LOGNING AF ELEKTRONISK SAGSBEHANDLING OG BORGERES ADGANG TIL INDSIGT I OPLYSNINGER

BILAGSRAPPORT

BORGERRÅDGIVERENS EGEN DRIFT-UNDERSØGELSER

KØBENHAVNS KOMMUNE

INDHOLDSFORTEGNELSE

BILAG 1 – BORGERRÅDGIVERENS OBSERVATIONER OG VURDERINGER

LOGNING AF KØBENHAVNS BORGERSERVICES ELEKTRONISKE SAGSBEHANDLING

Ifølge persondatalovens § 41, stk. 3, har Københavns Kommune ansvaret for, at de personoplysninger, som behandles af Københavns Kommune, er beskyttet med fornødne sikkerhedsforanstaltninger.

De nærmere sikkerhedsforanstaltninger er udmøntet i sikkerhedsbekendtgørelsen. Ifølge sikkerhedsbekendtgørelsens § 18 skal der foretages registrering af alle afviste adgangsforsøg til it-systemer, hvori der behandles følsomme personoplysninger, og der skal løbende ske opfølgning. Ifølge sikkerhedsbekendtgørelsens § 19 skal der foretages logning af alle anvendelser af personoplysninger. Reglerne har til formål at forebygge og forhindre misbrug af følsomme personoplysninger i forbindelse med elektronisk sagsbehandling.

Udover ovenstående lovbestemmelser følger det af Datatilsynets udtalelse af 26. juni 2006 (j. nr. 2006-329-0022), at kommuner, der etablerer borgerservicecentre, løbende skal foretage stikprøvekontrol af loggen i it-systemer, hvori der behandles følsomme personoplysninger, i et omfang der opfylder Datatilsynets minimumskrav, som er nærmere beskrevet i publikationen Datasikkerhed i borgerservicecentre – regler og praksis.

Regulativ for it-sikkerhed i Københavns Kommune indeholder bestemmelser om de interne organisatoriske forhold i relation til ansvaret for it-sikkerhedsforanstaltninger.

Siden Borgerrepræsentationen den 16. december 2010 godkendte det daværende Regulativ for it-sikkerhed i Københavns Kommune, har regulativet indeholdt bestemmelser om, at det påhviler It-sikkerhedsfunktionen i Koncernservice (herefter Koncern IT) at føre dagligt tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser, og om, at It-sikkerhedsfunktionen har en rådgivnings- og vejledningsfunktion i relation til it-sikkerhed.

Det er de enkelte forvaltninger, der har ansvaret for at iværksætte og kontrollere sikkerhedsforanstaltninger i forhold til deres egne it-systemer, hvis forvaltningerne selv har anskaffet systemet og udpeget en systemejer inden for egen forvaltning. Forvaltningerne har derimod ikke ansvaret for fælles it-systemer, hvis der er udpeget en systemejer i Koncern IT for det pågældende system.

Det følger af Regulativ for it-sikkerhed i Københavns Kommune, at systemejeren bl.a. har ansvaret for at sikre, at it-systemets funktionalitet og anvendelse understøtter it-sikkerhedskravene, herunder at it-systemet lever op til kravene i it-sikkerhedshåndbogen, og at it-systemet kan logge behandling af data, når dette er påkrævet. Det følger videre af de uddybende it-sikkerhedsregler for Københavns Kommune, at der løbende skal ske opfølgning på registrering af afviste adgangsforsøg til it-systemer, hvor der behandles følsomme personoplysninger, herunder løbende opfølgning på loggen af behandling af følsomme personoplysninger.

Det er min opfattelse, at det følger af ansvarsuddelegeringen efter Regulativ for it-sikkerhed i Københavns Kommune, at det påhviler den til en hver tid værende systemejer i forhold til de enkelte it-systemer, som anvendes til behandling af følsomme personoplysninger, at foretage løbende opfølgning på registrering af afviste adgangsforsøg, herunder løbende opfølgning på loggen af behandlingen af følsomme personoplysninger.

Kultur- og Fritidsforvaltningen har i brev af 5. oktober 2015 oplyst, at Københavns Borgerservice alene behandler følsomme personoplysninger i it-systemet KMD Sag. I Kultur- og Fritidsforvaltningens høringsbemærkninger af 28. april 2017 til Borgerrådgiverens foreløbige rapport I har for-

valtningen korrigerende oplyst, at Københavns Borgerservice anvender i alt 14 forskellige it-systemer, hvori der behandles fortrolige og følsomme personoplysninger (se oversigten i afsnit 2 i Borgerrådgiverens rapport).

Opfølgning på registrering af afviste adgangsforsøg til it-systemerne i Københavns Borgerservice

På baggrund af de oplysninger, som jeg har modtaget fra forvaltningerne, må jeg lægge til grund, at der er foretaget opfølgning på registrering af Københavns Borgerservices afviste adgangsforsøg til it-systemerne KMD Sag, CPR og ID-Port, i overensstemmelse med sikkerhedsbekendtgørelsens § 18.

Jeg kan på baggrund af det modtagne materiale fra forvaltningerne ikke vurdere, om der er foretaget opfølgning på registrering af Københavns Borgerservices afviste adgangsforsøg til de øvrige it-systemer.

Logning af søgninger i it-systemet Notus Kommunal, sygesikring

Kultur- og Fritidsforvaltningen har i svar af 5. oktober 2015 på Borgerrådgiverens opfølgende spørgsmål oplyst, at Notus Kommunal, sygesikring, ikke logger søgninger.

Søgninger på personer i Notus Kommunal, sygesikring, kan efter min opfattelse resultere i fremsøgning af fortrolige eller følsomme personoplysninger, hvilket efter min opfattelse skal logges i overensstemmelse med sikkerhedsbekendtgørelsens § 19.

Jeg finder det på baggrund af ovenstående tvivlsomt, om loggen i Notus Kommunal, sygesikring, opfylder sikkerhedsbekendtgørelsens § 19.

Jeg har noteret mig, at Kultur- og Fritidsforvaltnings i notat af15. september 2017 har oplyst, at forvaltningen efter at have modtaget Borgerrådgiverens foreløbige rapport II i juni 2017 har anskaffet et logningsmodul til it-systemet Notus Kommunal, sygesikring, som gør det muligt at logge søgninger på personer i it-systemet.

Stikprøvekontrol (opfølgning) af loggen af Københavns Borgerservices behandling af personoplysninger i it-systemerne

Der er uoverensstemmende oplysningerne i Kultur- og Fritidsforvaltningens svar af 5. oktober 2015 på Borgerrådgiverens opfølgende spørgsmål, Kultur- og Fritidsforvaltningens høringsbemærkninger af 28. april 2017, herunder forvaltningens notater af henholdsvis 15. september 2017 og 2. oktober 2017 om, hvilke it-systemer Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger.

Kultur- og Fritidsforvaltningens svar om anvendte it-systemer giver indtryk af, at Kultur- og Fritidsforvaltningen ikke har haft et fornødent overblik over, hvilke it-systemer Københavns Borgerservice anvender til behandling af fortrolige for følsomme personoplysninger.

Jeg har noteret mig, at Kultur- og Fritidsforvaltningens i notat af 2. oktober 2017 har oplyst, at forvaltningen gennemgår hele systemporteføljen med henblik på at sikre, at forvaltningen fremadrettet er complient på stikprøvekontrolområdet.

KMD Sag

Min undersøgelse viser, at der har været udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag indtil den 31. december 2014. Koncern IT har oplyst, at der siden den 1. januar 2015 efter aftale med Socialforvaltningen har været udpeget en systemejer i Koncern IT til it-systemet KMD Sag.

Ved mit iværksættelsesbrev af 8. august 2014 til Kultur- og Fritidsforvaltningen stillede jeg spørgsmål til, hvordan der foretages opfølgning på registrering af afviste adgangsforsøg i it-systemer, hvori Københavns Borgerservice behandler fortrolige og følsomme personoplysninger, og hvordan der foretages opfølgning på loggen af behandlingen af fortrolige og følsomme personoplysninger i sådanne it-systemer.

