke overføre eller tillade overførsel af personoplysninger til lande uden for Danmark. *Hvis 8.5 anvendes bortfalder punkt 8.1-8.4 og 8.5 bliver således til punkt 8.1.*]

9. Behandling udenfor Leverandørens lokaliteter

9.1 Hvis Leverandøren eller Leverandørens underdatabehandlere - når der foretages en behandling af Kommunens data - har behov for at foretage databehandling fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser) skal dette ske i overensstemmelse med Aftalens bilag 1. Behandlingen skal endvidere følge Datatilsynets retningslinjer, herunder retningslinjer vedrørende anvendelse af kryptering og digital signatur [og ellers i øvrigt følge de principper og anbefalinger, der er gældende i ISO 27001 med senere ændringer.] *[Sætningen udtages hvis ikke relevant.]*

10. Tavshedspligt og fortrolighed

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

10.2 Leverandøren skal sikre, at alle der behandler oplysninger omfattet af Aftalen herunder ansatte, tredjeparter (fx en reparatør) og underdatabehandlere

underskriver en tavshedspligtserklæring, hvorved de underlægges tidsubestemt tavshedspligt omkring oplysninger, de måtte blive bekendt med.

10.3 Leverandøren skal på opfordring fra Kommunen kunne fremsende tavshedspligterklæringer jf. punkt 10.2.

11. Kontroller og erklæringer

11.1 Leverandøren er forpligtet til uden unødigt ophold at give Kommunen tilstrækkelige oplysninger til, at Kommunen til enhver tid kan sikre sig, at der er implementeret de nødvendige og tilstrækkelige sikkerhedsforanstaltninger jf. punkt 7.1.

11.2 Leverandøren er indforstået med, at Kommunen, en repræsentant for Kommunen eller dennes revision (såvel intern som ekstern) har adgang til al nødvendig information, der vedrører indholdet i Aftalen, samt adgang til at foretage sikkerhedsrevision, få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at leverandøren overholder de krav, der følger af lovgivningen og denne Aftale.

[Kommunen skal vælge en af bestemmelserne 11.3, 11.4 eller 11.5 og herefter slette de bestemmelser, som ikke er relevante for aftalen.]

11.3 [Leverandøren skal hvert år vederlagsfrit til Kommunen fremsende en erklæring om overholdelse af punkt 7 i forbindelse med behandlingen af de omfattede personoplysninger. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder [eller efter reglerne i ISAE 3000, type 2] på området, og skal omfatte både Leverandørens og eventuelle underleverandørers databehandling. Den første erklæring skal foreligge 12 måneder efter Aftalens indgåelse.]

11.4 [Leverandøren skal efter særskilt aftale med Kommunen om indholdet af erklæringen om overholdelse af punkt 7 og Leverandørens pris herfor, fremsende en erklæring udarbejdet i forbindelse med behandlingen af de i Aftalen omfattede personoplysninger. Erklæringen skal udarbejdes i overensstemmelse med gældende anerkendte branchestandarder [eller efter reglerne i ISAE 3000 type X] på området, og skal omfatte både Leverandørens og eventuelle underleverandørers databehandling.]

11.5 [Kommunen vil [XX gang(e)] årligt foretage et tilsyn om overholdelse af punkt 7 hos Leverandøren. Omkostningerne i forbindelse med dette tilsyn afholder Kommunen selv.]

11.6 I tilfælde af, at Kommunen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion af de ovennævnte foranstaltninger, forpligter Leverandøren og Leverandørens underleverandører sig til uden yderligere omkostninger for Kommunen at stille tid og ressourcer til rådighed herfor.

12. Ændringer i Aftalen

[Kommunen skal vælge en af bestemmelserne 12.1 eller 12.2 og herefter slette den bestemmelse, som ikke relevant for aftalen.]

12.1 [Kommunen kan til enhver tid, med et forudgående varsel på mindst [30 dage], foretage ændringer i Aftalen og instruksen jf. bilag 3 i denne Aftale. Ændringerne og omkostningerne herfor aftales skriftligt mellem Kommunen og Leverandøren forinden ændringerne gennemføres. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.]

12.2 [Kommunen kan til enhver tid, med et forudgående varsel på mindst [30 dage], foretage ændringer i Aftalen og instruksen jf. bilag 3 i denne Aftale. Ændringerne og omkostningerne herfor aftales skriftligt mellem Kommunen og Leverandøren, jf. bestemmelserne om ændringshåndtering i hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.]

