Bilag 1

Databehandleraftalen

§ 1. Denne databehandleraftale finder anvendelse for det fælles offentlige IT samarbejde mellem kommunerne og Grønlands Selvstyre.

§ 2. Dette dokument er det retligt bindende dokument i medfør af § 42, stk. 2 i anordning om ikrafttræden for Grønland af lov om behandling af personoplysninger (persondataanordningen).

Udpegning af databehandler

§ 3. Inussuk IT er databehandler for det for det fælles offentlige IT samarbejde mellem kommunerne og Grønlands Selvstyre.

Stk. 2. Inussuk IT offentliggør en liste over IT-systemer omfattet af denne databehandleraftale på deres hjemmeside.

Dataansvarlig og databehandler

§ 4. De enkelte myndigheder er selvstændigt dataansvarlige for behandlingen af de personoplysninger, som myndigheden behandler i alle de IT-systemer, de benytter, herunder de fælles IT-systemer.

Stk. 2. Den dataansvarlige skal træffe de organisatoriske og tekniske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven jf. persondataanordningens § 41, stk. 2 og sikkerhedsbekendtgørelsen.

§ 5. Databehandleren og de dataansvarlige er hver især underlagt de opgaver og ansvar, der følger af persondataanordningens og sikkerhedsbekendtgørelsens generelle regler om den dataansvarlige og databehandleren, navnlig persondataanordningens §§ 41-42, med de præciseringer, der følger af dette cirkulære.

§ 6. Databehandlerens behandling kan blandt andet omfatte følgende typer af personoplysninger:

1) Almindelige personoplysninger.
2) Særlige kategorier af personoplysninger (følsomme personoplysninger).
3) Personnumre.
4) Oplysninger om strafbare forhold.

Stk. 2. Databehandlerens behandling vedrører flere typer af registrerede personer, blandt andet borgere og medarbejdere. Oplysninger om de registrerede personer fremgår af indholdet

i og metadata tilknyttet de data, som dataansvarlige myndigheder behandler i fælles IT-systemer.

Databehandleren handler efter instruks

§ 7. Databehandleren er berettiget og forpligtet til at træffe beslutning om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige sikkerhedsniveau omkring behandling af personoplysninger.

Stk. 2. Databehandleren skal fastsætte procedurer, der skal sikre IT-systemernes vedvarende fortrolighed, integritet, tilgængelighed og robusthed.

Stk. 3. Databehandleren må behandle personoplysninger i forbindelse med sikring af IT-systemernes fortrolighed, integritet, tilgængelighed og robusthed.

Stk. 4. Databehandleren underretter den dataansvarlige, hvis en instruks efter databehandlerens vurdering er i strid med persondataanordningen, sikkerhedsbekendtgørelsen eller anden lovgivning, herunder IT-sikkerhedsstandarder fastsat i IT- og informationssikkerhedspolitikken og god data skik.

Stk.5. Databehandlerens behandling af personoplysninger på vegne af centraladministrationens myndigheder er ikke tidsbegrænset, men varer indtil cirkulæret ophæves.

Stk. 6. Databehandleren kan videregive metadata fra fælles IT-systemer til brug for udførelse af f.eks. statistiske eller videnskabelige undersøgelser, jf. persondataanordningens § 10, når den rekvirerende aktør efter lovgivningen har hjemmel og de fornødne tilladelser til, at videregivelse af personoplysninger til sådanne formål kan ske.

Stk. 7. I forbindelse med videregivelser i henhold til stk. 6, bliver databehandleren selvstændig dataansvarlig for de videregivne personoplysninger, og databehandleren er ansvarlig for at sikre, at der er en gyldig hjemmel til videregivelsen.

Fortrolighed og tavshedspligt

§ 8. Databehandleren skal sikre, at de personer, der autoriseres til at behandle personoplysninger i fælles IT-systemer har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

Stk. 2. Databehandleren skal ligeledes sikre, at krav om fortrolighed er underlagt en passende lovbestemt tavshedspligt i skriftlige databehandleraftalen med leverandører, og at dette krav også videreføres i databehandleraftaler til underleverandører.