Kultur- og Fritidsforvaltningen oplyste bl.a. i høringssvar af 16. september 2014, at det kun er ved konkrete mistanker, at der sammen med leverandøren og Koncern IT afdækkes faktiske forløb i enkeltsager. Kultur- og Fritidsforvaltningen henviste i høringssvaret til, at It-sikkerhedslederfunktionen i Koncern IT bør foretage stikprøvekontroller.

Jeg forstår høringssvaret af 16. september 2014 fra Kultur- og Fritidsforvaltningen således, at forvaltningen henviser til processen efter it-sikkerhedshåndbogen om bestilling af it-sikkerhedsrapporter ved begrundet mistanke til en medarbejder om misbrug og strafbare forhold. Jeg forstår herudover svaret således, at forvaltningen henviser til It-sikkerhedsfunktionens mulighed for at føre tilsyn med forvaltningernes it-sikkerhedsforanstaltninger. På baggrund af høringssvaret er det mit indtryk, at Kultur- og Fritidsforvaltningen på tidspunktet for høringssvaret ikke havde kendskab til, at det påhvilede systemejeren i Socialforvaltningen at foretage opfølgning på registrering af afviste adgangsforsøg og opfølgning på loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag.

Ved iværksættelsesbrev af 7. juli 2016 overførte jeg undersøgelsen vedrørende logning af elektronisk sagsbehandling til Socialforvaltningen og stillede spørgsmål vedrørende opfølgning på registrering af afviste adgangsforsøg samt opfølgning på loggen som i mit tidligere brev til Kultur- og Fritidsforvaltningen.

Socialforvaltningen oplyste i høringssvaret af 12. august 2016, at der ikke er udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag. Forvaltningen henviste til systemejer i Koncern IT.

På baggrund af Socialforvaltningens svar er det mit indtryk, at Socialforvaltningen på tidspunktet for høringssvaret ikke havde kendskab til, at det påhvilede den daværende systemejer i Socialforvaltningen til it-systemet KMD Sag at foretage stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag.

Sammenholdt giver høringssvarene fra Kultur- og Fritidsforvaltningen og Socialforvaltningen indtryk af, at der ikke har været et samarbejde mellem forvaltningerne i forhold til opgaven med stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag.

På baggrund af svarene fra Kultur- og Fritidsforvaltningen og Socialforvaltningen må jeg lægge til grund, at der i perioden, hvor der har været udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag, ikke er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af følsomme personoplysninger i it-systemet KMD Sag er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af følsomme personoplysninger i it-systemet KMD Sag i Københavns Borgerservice i perioden, hvor der har været udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag, ikke er blevet identificeret..

Ved iværksættelsesbrev af 15. august 2016 overførte jeg undersøgelsen vedrørende logning af elektronisk sagsbehandling til Økonomiforvaltningen og stillede spørgsmål vedrørende opfølgning

på registrering af afviste adgangsforsøg og opfølgning på loggen som i mit brev til Kultur- og Fritidsforvaltningen samt Socialforvaltningen.

Økonomiforvaltningen oplyste bl.a. i høringssvar af 5. september 2016, at der på baggrund af It-sikkerhedsfunktionens vejledning vedrørende "Krav om stikprøver af loggen i borgerservicecentre" og It-sikkerhedsfunktionens senere udarbejdede best practice "for gennemførelse af stikprøvekontrol af loggen" er gennemført en række stikprøvekontroller af Københavns Borgerservices medarbejderes anvendelse af bl.a. it-systemet KMD Sag.

Jeg rettede telefonisk henvendelse til Koncern IT den 10. februar 2017 og stillede opfølgende spørgsmål vedrørende antallet af foretagne stikprøvekontroller af Københavns Borgerservice behandling af følsomme personoplysninger i it-systemet KMD Sag, og jeg bad om en status vedrørende SIEM-systemet. Koncern IT svarede, at Koncern IT har kendskab til to udførte stikprøvekontroller i Københavns Borgerservice vedrørende medarbejdernes anvendelse af it-systemet KMD Sag, og at der herudover er kendskab til et enkelt tilfælde, hvor Københavns Borgerservice har bestilt en it-sikkerhedsrapport på baggrund af en konkret mistanke om misbrug.

Økonomiforvaltningen har i høringsbemærkningerne af 6. juli 2017 oplyst, at den automatiske logopfølgning tilknyttet it-systemet KMD Sag nu er i stabil drift, og at regelmæssig opfølgning med rapporter til systemejer vil blive igangsat i eftersommeren 2017.

Kultur- og Fritidsforvaltningen har i høringsbemærkninger af 9. august 2017 oplyst, at Kultur- og Fritidsforvaltningen fra december 2015 har foretaget stikprøvekontroller.

På baggrund af svarene fra Økonomiforvaltningen, Koncern IT og Kultur- og Fritidsforvaltningen må jeg lægge til grund, at der først blev foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag fra december 2015.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag indtil december 2015 er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Det er uklart, hvor hyppigt der er foretaget stikprøvekontroller fra december 2015, indtil det er blevet muligt at foretage automatiseret logopfølgning i it-systemet KMD Sag i eftersommeren 2017. Jeg lægger vægt på, at der er uoverensstemmelse mellem Økonomiforvaltningens og Kultur- og Fritidsforvaltningens oplysninger om hyppigheden af stikprøvekontroller i den ovenfor anførte periode.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemet KMD Sag ikke er blevet identificeret igennem en årrække, fordi der alene er sket logopfølgning i tilfælde af konkret mistanke om misbrug.

CPR

Der er udpeget en systemejer i Kultur- og Fritidsforvaltningen til it-systemet CPR.

Jeg har ved telefoniske opkald af 8. og 11. september 2017 til Kultur- og Fritidsforvaltningen, herunder ved e-mail af 27. september 2017 stillet opfølgende spørgsmål om foretagne stikprøvekontroller i it-systemerne ved Københavns Borgerservice.

Det fremgår af Kultur- og Fritidsforvaltningens notat af 2. oktober 2017, at der først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CPR fra 2015.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CPR indtil 2015 er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemet CPR ikke er blevet identificeret igennem en årrække, fordi der alene er sket logopfølgning i tilfælde af konkret mistanke om misbrug.

KMD Social Pension og kørekortsregisteret
Der er udpeget en systemejer i Kultur- og Fritidsforvaltningen til it-systemerne KMD Social Pension og kørekortsregisteret.

Det fremgår af Kultur- og Fritidsforvaltningen notat af 2. oktober 2017, at der først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Social Pension og kørekortsregisteret fra 2016.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Social Pension og kørekortsregisteret indtil 2016 er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemerne KMD Social Pension og kørekortsregisteret ikke er blevet identificeret igennem en årrække, fordi der alene er sket logopfølgning i tilfælde af konkret mistanke om misbrug.

Notus Kommunal, sygesikring
Der er udpeget en systemejer i Kultur- og Fritidsforvaltningen til it-systemet Notus Kommunal, sygesikring.

Af Kultur- og Fritidsforvaltningens notat af 2. oktober 2017 fremgår, at der først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Social Pension og kørekortsregisteret fra 2017.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Notus Kommunal, sygesikring indtil 2017 er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemet Notus Kommunal, sygesikring, ikke er blevet identificeret igennem en årrække, fordi der alene er sket logopfølgning i tilfælde af konkret mistanke om misbrug.

Skat Extranet
Der er udpeget en systemejer i Koncern IT til it-systemet Skat Extranet.

Oplysningerne, som jeg har modtaget fra Kultur- og Fritidsforvaltningen, giver ikke indtryk af, at der har været et samarbejde mellem Kultur- og Fritidsforvaltningen og Koncern IT i forhold til opgaven med stikprøvekontrol af loggen af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet. Herudover er it-systemet Skat Extranet hverken i It-sikkerhedsfunktionens vejledning vedrørende "Krav om stikprøver af loggen i borgerservicecentre" eller i It-sikkerhedsfunktionens best practice "for gennemførelse af stikprøvekontrol af loggen" nævnt som et it-system, der indgår i stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger.