12.3 I det omfang ændringer i lovgivningen om behandling af personoplysninger jf. punkt 1 giver anledning til dette, er Kommunen med et varsel på [30 dage] og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen.

13. Sletning af data

13.1 Leverandøren og underdatabehandlere skal ved skriftligt påkrav herom fra Kommunen enten slette eller tilbagelevere alle personoplysninger til Kommunen efter at behandlingen af personoplysningerne i medfør af hovedaftalen mellem Leverandøren og Kommunen er ophørt.

13.2 Kommunen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af de pågældende personoplysninger.

14. Misligholdelse og tvistigheder

14.1 Reguleringen af misligholdelse og tvistigheder følger af bestemmelserne i den eller de med relevans for Aftalen indgåede aftaler om samme, og i det omfang dette ikke er reguleret, gælder de generelle regler og principper herom.

15. Erstatning og forsikring

15.1 Reguleringen af erstatnings- og forsikringsspørgsmål følger af bestemmelserne i hovedaftalen og den eller de med relevans for Aftalen indgåede aftaler om samme, og hvis det ikke er reguleret, gælder de generelle regler og principper herom.

16. Ikrafttræden og varighed

16.1 Aftalen indgås ved begge parters underskrift og løber så længe der foretages databehandling som beskrevet i Aftalen.

Aftalen underskrives eller signeres digitalt og skal foreligge elektronisk hos Kommunen og Leverandøren.

For Kommunen	For Leverandøren
Dato	Dato
_____	_____

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Underleverandører (underdatabehandlere)

[Bilag 3 – Instruks]

[Bilag 4 – Kommunens it-sikkerhedsregulativ]

[Bilag 5 – Kommunens it-sikkerhedspolitik]

[Bilag 6 – Supplerende it-sikkerhedsregler]

[Bilag 7 – Kommunens godkendelse af Leverandørens behandling i tredjelande jf. punkt 8]

Bilag 1 – Sikkerhed

[Bilag 1 udfyldes af Leverandøren. De angivne overskrifter er vejledende og bør alt afhængig af, om Leverandøren behandler personoplysninger på vegne af Kommunen indtil eller efter 24. maj 2018 suppleres, minimeres, ændres eller fjernes efter behov. De angivne tekster er således alene vejledende og SKAL suppleres og udbygges konkret i forhold til Aftalen.]

Hvis Leverandøren alene behandler personoplysninger på vegne af Kommunen indtil 24. maj 2018, skal bilag 1 indeholde en regulering, som omfattet af Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen.

Hvis Leverandøren også skal behandle personoplysninger på vegne af Kommunen fra 25. maj 2018, skal bilag 1 indeholde en regulering, som omfattet af Databeskyttelsesforordningens artikel 32.

1. Indledning

Bilag 1 indeholder en beskrivelse af de sikkerhedsmæssige krav, som Leverandøren, i medfør af Aftalen, har ansvar for at overholde eller sikre overholdelse af hos Leverandørens underleverandører jf. bilag 2.

Hvis Leverandøren ikke foretager behandling af personoplysninger i medfør af Aftalen, og hvis Leverandøren har indgået aftale med en underleverandør herom, har Leverandøren ansvaret for at pålægge Leverandørens underleverandører jf. bilag 2 at overholde Aftalens krav om sikkerhed.

Leverandøren har således ansvaret for, at Leverandøren eller Leverandørens underleverandører etablerer en række foranstaltninger, som skaber et sikkerhedsniveau, som beskrevet i bilag 1, og som passer til de aftalte behandlinger, jf. instruks bilag 3.

2. Sikkerhed

Tekniske og organisatoriske foranstaltninger fastlægges for at etablere et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. instruks i bilag 3.

Indtil 24. maj 2018 skal de tekniske og organisatoriske foranstaltninger fastlægges ud fra Sikkerhedsbekendtgørelsens regler om blandt andet administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.

Herudover skal de tekniske og organisatoriske foranstaltninger fastlægges ud fra Sikkerhedsbekendtgørelsens regler om instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinjer for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Fra 25. maj 2018 skal foranstaltningerne fastlægges ud fra overvejelser om:

1. hvad der kan lade sig gøre rent teknisk

2. implementeringsomkostningerne

3. den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen, bilag 3

4. den risiko, der er forbundet med behandlingerne, herunder risikoen for:

a) tilintetgørelse af oplysningerne

b) tab af oplysningerne

c) ændring af oplysningerne

d) uautoriseret videregivelse af oplysningerne

e) uautoriseret adgang til oplysningerne

f) konsekvenserne for borgerne ved et lavere sikkerhedsniveau

Eksempler på foranstaltninger kan være:

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. Systemoverblik og dataflow (gerne også grafisk)

[Indsættes]

4. Organisatorisk sikkerhed

I det følgende redegøres der i relevant omfang for de organisatoriske forhold herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer.