Behandlingssikkerhed

§ 9. For fælles IT-systemer instrueres databehandleren i at træffe alle de fornødne tekniske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Stk. 2. Databehandleren instrueres i at fastsætte retningslinjer for tekniske sikkerhedsforanstaltninger. Herunder:

1) Login- og autentifikationskrav til sikker adgang til IT-systemerne
2) Backup
3) Logning af IT-systemer
4) Procedure for softwareinstallationen af IT-systemer

Stk. 3. Databehandleren skal fastsætte retningslinjer for tekniske sikkerhedsforanstaltninger vedrørende centraladministrationens pc-arbejdsstationer. Herunder:

1) Sikkerhedsopdatering af centraladministrationens udleverede pc-arbejdsstationer
2) Brugernes adgang til at fastlægge og installere softwareinstallationer

Stk. 4. Databehandleren sikrer herved, at der gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau under hensyntagen til:

1) Det aktuelle tekniske niveau
2) Implementeringsomkostningerne
3) Den pågældende behandlingskarakter, -omfang, -sammenhæng og -formål
4) Risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Stk. 4. På baggrund af resultatet af den risikovurdering, som databehandleren har gennemført, gennemfører databehandleren passende foranstaltninger for at imødegå de identificerede risici. Der kan alt efter, hvad der er relevant, være tale om følgende foranstaltninger:

1) Kryptering af personoplysninger.
2) Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester.
3) Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse.
4) En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 5. Databehandleren fastsætter nærmere interne bestemmelser, i eget informationssikkerhedsledelsessystem, om sikkerhedsforanstaltninger i databehandlingen, der navnlig skal omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af IT-udstyr. Desuden skal der fastsættes retningslinjer for tilsynet med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for databehandlingen.

1) De interne bestemmelser gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos databehandleren.
2) Databehandleren giver den fornødne instruktion til egne medarbejdere, som behandler personoplysninger. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af stk. 4.

3) På steder, hvor der foretages behandling af personoplysninger, træffes der forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

Stk. 6. Databehandleren er ansvarlig for iagttagelse af reglen om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forhold til udvikling, drift, vedligeholdelse og forvaltning af fælles IT-systemer.

Autorisation og adgangskontrol

§ 10. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.

Stk. 2. Der må kun autoriseres personer, der beskæftiger sig med de formål, hvortil personoplysningerne behandles. De enkelte personer må ikke autoriseres til anvendelser, som de ikke har behov for.

Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

Stk. 4. Der træffes foranstaltninger for at sikre, at kun autoriserede personer kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Stk. 5. Autorisationer, jf. stk. 1, skal angive, i hvilket omfang brugeren må forespørge, eksportere, indføre eller slette personoplysninger.

Stk. 6. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i stk. 1-4.

Stk. 7. Kontrol i medfør af stk. 6 skal foretages mindst én gang hvert halve år.

Stk. 8. Databehandlerne instrueres i at fastsætte retningslinjer for oprettelse, ændring og ophør af autorisationer til personer til IT-systemer.

Godkendelse af underdatabehandlere

§ 11. Databehandleren har generel godkendelse til at anvende underdatabehandlere til fælles IT-systemer, herunder at indgå nødvendige dataoverførelsesaftaler med dem. Planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere offentliggøres på centraladministrationens intranet.

Stk. 2. Ved anvendelse af underdatabehandlere er databehandleren ansvarlig for at efterleve kravene i persondataanordningens afsnit IV. Databehandleren er herefter blandt andet forpligtet til:

1) Alene at anvende underdatadatabehandlere, der kan stille de fornødne garantier for, at de gennemfører de passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i persondataanordningen og sikrer beskyttelse af den registreredes rettigheder.

2) At sikre at der foreligger en gyldig underdatabehandleraftale mellem databehandleren og en eventuel underdatabehandler.

Anvendelse af underdatabehandlere

§ 12. Databehandlerens underdatabehandlere til fælles IT-systemer vil fremgå på centraladministrationens intranet. Oplysninger om underdatabehandlere kan fremsendes til centraladministrationens myndigheder efter skriftlig anmodning herom til den relevante databehandler.

Stk. 2. Databehandleren sørger for at pålægge underdatabehandlere de samme databeskyttelsesforpligtelser, som dem, der er fastsat ved dette cirkulære, gennem en kontrakt eller andet retligt bindende dokument, 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 persondataanordningen.

Stk. 3. 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, dette cirkulære og centraladministrationens informationssikkerhedspolitik.

Stk. 4. Databehandleren fører tilsyn med underdatabehandlerens overholdelse af underdatabehandleraftalen. De dataansvarlige har ikke mulighed for at føre tilsyn direkte med underdatabehandleren uden databehandlerens forudgående skriftlige godkendelse.