Jeg må på baggrund af de foreliggende oplysninger lægge til grund, at der ikke er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet i Københavns Borgerservice ikke identificeres, fordi der alene sker logopfølgning i tilfælde af konkret mistanke om misbrug.

CSC Social
Der er udpeget en systemejer i Socialforvaltningen til it-systemet CSC Social.

Sammenholdt giver høringssvarene fra Kultur- og Fritidsforvaltningen og Socialforvaltningen indtryk af, at der heller ikke har været et samarbejde mellem Kultur- og Fritidsforvaltningen og Socialforvaltningen i forhold til opgaven med stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CSC Social. Herudover er it-systemet CSC Social hverken i It-sikkerhedsfunktionens vejledning vedrørende "Krav om stikprøver af loggen i borgerservicecentre" eller i It-sikkerhedsfunktionens best practice "for gennemførelse af stikprøvekontrol af loggen" nævnt som et it-system, der indgår i stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger.

Jeg må på baggrund af de foreliggende oplysninger lægge til grund, at der ikke er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CSC Social.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CSC Social er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i it-systemet CSC Social i Københavns Borgerservice ikke identificeres, fordi der alene sker logopfølgning i tilfælde af konkret mistanke om misbrug.

Øvrige it-systemer
Der er udpeget en systemejer i Kultur- og Fritidsforvaltningen til de følgende øvrige it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger: Pasregisteret, straksudstedelse af NemID (NemID Privat), ID-Port (pas og kørekort), køreprøvebookning, P-Data (KMD udtræk fra CPR) og Safepay, kasseløsning.

Københavns Borgerservices anvender herudover it-systemerne KMD Mainframe og fritagelse fra digital post til behandling af fortrolige og følsomme personoplysninger. Der er ikke udpeget en systemejer til disse it-systemer.

Det fremgår ikke af Kultur- og Fritidsforvaltningens notat af 2. oktober 2017, at Kultur- og Fritidsforvaltningen har foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i de ovenfor anførte it-systemer.

Jeg må på den baggrund konkludere, at der ikke er foretaget stikprøvekontrol af loggen af de ovenfor anførte systemer.

Jeg vurderer, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne pasregisteret, fritagelse for digital post, straksudstedelse af NemID (NemID Privat), KMD Mainframe, ID-Port (pas og kørekort), køreprøvebookning, P-Data (KMD udtræk fra CPR) og Safepay, kasseløsning er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg vurderer, at der på baggrund af ovenstående mangel er risiko for, at eventuelt misbrug af fortrolige og følsomme personoplysninger i de ovenfor anførte it-systemer ikke identificeres, fordi der alene sker logopfølgning i tilfælde af konkret mistanke om misbrug.

It-sikkerhedsfunktionens vejledning om stikprøvekontrol

Det fremgår af dokumentationen, som jeg har modtaget med Økonomiforvaltningens høringssvar af 5. september 2016, at It-sikkerhedsfunktionens vejledning vedrørende "Krav om stikprøver af loggen i borgerservicecentre" er dateret den 18. september 2015, og It-sikkerhedsfunktionens best practice "for gennemførelse af stikprøvekontrol af loggen" er dateret den 23. oktober 2015. Materialet er således først udarbejdet mere end 5 år efter, at It-sikkerhedsfunktionen blev oprettet i marts 2010, hvorved It-sikkerhedsfunktionen bl.a. fik kompetence til at vejlede mv. om it-sikkerhedsspørgsmål. Jeg har noteret mig oplysningerne i Koncern IT's høringsbemærkninger af 6. juli 2017 om, at It-sikkerhedsfunktionen inden udarbejdelse af vejledningen var i en længere dialog med Kultur- og Fritidsforvaltningen om, hvordan forvaltningen bedst muligt kunne opfylde kravene.

Det er min opfattelse, at It-sikkerhedsfunktion i Koncern IT på et langt tidligere tidspunkt end sket burde have fulgt op over for Københavns Borgerservice med vejledning og best practice i anledning af Datatilsynets udtalelse.

Det fremgår af vejledningen, at It-sikkerhedsfunktionen anbefaler, at Københavns Borgerservice foretager stikprøvekontroller af loggen.

Det er min opfattelse, at vejledningen i stedet for at være formuleret som en anbefaling burde have været formuleret som et pålæg om at gennemføre stikprøvekontrol i samarbejde med systemejeren. Jeg lægger vægt på, at Datatilsynets udtalelse forpligtiger kommuner, der etablerer borgerservicecentre, til at gennemføre stikprøvekontrol, jf. sikkerhedsbekendtgørelsens § 4, og at It-sikkerhedsfunktion efter min opfattelse inden for rammerne af Regulativ for it-sikkerhed i Københavns Kommune, har adgang til at give påbud til alle enheder og medarbejdere i relation til it-sikkerhed, jf. Regulativ for it-sikkerhed i Københavns Kommune § 8, stk. 8.

It-sikkerhedsfunktionens tilsyn med hensyn til foretagelse af stikprøvekontrol

I min generelle egen drift-undersøgelse vedrørende sikring af borgernes personoplysninger, som har snitflader til nærværende undersøgelse, konkluderede jeg, at Koncern IT's It-sikkerhedsfunktion ikke foretager tilsyn med forvaltningernes opfølgning på registrering af afviste adgangsforsøg og forvaltningernes opfølgning på loggen af behandling af følsomme personoplysninger.

Min undersøgelse viser, at It-sikkerhedsfunktionen først i december 2015 foretog tilsyn med hensyn til foretagelse af stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemer ved Københavns Borgerservice. Det er min opfattelse, at It-sikkerhedsfunktionen på et langt tidligere tidspunkt end sket burde have foretaget tilsyn i lyset af Datatilsynets udtalelse af 26. juni 2006.

ADGANG TIL INDSIGT I OPLYSNINGER EFTER PERSONDATALOVEN

Kultur- og Fritidsforvaltningen har i høringssvaret oplyst, at Københavns Borgerservice følger kommunens procedure ved anmodning om indsigt efter persondataloven, hvorefter svar på anmodning om indsigt efter persondataloven sendes til it-sikkerhedsfunktionen i Koncern IT, som koordinerer et samlet svar til den pågældende borger med oplysning om it-systemerne i kommunen, hvor den pågældende er registreret.

Jeg finder, at proceduren er hensigtsmæssig og har ingen yderligere bemærkninger hertil, Jeg har ikke herved taget stilling til hensigtsmæssigheden af den procedure, der anvendes af It-sikkerhedsfunktionen i Koncern IT til koordinering af et samlet kommunalt svar på indsigtsanmodninger.

BILAG 2 – METODE

2.1 GENERELT FOR BORGERRÅDGIVERENS EGEN DRIFT-UNDERSØGELSER

Borgerrådgiverens generelle egen drift-undersøgelse indledes med en høring af den eller de involverede forvaltninger. For hver forvaltning, som inddrages, høres såvel forvaltningens direktion som eventuelle relevante decentrale enheder.

I høringsbrevet beskriver Borgerrådgiveren i generelle vendinger temaet for undersøgelsen og beder om en række oplysninger og dokumentationsmateriale, herunder eventuelt om udlån af relevante sagsakter til nærmere undersøgelse.

Nogle undersøgelser vil være meget omfattende, mens andre vil være målrettede mod nærmere udvalgte forhold. Dette er forudsat ved udvidelsen af Borgerrådgiverens kompetence.

På baggrund af denne dokumentationsindsamling udarbejder Borgerrådgiveren en foreløbig rapport, som sendes til forvaltningen med henblik på forvaltningens og eventuelle decentrale enheders bemærkninger til rapportens faktiske oplysninger.