[Indsættes]

5. Sikkerhedsforanstaltninger

I det følgende redegøres for de sikkerhedsforanstaltninger, som er fastlagt for systemet.

[Indsættes]

a. Fysisk sikkerhed

- Servertyper
- Placering af servere
- Fysisk inspektion og kontakt

b. Netværkssikkerhed

c. [Applikationssikkerhed]

d. [Dataafgrænsning]

6. Autorisationer og adgangskontrol

I det følgende redegøres for procedurer og kontroller, der sikrer, at:

a. kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.

b. der kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

c. der alene autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

d. kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

[Indsættes]

7. Logning, audits og rapporter

Der skal foretages maskinel registrering (logning) af behandlinger af fortrolige personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Kravet om logning finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Kravet om logning finder ej heller anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en

forud defineret massebehandling af personoplysninger (»batch«-kørsler). Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Kravet om logning finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Kravet finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger.

8. Kontrol med afviste adgangsforsøg

Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i myndigheden.

Bilag 2 – Underleverandører (underdatabehandlere)

Her angiver Leverandøren oplysninger om underleverandører, som er godkendt af Kommunen jf. punkt 5.2 i Aftalen.

1. **Lokation(er) for behandlingen.** (*Skal oplyses af databehandleren, uanset om denne benytter sig af underdatabehandlere eller ej*)
   [Indsættes]
2. **[Angivelse af underleverandører]**

   [Navn, adresse, cvr mm på underleverandører]

Bilag 3 – Instruks

Instruks
Kommunen instruerer hermed Leverandøren og Leverandørens eventuelle underdatabehandler om at foretage følgende behandlinger.

På anmodning fra følgende:

- [Navn på myndighed(er)]
- [Navn på leverandør eller anden part]

Til nævnte til brug for drift/levering af følgende ydelser/løsning:

- [Beskrivelse af løsningen jf. Aftalens punkt 2.1]

1.1 Behandlingens betegnelse og formål

Indsæt en beskrivelse af formålet med behandlingen af personoplysninger.

1.2 [Udfasning af nuværende it-system

I forbindelse med udfasning af [tidligere system] sker der desuden en behandling af personoplysninger fra eksisterende systemer [XX].

Data flyttes fra eksisterende systemer til det nye System via [en sikret FTP-forbindelse].]

1.3 Generel beskrivelse

Beskriv de typer af behandling, som vil indgå, herunder processer, varigheden, tidsfrister for sletning og karakteren af behandlingen.

1.4 Oplysningernes følsomhed (kategorier af personoplysninger)

[Behandlingerne indeholder følsomme oplysninger (pdl § 7)/semifølsomme oplysninger (pdl § 8)/almindelige personoplysninger (pdl § 6). Leverandøren bør afspejle oplysningernes følsomhed i niveauet for behandlingssikkerheden, jf. bilag 1.]

[Indsættes]

☐ Racemæssig eller etnisk baggrund (artikel 9)
☐ Politisk overbevisning (artikel 9)
☐ Religiøs overbevisning (artikel 9)
☐ Filosofisk overbevisning (artikel 9)
☐ Fagforeningsmæssige tilhørsforhold (artikel 9)
☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v. (artikel 9)
☐ Seksuelle forhold (artikel 9)

1.5 Behandles der andre oplysninger om enkeltpersoners rent private forhold

☐ Strafbare forhold (artikel 10)
☐ Foreningsmæssige forhold (artikel 9)
☐ Væsentlige sociale problemer (§ 8)
☐ Andre forhold, som ikke er nævnt under punkt 1.4.

_____

_____

1.6 Der behandles oplysninger om følgende kategorier af registrerede (fx borgere, elever, kontanthjælpsmodtagere mm)

A) [Indsæt kategori af personer]

B) [Indsæt kategori af personer]

C) [Indsæt kategori af personer]

1.7 [Tredjelande (ikke medlemslande)

Kommunens godkendelse jf. Aftalens punkt 8 vedlægges Aftalen som bilag [4]

Der påtænkes overført oplysninger til tredjelande:

☐ Nej

☐ Ja, overførelsen sker med følgende formål jf. punkt 8:]