Stk. 5. Databehandlerens tilsyn med underdatabehandlere udføres blandt andet ved at:

1) Underdatabehandleren én gang årligt skal indhente en revisionserklæring fra en uafhængig revisor angående underdatabehandleren og dennes eventuelle underdatabehandleres behandling af informationssikkerhed og personoplysninger i medfør af den til enhver tid gældende underdatabehandleraftale. Databehandleren modtager revisionserklæringen fra underdatabehandleren, hvorefter den stilles til rådighed for de dataansvarlige myndigheder.
2) Databehandleren, eller en uafhængig revisor bemyndiget af databehandleren, har ret til at foretage inspektioner af underdatabehandlerens fysiske faciliteter, hvor der behandles personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt underdatabehandleren har truffet de sikkerhedsforanstaltninger, der følger af underdatabehandleraftalen samt gældende databeskyttelsesret.
3) Databehandleren har løbende mulighed for at indhente informationer baseret på resultaterne af enten revisionserklæringen, inspektionen af de fysiske faciliteter eller de modtagende informationer. Når der er behov for det, er databehandleren forpligtet til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af gældende databeskyttelsesret.
4) Underdatabehandleren skal give myndigheder, eller deres udpegede repræsentanter, der i henhold til databeskyttelsesreglerne har ret til adgang til databehandlerens og underdatabehandlerens faciliteter, adgang til underdatabehandlerens fysiske faciliteter mod forevisning af behørig legitimation.

Stk. 6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for de dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

Overførsel af personoplysninger til tredjelande

§ 13. Databehandleren må ikke overføre personoplysninger til tredjelande, herunder anvende underdatabehandlere i tredjelande, uden godkendelse fra den dataansvarlige. Hvis den dataansvarlige godkender en sådan overførsel skal kapitel 7 i persondataanordningen samtidig overholdes.

Bistand til den dataansvarlige

§ 14. 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 er fastlagt i persondataanordningens kapitel 9 og 10.

Stk. 2. Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den i dens rolle som dataansvarlig skal sikre overholdelsen af nedenstående regler i persondataanordningen:

1) Oplysningspligten ved indsamling af personoplysninger hos den registrerede, jf. § 28.
2) Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede, jf. § 29.
3) Den registreredes indsigtsret, jf. § 31.
4) Retten til begrænsning af behandling, jf. § 35.
5) Retten til indsigelse, jf. § 36.
6) Retten til berigtigelse, sletning og blokering, jf. § 37, stk. 1.
7) Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling, jf. § 37, stk. 2.

Stk. 3. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af persondataanordningens afsnit IV og sikkerhedsbekendtgørelsen under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren. Dette indebærer, at databehandlerens under hensyntagen til behandlingens karakter skal bistå den enkelte dataansvarlige i forbindelse med, at denne skal sikre overholdelsen af:

1) Forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen.
2) Forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter at den enkelte dataansvarlige er blevet bekendt med bruddet, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
3) 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.
4) Forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, og forpligtelsen til at høre Datatilsynet inden behandling, hvis en

konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den enkelte dataansvarlige for at begrænse risikoen.

Underretning om brud på persondatasikkerhed til Datatilsynet

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

Stk. 2. Databehandlerens underretning til den dataansvarlige skal ske uden unødig forsinkelse og om muligt senest indenfor 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til Datatilsynet. Den dataansvarlige underretter de registrerede om bruddet på persondatasikkerheden.

Stk. 3. Databehandleren kan på vegne af samtlige dataansvarlige omfattet af dette cirkulære, under hensyn til sagens karakter, bruddets omfang og såfremt bruddet omfatter et fælles IT-system, foretage en samlet anmeldelse til Datatilsynet.

Stk. 4. I overensstemmelse med stk. 1 skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til Datatilsynet. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, der skal fremgå af den dataansvarlige anmeldelse af bruddet til Datatilsynet:

1) 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.
2) De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
3) 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.

Sletning af personoplysninger

§ 16. Databehandleren fastsætter sletteregler for fælles IT-systemer.

Stk. 2. Fælles IT-systemer der er omfattet af afleveringspligt efter arkivlovens bestemmelser må tidligst slettes efter, at der er blevet afleveret til National Arkivet.

Tilsyn og revision

§ 17. Det departement, der har databehandleren tildelt i dets ressortområde, jf. cirkulære om fordeling af anliggender (Ressortfordelingen), fører tilsyn med databehandler på vegne af de dataansvarlige. Departementet udarbejder en tilsynsrapport på baggrund af deres tilsyn, der stilles til rådighed for de dataansvarlige.

Stk. 2. De dataansvarlige har ikke mulighed for at foretage inspektioner af databehandlerens fysiske faciliteter af ressourcemæssige og sikkerhedsmæssige grunde. Databehandlerne udarbejder i stedet en redegørelse om databehandlingen.

Stk. 3. Databehandlerne stiller oplysninger, der er relevante og nødvendige for at påvise overholdelse af kravene i cirkulæret, til rådighed for de dataansvarlige, herunder oplysninger vedrørende underdatabehandlere.

Orientering af den anden part

§ 18. Databehandlerne og de dataansvarlige orienterer hinanden om væsentlige forhold, der har betydning for den behandling, der er omfattet af dette cirkulære.