Den foreløbige rapport vil også indeholde de udtalelser (herunder kritik/henstilling), som Borgerrådgiveren forventer at fremkomme med, men disse har netop en foreløbig karakter, eftersom faktuelle oplysninger i rapporten kan korrigeres gennem forvaltningens bemærkninger. Forvaltningen informeres således allerede på dette tidspunkt om det forventede udfald af undersøgelsen.

Efter modtagelse af forvaltningens eventuelle bemærkninger indarbejder Borgerrådgiveren bemærkningerne til de faktiske forhold og foretager eventuelle ændringer i undersøgelsens konklusioner, som disse måtte give anledning til. Borgerrådgiveren udarbejder på denne baggrund den endelige rapport. Rapporten er stilet til den involverede forvaltning og eventuelle decentrale enheder.

I nogle tilfælde kan den endelige rapport indeholde uafklarede spørgsmål eller af andre grunde kræve en opfølgning, f.eks. fordi Borgerrådgiveren har bedt om en underretning om, hvad en henstilling giver anledning til. I disse tilfælde vil den endelige rapport følges op af en (eller flere) opfølgningsrapport(er), indtil alle forhold i undersøgelsen er afklaret.

2.2 DENNE UNDERSØGELSES METODE

Denne undersøgelse er gennemført efter de generelle principper nævnt ovenfor.

Borgerrådgiverens høringsbreve til forvaltningerne og forvaltningernes høringssvar med dokumentation mv. er indsat som bilag 4-22. Datatilsynets udtalelse af 26. juni 2006 er indsat som bilag 23

2.3 REAKTIONSMIDLER OG BEDØMMELSESGRUNDLAG

Borgerrådgiverens reaktionsmidler er de samme som Folketingets Ombudsmands. Borgerrådgiveren kan således udtale kritik og komme med henstillinger til Københavns Kommune. Kritik er udtryk for en faglig vurdering af, at regler og retningslinjer mv. ikke er overholdt.

Borgerrådgiveren kan henstille til kommunen at ændre procedurer eller lignende på et givent område.

Derudover kan Borgerrådgiveren påpege mere generelle problemstillinger i sin årsberetning, som afgives til Borgerrepræsentationen.

Borgerrådgiveren har i forbindelse med sin egen drift-virksomhed lagt sig fast på en sproglig skala for graduering af kritikkens alvorlighed. Skalaen omfatter konstateringer af, at noget er uheldigt, konstateringer af begåede fejl, at noget er beklageligt, meget beklageligt, kritisabelt, meget kritisabelt eller stærkt kritisabelt. Skalaen med bemærkninger er indsat i hovedrapporten.

Bedømmelsesgrundlaget for Borgerrådgiveren er det samme som Folketingets Ombudsmands, nemlig skreven ret (herunder love, bekendtgørelser, cirkulærer og vejledninger), god forvaltningsskik samt overordnede humanitære og medmenneskelige betragtninger. Hertil kommer Københavns Kommunes værdigrundlag, og andre politisk vedtagne retningslinjer. Borgerrådgiveren bestræber sig desuden på at anvende samme målestok for sine vurderinger som Folketingets Ombudsmand.

Borgerrådgiverens opgave er at undersøge, om kommunens forvaltninger og institutioner overholder gældende lovgivning, god forvaltningsskik, kommunens vedtagne politikker og beslutninger om serviceniveau og -standard. Borgerrådgiveren har således ikke særligt til opgave at komme med ros eller lignende tilkendegivelser om positive forhold.

Borgerrådgiverens rapporter om egen drift-undersøgelser vil derfor ikke indeholde ros (i hvert fald ikke i videre omfang), og læseren bør notere sig, at fraværet af ros ikke er ensbetydende med, at Borgerrådgiveren alene har konstateret negative forhold i forbindelse med sin undersøgelse.

BILAG 3 – VURDERINGSGRUNDLAG

3.1 DET JURIDISKE GRUNDLAG – LOGNING AF ELEKTRONISK SAGSBEHANDLING

Undersøgelsen vedrørende logning af elektronisk sagsbehandling (sikkerhedsforanstaltninger) tager udgangspunkt i nedenstående lovregler, Datatilsynets vejledning til sikkerhedsbekendtgørelsen, herunder Datatilsynets udtalelse med udtalelse om, at kommuner, der etablerer borgerservicecentre, skal gennemføre stikprøvekontrol af loggen i it-systemer.

Persondataloven
De overordnede regler for datasikkerheden (behandlingssikkerhed) er fastsat i persondatalovens § 41.

Persondatalovens § 41, stk. 1, 3 og 5 lyder det således:

> "…
> **§ 41**. Personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov
> *Stk. 3.* Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske 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. Tilsvarende gælder for databehandlere.
> *Stk. 5.* Justitsministeren kan fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger.
> …"

Sikkerhedsbekendtgørelsen
Justitsministeren har i medfør af persondatalovens § 41, stk. 5, udstedt sikkerhedsbekendtgørelsen.

Sikkerhedsbekendtgørelsen indeholder de nærmere regler om de sikkerhedsforanstaltninger, som den dataansvarlige myndighed skal træffe i henhold til § 41, stk. 3, i persondataloven.

Det følger af sikkerhedsbekendtgørelsens § 3, at den dataansvarlige myndighed skal træffe fornødne tekniske og organisatoriske foranstaltninger med henblik på beskyttelse af personoplysninger. Bestemmelsen er en gengivelse af persondatalovens § 41, stk. 3, jf. ovenfor.

Det følger af sikkerhedsbekendtgørelsens § 4, at Datatilsynet fører tilsyn med overholdelsen af sikkerhedsbekendtgørelsen og kan komme med henstillinger over for den dataansvarlige myndighed. Bestemmelsen lyder således:

> "…
> Datatilsynet fører tilsyn med overholdelsen af denne bekendtgørelse og kan i den forbindelse komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger, jf. § 3.
> …"

Det følger af sikkerhedsbekendtgørelsens § 5, at den dataansvarlige myndighed skal fastsætte nærmere interne sikkerhedsbestemmelser. Bestemmelsen lyder således:

"…
§ 5. Den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af denne bekendtgørelse. Bestemmelserne skal navnlig 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 edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.
…"

Sikkerhedsbekendtgørelsens kapitel 3 indeholder supplerende sikkerhedsforanstaltninger for behandlingen af fortrolige personoplysninger. Sikkerhedsbekendtgørelsens kapitel 3 gælder ikke for anvendelse af ikke-fortrolige personoplysninger eller for fortrolige personoplysninger, som i øvrigt er undtaget i henhold til reglerne i kapitel 3.

Sikkerhedsbekendtgørelsens § 15 lyder således:

"…
§ 15. Bestemmelserne i kapitel 3 finder ikke anvendelse i det omfang de behandlede oplysninger ikke i sig selv ville være omfattet af anmeldelsespligt til Datatilsynet.
…"

Det følger af sikkerhedsbekendtgørelsens § 18 (i kapitel 3), at der skal ske kontrol med afviste adgangsforsøg. Bestemmelsen lyder således:

"…
§18. 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
…"

Efter sikkerhedsbekendtgørelsens § 19 (i kapitel 3) skal der ske logning af alle anvendelser af personoplysninger. Bestemmelsen har følgende ordlyd:

"…
§ 19. Der skal foretages maskinel registrering (logning) af alle anvendelser af 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.
Stk. 2. Bestemmelsen i stk. 1 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.
Stk. 3. Bestemmelsen i stk. 1 finder ikke 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.
Stk. 4. Bestemmelsen i stk. 1 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.
Stk. 5. Bestemmelsen i stk. 1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfat-

ter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger.
…"

Datatilsynets vejledning til sikkerhedsbekendtgørelsen
Følgende fremgår bl.a. af Datatilsynets vejledning vedrørende logningskravet efter sikkerhedsbekendtgørelsens § 19:

"…
Efter bestemmelsen skal der som udgangspunkt foretages logning af alle anvendelser af personoplysningerne, som sker i behandlingen, jf. dog § 15. Herudover indeholder stk. 2 - 6 visse undtagelser fra det generelle logningskrav.

Ved »alle anvendelser af personoplysninger« skal her forstås de anvendelser, som foretages af brugere af systemet i forbindelse med deres arbejde. Der er en række aktiviteter i forbindelse med driftsafvikling, som indebærer overvågning af og indgriben i systemerne af drifts- og systemmedarbejdere. Anvendelser af personoplysninger i forbindelse med sådanne aktiviteter er ikke omfattet af logningskravet.

Logningen skal bl.a. omfatte en angivelse af den person, som de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Foretages der en søgning på en person ved angivelse af personnummer, skal således det anvendte personnummer eller anden entydig identifikation af den pågældende person registreres i loggen. Hvis der søges på fødselsdato, skal den angivne dato (søgekriteriet) registreres i loggen, men der er ikke krav om registrering af identifikation af de enkelte personer, som indgår i søgeresultatet, dvs. alle fundne personer med den angivne fødselsdato. Angivelsen i loggen af det anvendte søgekriterium giver mulighed for efterfølgende at rekonstruere behandlingen, herunder hvilke personer som indgik i behandlingen, hvilket bl.a. er formålet med logningen.
…"

Datatilsynets udtalelse om stikprøvekontrol af logfiler
Datatilsynet har ved udtalelse af 26. juni 2006 (j. nr. 2006-329-0022) i forbindelse med gennemførelsen af lovgivningen om kommunale borgerservicecentre henstillet, at kommuner, der etablerer borgerservicecentre, skal foretage stikprøvekontrol af loggen af behandling af følsomme personoplysninger i it-systemer.

Datatilsynet udtaler bl.a. følgende:

"…
2.3. STIKPRØVEKONTROL AF LOGGEN
Datatilsynet finder, at den øgede adgang til personoplysninger i borgerservicecentre gør det påkrævet, at der foretages stikprøvekontrol af loggen. Dette gælder dog alene systemer, hvori der indgår anmeldelsespligtige behandlinger af personoplysninger, dvs. systemer, hvor der efter sikkerhedsbekendtgørelsen allerede er krav om logning.
(…)

Ifølge udkastet til publikationen skal stikprøverne foretages på kommunens eget initiativ, med jævne mellemrum og med vilkårlige intervaller.

Der er i den forbindelse givet et eksempel på, hvordan ordningen kan være beskrevet i kommunens uddybende sikkerhedsregler.

Datatilsynet finder, at det i eksemplet anførte, hvorefter kontrollen foretages med forskellige intervaller, dog højest 6 måneder, er udtryk for en passende afvejning af de bagvedliggende hensyn.

Datatilsynet skal herefter henstille, at kommuner, der etablerer borgerservicecentre, som minimum foretager stikprøvekontrol af logfiler i et omfang, der svarer til det anførte i eksempelboks [9, *min tilføjelse*] (…).

Det tilføjes, at Datatilsynet vil være indstillet på at lade den manuelle stikprøvekontrol af loggen erstatte af en automatiseret overvågning, der bl.a. afdækker uhensigtsmæssige eller usædvanlige søgemønstre og dermed er bedre egnet end stikprøvekontrol til at afsløre misbrug.
…"

I det følgende gengives eksempelboks 9 fra publikationen Datasikkerhed i borgerservicecentre – regler og praksis:

"…

Eksempelboks 9:

I X Kommunes uddybende sikkerhedsregler står der:

Stikprøver af loggen
Stikprøverne foretages af de opslag, som borgerservicecentermedarbejderne foretager i de logningspligtige it-systemer. Stikprøverne falder med forskellige intervaller, f.eks. 1 måned, 2½ måned, 5 måneder, 3 måneder osv., dog højst 6 måneder. Datoerne fremgår af et bilag, som kun sikkerhedsmedarbejderne har adgang til.

En stikprøve omfatter 5 – 6 opslag foretaget 1 – 3 dage før, medarbejderen anmodes om at redegøre for årsagen til opslagene.

Stikprøverne udskrives og forelægges de medarbejdere, der har foretaget opslagene. De skriver på udskriften, hvad årsagen til opslagene var (evt. journalnumre på de sager, som opslagene vedrørte). Stikprøverne med medarbejderens noteringer lægges til den chef, som har den største indsigt i vedkommendes arbejde. Giver det chefen anledning til spørgsmål, taler chefen med medarbejderen / sikkerhedsmedarbejderen. Giver det ikke anledning til spørgsmål, betragtes kontrollen som gennemført med tilfredsstillende resultat. Hver 2. måned udsendes en meddelelse på intranettet om, at opslag i de fleste af kommunens it-systemer logges, at opslagene til enhver tid kan blive kontrolleret, og at de opslag, som borgerservicecenter-medarbejderne foretager, kontrolleres jævnligt ved stikprøver. I de af kommunens it-systemer, hvor det er muligt at tilpasse åbningsbilledet, står samme besked.

…"

Regulativ for it-sikkerhed i Københavns Kommune
Københavns Kommune har i medfør af sikkerhedsbekendtgørelsens § 5 udstedt Regulativ for it-sikkerhed i Københavns Kommune.

Regulativet for it-sikkerhed i Københavns Kommune (version 2.2., publiceret den 8. juli 2014) indeholder bl.a. it-sikkerhedsbestemmelserne for Københavns Kommune samt den nærmere opgavefordeling mellem Koncern IT og forvaltningerne i relation til iværksættelse og kontrol af sikkerhedsforanstaltninger.

Det følger af Regulativ for it-sikkerhed i Københavns Kommunes § 8, at it-sikkerhedsfunktionen i Koncern IT (tidligere Koncernservice) fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelse, og at it-sikkerhedsfunktionen kan komme med påbud til alle ansatte og enheder vedrørende it-sikkerhed:

Regulativ for it-sikkerhed i Københavns Kommunes § 8 har følgende ordlyd:

"…
§ 8. It-sikkerhedsfunktionen er placeret i Koncernservice i Økonomiforvaltningen. i Københavns Kommune.
Stk. 2 It-sikkerhedsfunktionen fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser og koordinerer kommunens it-sikkerhedsarbejde.
Stk. 3. It-sikkerhedsfunktionen tilrettelægger informations- og uddannelsesaktiviteter for medarbejdere, der varetager kommunens It-sikkerhedsfunktioner.
Stk. 4. It-sikkerhedsfunktionen rådgiver kommunen om it-sikkerhedsmæssige forhold.
Stk. 5. It-sikkerhedsfunktionen kan afkræve enhver medarbejder i kommunen oplysninger, som har betydning for varetagelsen af tilsynsfunktionen.
Stk. 6. It-sikkerhedsfunktionen skal sikre at der sker kontrol af adgangsrettigheder og autorisationer, der er givet til medarbejderne.
Stk. 7. It-sikkerhedsfunktionens opgaver, jf. stk. 1-6, varetages for Brandvæsenets egne it-systemer af en it-sikkerhedsleder for Brandvæsenet.
Stk. 8. It-sikkerhedsfunktionen kan komme med påbud til alle ansatte og enheder i kommunen om hvorledes man skal forholde sig i relation til it-sikkerhed.
Stk. 9. Som led i den almindelige revision af kommunen skal der også foretages revision af it-sikkerheden. It-sikkerhedsfunktionen aftaler med revisor hvorledes it-sikkerhedsrevisionen skal udføres.
…"

…"

Regulativ for it-sikkerhed i Københavns Kommune § 10 fastlægger forvaltningernes opgaver i relation til sikkerhedsforanstaltningerne. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 10, stk. 2 og stk. 5.:

"…
§ 10 […]
Stk. 2. Direktionen skal inden for eget område iværksætte de foranstaltninger, der er nødvendige for at opnå en tilstrækkelig it-sikkerhed, indenfor de rammer som er opstillet i It-sikkerhedshåndbogen.
Stk. 5. Direktionen skal inden for eget område udpege en systemejer for it-systemer forvaltningen har ansvaret for samt mindst en stedfortræder for hver systemejer, hvor intet andet er besluttet er det direktionen der er stedfortræder. Koncernservice kan efter aftale overtage systemejerskabet for systemer indenfor den enkelte forvaltnings eget
område. Hvis dette sker skal Koncernservice direktion udpege systemejerne samt mindst en stedfortræder for hver af systemejerne. Direktionen for Koncernservice skal udpege en systemejer for hvert af de fællessystemer, som Koncernservice er ansvarlig for.
…"

Det følger bl.a. af Regulativ for it-sikkerhed i Københavns Kommune § 11, at det påhviler systemejerne til it-systemerne at sikre, at systemerne understøtter it-sikkerhedskravene samt at sikre, at it-systemerne lever op til kommunens it-sikkerhedsregler samt gældende lovgivning. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 11, stk. 1-4, samt stk. 7:

"…
§ 11. Systemejeren skal sikre, at systemets funktionalitet og anvendelse løbende tilpasses og bedst muligt understøtter It-sikkerhedskravene samt forretningens og brugernes behov.
Stk. 2. Før anskaffelse af nye systemer skal systemejeren have godkendt anskaffelsen af systemet. Dette sker i forbindelse med registreringen i kommunens fortegnelse over it-system. I forbindelse med anskaffelsen af systemet skal der foreligge en kortfattet risikoanalyse. Systemejeren har mulighed for at få separat itsikkerhedsgodkendelse af andet end nye systemer.
Stk. 3. Systemejerskabet skal varetages ud fra kommunens forretningsmæssige behov. Systemejeren er ansvarlig for it-systemets funktionalitet, opbygning, anvendelse og sikkerhedsløsning. Der kan indgås aftale mellem forvaltningen og leverandøren/driftcentret som beskriver

niveauet for service. Ændringer i systemer som har snitflader/deling af it-ressourcer med Koncernservice og kommunens administrative net skal ske efter Koncernservice "change" procedure.
Stk. 4. Systemejer er ansvarlig for, at it-systemet kan anvendes mest muligt effektivt og at systemet løbende forbedres, så det bedst muligt understøtter arbejdsopgaverne og kommunens forretningsmæssige behov og lever op til kravene i It-sikkerhedshåndbogen. Der skal etableres processer, der sikre en stabil, effektiv og sikker drift af systemet.
Stk. 7. Systemejeren skal sikre, at it-systemet kan logge behandling af data, når det er krævet i de uddybende It-sikkerhedsregler og som følge af gældende lovgivning.
…"

Det følger bl.a. af Regulativ for it-sikkerhed i Københavns Kommune §§17-18, at forvaltningerne inden for eget område skal sikre, at specifik lovgivning af betydning for it-sikkerheden overholdes, og at det daglige ansvar for overholdelse af persondataloven i forbindelse med behandling af personoplysninger påhviler forvaltningerne. Det lyder således i §§ 17-18:

"…
§17. De respektive direktioner[…] skal inden for eget område sikre, at specifik lovgivning af betydning for it-sikkerheden og eksterne it-sikkerhedskrav for det pågældende område bliver identificeret, dokumenteret og overholdt.
§ 18. Det daglige ansvar for overholdelsen af reglerne i persondataloven i forbindelse med behandling af personoplysninger påhviler de respektive direktioner […]"

Uddybende sikkerhedsregler for Københavns Kommune

Det fremgår af Koncern IT's seneste uddybende sikkerhedsregler for Københavns Kommune (version 2.2., publiceret den 8. juli 2014), om logning, at der løbende skal følges op på logdata, og at fejllogs regelmæssigt skal analyses og gennemgås. Det lyder således i afsnit 10.10 om logning:

"…
Brugerlogning

- It-systemer hvor personoplysninger behandles, skal omfattes af logning, med mindre de er undtaget fra logning i Justitsministeriets Bekendtgørelse om it-sikkerhed nr. 528 § 19. Logdata skal f.eks. indeholde dato for systemanvendelse og specificering af systemer, log-on og log-off.
- Fejlede og succesfulde adgangsforsøg
- Logning af brugen af udvidede rettigheder på kritiske systemer
- Logning af data indeholdende personfølsomme oplysninger skal opbevares i 6 måneder, hvorefter logdata skal slettes. Undtagelser hvor logdata skal opbevares i op til 5 år, skal være dokumenteret.
- It-systemer, hvor data der er omfattet af Københavns kommunes kasse og regnskabsregulativ opbevares, skal logge i henhold til denne.

Systemlogning

- Installation og brugen af systemværktøjer på kritisk systemer
- Brugen af kritiske transaktionstyper, herunder læsning og ændring af data.
- Konfigurationsændringer
- Benyttede netværksprotokoller
- Aktivering/deaktivering af systemkontroller såsom antivirus, firewall og andre logiske sikringskontroller.

Opfølgning på logning

- Der skal løbende følges op på logdata med henblik på at identificere uhensigtsmæssigheder f.eks. overskridelser af tærskelværdier, forsøg på uretmæssig adgang til kritiske data, uventede ændringer og til/frakobling af udstyr til systemer eller netværk.
- Alarmer fra fysiske og logiske adgangskontrolsystemer omfattende benyttede adgange, forsøg på adgang og aktivering/deaktivering af kontroller i disse systemer, skal håndteres.

Fejllogs

- Fejllogs skal regelmæssigt analyseres og gennemgås for at sikre alle fejl bliver rettet på tilfredsstillende vis.
- Korrigerende og kompenserende foranstaltninger, der kan påvirke beskyttelsen af data på systemerne skal dokumenteres.

Administratorlogs

- Hvis et system indeholder personfølsomme data eller værdi data skal aktiviteter udført af systemadministratorer og andre med særlige rettigheder logges. Hvor det er teknisk muligt skal der være etableret funktionsadskillelse, således at systemadministratorer ikke selv kan ændre loginformationer.

Beskyttelse af logdata

- Logfaciliteter og loginformation skal være beskyttet, således at risikoen for uautoriseret adgang eller manipulation af indholdet reduceres.

…"

3.2. DET JURIDISKE GRUNDLAG – ADGANG TIL INDSIGT I PERSONOPLYSNINGER EFTER PERSONDATALOVEN

Undersøgelsen vedrørende adgang til indsigt i oplysninger efter persondataloven tager udgangspunkt i Persondatalovens § 31 med følgende ordlyd:

"…
§ 31. Fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om,
1) hvilke oplysninger der behandles,
2) behandlingens formål,
3) kategorierne af modtagere af oplysningerne og
4) tilgængelig information om, hvorfra disse oplysninger stammer.
Stk. 2. Den dataansvarlige skal snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.
…"

3.3 UNDERSØGELSESFORLØB OG DOKUMENTATIONSGRUNDLAGET (DATA)

Borgerrådgiveren iværksatte nærværende egen drift-undersøgelse ved brev af 8. august 2014 til Kultur- og Fritidsforvaltningen. Undersøgelsen blev iværksat over for forvaltningen, fordi Borgerrådgiveren på daværende tidspunkt antog, at der var udpeget en systemejer i Kultur- og Fritidsforvaltningen i forhold til de it-systemer, som Københavns Borgerservice anvender til behandling af følsomme personoplysninger. Til brug for undersøgelsen modtog Borgerrådgiveren høringssvar af 16. september 2014 fra Kultur- og Fritidsforvaltningen samt dokumentation i form af procedurer, vejledning, retningslinjer mv. i relation til hhv. logning af elektronisk sagsbehandling hhv. adgang til indsigt i personoplysninger efter persondataloven. Borgerrådgiveren stillede ved brev af 26. maj 2015 til Kultur- og Fritidsforvaltningen opfølgende spørgsmål, hvilket blev bevaret af forvaltningen ved brev af 5. oktober 2015. Den modtagne dokumentation fra Kultur- og Fritidsforvaltningen i relation til logning af elektronisk sagsbehandling er udeladt i nærværende undersøgelse, fordi Borgerrådgiverens overførte denne del af undersøgelsen til Socialforvaltningen og dernæst til Økonomiforvaltningen, se straks nedenfor.

Borgerrådgiveren overførte undersøgelsen vedrørende logning af elektronisk sagsbehandling ved iværksættelsesbrev af 7. juli 2016 til Socialforvaltningen, da Borgerrådgiveren blev bekendt med, at der var udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag, som Københavns Borgerservice anvender til behandling af følsomme personoplysninger. Borgerrådgiveren modtog høringssvar af 12. august 2016, hvor det imidlertid fremgår, at der ikke er udpeget systemejer i Socialforvaltningen til KMD Sag.

Borgerrådgiveren overførte dernæst undersøgelsen vedrørende logning af elektronisk sagsbehandling ved iværksættelsesbrev af 15. august 2016 til Økonomiforvaltningen, da Borgerrådgiveren fik kendskab til, at der var udpeget en systemejer i Koncern IT til KMD Sag. Til brug for undersøgelsen modtog Borgerrådgiveren høringssvar af 5. september 2016 samt dokumentation i form af vejledninger og retningslinjer (best practice) vedrørende stikprøvekontrol, herunder beskrivelse af logning i KMD Sag.

Borgerrådgiveren sendte foreløbig rapport til Kultur- og Fritidsforvaltningen, Økonomiforvaltningen og Socialforvaltningen den 28. februar 2017. Borgerrådgiveren modtog Økonomiforvaltningens høringsbemærkninger den 5. april 2017, Socialforvaltningens høringsbemærkninger den 7. april 2017 samt Kultur- og Fritidsforvaltningens høringsbemærkninger den 28. april 2017.

Borgerrådgiveren sendte efterfølgende foreløbig rapport II til forvaltningerne den 23. juni 2017. Borgerrådgiveren modtog Økonomiforvaltningens høringsbemærkninger II den 2. august 2017, Socialforvaltningens høringsbemærkninger II den 11. august 2017 samt Kultur- og Fritidsforvaltningens høringsbemærkninger II den 9. august 2017.

Borgerrådgiveren har videre telefonisk den 8. og 11. september 2017 til Kultur- og Fritidsforvaltningen og ved e-mail af 27. september 2017 til Kultur- og Fritidsforvaltningen stillet opfølgende spørgsmål om foretagne stikprøvekontroller, hvilket Kultur- og Fritidsforvaltningen har besvaret ved notat af 15. september 2017 og notat af 2. oktober 2017.

BILAG 4 – BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL KULTUR- OG FRITIDSFORVALTNINGEN

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Til Kultur- og Fritidsforvaltningen – direktionen

Sendt pr. mail til

08-08-2014

Sagsnr.
2014-0117411
2014-0118160

Dokumentnr.
2014-0117411-2

Vedrørende Borgerrådgiverens inspektion af Borgerservice Bispebjerg samt iværksættelse af generel egen drift-undersøgelse

Borgerrådgiveren kan af egen drift iværksætte undersøgelser af konkrete og generelle forhold samt gennemføre inspektioner i Københavns Kommune. Kompetencen følger af vedtægt for Borgerrådgiveren §§ 12-13, som lyder således:

"...
§ 12. Borgerrådgiveren kan af egen drift optage en konkret sag til undersøgelse, når der må formodes at foreligge et principielt aspekt, eller såfremt der efter de foreliggende oplysninger må antages at være tale om grove eller væsentlige fejl.
Stk. 2. Borgerrådgiveren kan af egen drift gennemføre generelle undersøgelser af udvalgte forvaltningsområder efter samråd med Borgerrådgiverudvalget.

§ 13. Borgerrådgiveren kan foretage inspektioner af institutioner, virksomheder samt tjenestesteder, der hører under Borgerrepræsentationens virksomhed.
..."

Vedtægten kan findes på følgende link:

http://www.kk.dk/da/borger/borgerraadgiveren/om-borgerraadgiveren

Baggrunden for iværksættelsen
Borgerrådgiverudvalget bekræftede den 24. januar 2014 Borgerrådgiverens egen drift-plan for 2014, som indeholder en inspektion af et borgerservicecenter samt en generel egen drift-undersøgelse af logning af elektronisk sagsbehandling og borgernes adgang til indsigt i oplysninger efter persondataloven. Begge undersøgelser vedrører Københavns Borgerservice under Kultur- og Fritidsforvaltningen.

De to undersøgelser iværksættes samtidigt med dette brev under hensyn til deres indbyrdes snitflader.

Ad) Inspektionen af Borgerservice Bispebjerg
Jeg har på ovennævnte baggrund valgt at foretage inspektion af Borgerservice Bispebjerg. Til grund for udvælgelsen ligger alene generelle kriterier, herunder Borgerservice Bispebjergs digitale profil, og ikke et forhåndskendskab til forholdene på Borgerservice Bispebjerg.

Inspektionen vil primært rette sig mod den konkrete opgaveløsning i Borgerservice Bispebjerg med udgangspunkt i Borgerrådgiverudvalgets ønske om en undersøgelse af sikring af datasikkerhed i forbindelse med brug af digital adgang via kommunalt udstyr, herunder særligt sikringen af borgernes følsomme eller fortrolige oplysninger, der indtastes via offentligt tilgængelige pc'ere. Herudover inspiceres også i relevant omfang de fysiske rammer (indretning) for sikring af fortrolighed i samtalen mellem borger og kommunen i forvaltningsenhedens modtagelsesafsnit, håndtering af henvendelser, ventetider og svarfrister, vejledning mv.

Den fysiske del af inspektionen vil bl.a. angå borgernes mulighed for ugenert at indtaste følsomme eller fortrolige oplysninger, printe oplysninger uden uvedkommendes adgang til printet samt mulighed for at modtage vejledning uden videregivelse af deres følsomme eller fortrolige oplysninger mv. til uvedkommende. Herudover retter inspektionen sig mod den fysiske indretning af lokalerne i forhold til afmærkning af diskretionsliner, herunder afstanden til tilhørere og eventuelt andre borgerekspeditioner samt adgangen til separate møderum og den fysiske tilgængelighed.

Inspektionen er planlagt til at finde sted:

tirsdag den 30. september 2014 fra kl. 10.00 – ca. 13.30.

Fra Borgerrådgiveren deltager jurist Daniel Soelberg Bach, jurist Katrine Fagerli, administrativ medarbejder Lise Thisted Simonsen foruden jeg selv.

Inspektionen består i et indledende møde med ledelse og medarbejderrepræsentanter fra kl. 10.00 og ca. en time frem, rundgang med besigtigelse af Borgerservice Bispebjerg samt et afsluttende møde med ledelsen. I øvrigt tilrettelægges inspektionen på stedet under hensyntagen til borgerne og medarbejderne og den aktuelle brug af Borgerservice Bispebjerg.

Materiale til brug for inspektionen:
Jeg beder om, at Borgerservice Bispebjerg senest 14 dage inden inspektionen fremsender eventuelle overordnede retningslinjer for borgerbetjeningen i centeret.

Jeg beder desuden om, at Borgerservice Bispebjerg senest 14 dage inden inspektionen fremsender eventuelle øvrige retningslinjer for behandlingen af borgernes henvendelser – herunder om f.eks. kommunikationen med borgere, elektronisk og fysisk håndtering af personfølsomme oplysninger, ventetider og svarfrister, vejledning, ekspedition af sager til andre forvaltningsenheder eller myndigheder, tavshedspligt og videregivelse af oplysninger mv. samt eventuelle skriftlige vejledninger, som udleveres til borgerne eller links til sådannes placering på internet.

Jeg beder ligeledes om, at Borgerservice Bispebjerg fremsender retningslinjer, baggrundsmateriale, politiker eller lignende materiale vedrørende digitalisering og borgernes anvendelse af kommunens digitale udstyr, digital sagsbehandling, kanalstrategier og lignende.

Såfremt Borgerservice Bispebjerg er i besiddelse af andet relevant materiale for inspektionen, imødeser jeg ligeledes dette 14 dage inden inspektionen.

Ad) Generel egen drift-undersøgelse af logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger efter persondataloven

Borgerrådgiverens generelle egen drift-undersøgelse er rettet mod samtlige borgerservicecentre i Kultur- og Fritidsforvaltningen.

Formålet med undersøgelsen er at belyse logning af elektronisk sagsbehandling (dvs. logning af anvendelse af personoplysninger). Herudover er det formålet med undersøgelsen at belyse, hvorledes anmodninger om indsigt i oplysninger efter persondataloven bliver behandlet i Borgerservice.

Undersøgelsen vil have fokus på borgerservicecentrenes procedurer og rutiner mv. dels i relation til logning af elektronisk sagsbehandling dels i relation til anmodninger om indsigt i oplysninger efter persondataloven.

Undersøgelsen tager udgangspunkt i nedenstående regler, men er ikke afgrænset hertil.

Regelgrundlag

Vedrørende logning af elektronisk sagsbehandling

De overordnede regler for datasikkerheden (behandlingssikkerhed) er fastsat i lov om behandling af personoplysninger (herefter persondataloven) §§ 41 og 42.

Persondatalovens § 41, stk. 1, stk. 3 og stk. 5 har følgende ordlyd:

"...
§ 41. Personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov

Stk. 3. Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske 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. Tilsvarende gælder for databehandlere.

Stk. 5. Justitsministeren kan fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger.
..."

Persondatalovens § 42, stk.1, har følgende ordlyd:

"...
§ 42. Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.
..."

Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Justitsministeren har i medfør af persondatalovens § 41, stk. 5 udstedt bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (herefter sikkerhedsbekendtgørelsen).

Sikkerhedsbekendtgørelsen indeholder de nærmere regler om de sikkerhedsforanstaltninger, som den offentlige forvaltning skal træffe i henhold til § 41, stk. 3 i persondataloven.

Det følger af sikkerhedsbekendtgørelsens § 5, at den dataansvarlige myndighed skal fastsætte nærmere interne sikkerhedsbestemmelser.

Sikkerhedsbekendtgørelsens kapitel 3 indeholder supplerende sikkerhedsforanstaltninger for behandlingen af fortrolige personoplysninger. Sikkerhedsbekendtgørelsens kapitel 3 gælder ikke for anvendelse af ikke-fortrolige personoplysninger eller for fortrolige personoplysninger, som i øvrigt er undtaget i henhold til reglerne i kapitel 3.

Det følger af sikkerhedsbekendtgørelsens § 18 (i kapitel 3), at der skal ske kontrol med afviste adgangsforsøg. Bestemmelsen lyder således:

> "...
> **§18.** 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
> ..."

Efter sikkerhedsbekendtgørelsens § 19, stk. 1, (i kapitel 3) skal der ske logning af alle anvendelser af personoplysninger. Bestemmelsen har følgende ordlyd:

> "...
> **§ 19.** Der skal foretages maskinel registrering (logning) af alle anvendelser af 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.
> ..."

Vedrørende indsigt i oplysninger efter persondataloven

Persondatalovens § 31 har følgende ordlyd:

> "...
> **§ 31**. Fremsætter en person begæring herom, skal den dataansvarlige give den pågældende meddelelse om, hvorvidt der behandles oplysninger om vedkommende. Behandles sådanne oplysninger, skal der på en let forståelig måde gives den registrerede meddelelse om,
> 1) hvilke oplysninger der behandles,
> 2) behandlingens formål,
> 3) kategorierne af modtagere af oplysningerne og
> 4) tilgængelig information om, hvorfra disse oplysninger stammer.
> *Stk. 2.* Den dataansvarlige skal snarest besvare begæringer som nævnt i stk. 1. Er begæringen ikke besvaret inden 4 uger efter modtagelsen, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge.
> ..."

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Anmodning om udtalelse og besvarelse af spørgsmål

Vedrørende logning af elektronisk sagsbehandling
Jeg beder om en udtalelse fra Kultur- og Fritidsforvaltningen med en generel beskrivelse af, hvilke foranstaltninger borgerservicecentrene er ansvarlige for – og hvilke foranstaltninger borgerservicecentrene udfører – i relation til logning af elektronisk sagsbehandling.

Jeg beder endvidere om, at Kultur- og Fritidsforvaltningen svarer på følgende spørgsmål:

- I hvilke it-systemer hos borgerservicecentrene anvendes fortrolige personoplysninger?
- Hvem er systemejere for de pågældende systemer (oplyses med angivelse af navn, forvaltning og kontaktoplysninger i form af telefon og e-mailadresser)?
- Er de pågældende it-systemer it-sikkerhedsgodkendt?
- Hvorledes sker der logning af anvendelse af personoplysninger i de pågældende it-systemer?
- Foretages der tilsyn med logning af anvendelse af personoplysninger? Og i givet fald hvorledes føres der tilsyn og hvor hyppigt?
- Hvorledes håndteres eventuelle brud på it-sikkerheden (jf.*)?
- Hvorledes følges op på log-registreringer om afviste adgangsforsøg til it-systemerne i borgerservicecentrene, hvor der behandles fortrolige eller følsomme personoplysninger?

(*Med brud på it-sikkerheden menes her: konstateringer eller formodninger om uberettiget videregivelse af borgernes personoplysninger, og/eller konstateringer eller formodning om, at medarbejdere uberettiget skaffer sig adgang til borgernes personoplysninger).

Vedrørende indsigt i oplysninger efter persondataloven
Jeg beder om, at det i udtalelsen fra Kultur- og Fritidsforvaltningen nærmere beskrives, hvorledes borgerservicecentrene håndterer anmodninger om indsigt i oplysninger efter persondataloven. Jeg er opmærksom på, at besvarelser af sådanne anmodninger koordineres i KS.

Jeg beder om, at Kultur- og Fritidsforvaltningen i den forbindelse oplyser proceduren for dels håndtering af anmodninger om indsigt fremsat over for Borgerservice og dels for undersøgelse af, om der foreligger oplysninger/registreringer vedrørende den pågældende borger.

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Anmodning om dokumentation
Jeg beder om kopi af eksisterende procedurer, forretningsgange, retningslinjer, rutiner mv. hos borgerservicecentrene vedrørende logning af elektronisk sagsbehandling samt vedrørende behandling af anmodninger om indsigt i oplysninger efter persondataloven.

Afsluttende bemærkninger for de to undersøgelser:
Jeg beder direktionen om internt i forvaltningen at koordinere orienteringen om inspektionen samt besvarelsen af mine anmodninger om redegørelser og dokumentation. Repræsentanter fra direktionen er naturligvis velkomne til at være til stede ved inspektionen.

Hvis det skønnes formålstjenligt, deltager Borgerrådgiveren naturligvis gerne i et møde om afgrænsning af de redegørelser og det materiale, jeg har anmodet om.

Såfremt der fra kommunens politiske niveau eller fra Folketingets Ombudsmand eller andre tilsynsmyndigheder er rejst eller rejses en tilsvarende undersøgelse, beder jeg om at modtage orientering herom.

Til orientering om inspektionen og Borgerrådgiverens egen driftkompetence vedlægger jeg til orientering:

- Kopi af indstilling om udvidelse af Borgerrådgiverens kompetence med adgang til at iværksætte undersøgelser på eget initiativ (egen drift-funktion) (BR 656/06)
- Notat om sagsgange og offentliggørelsesprocedurer for Borgerrådgiverens egen drift-undersøgelser (herunder inspektioner).

Jeg vil via Borgerrådgiverens hjemmeside
www.borgerraadgiver.kk.dk og eventuelt Borgerrådgiverens nyhedsbrev orientere offentligheden om, at jeg har iværksat denne inspektion og generelle egen drift-undersøgelse.

Eventuelle spørgsmål vedrørende inspektionen kan rettes til sagsbehandler jurist Katrine Fagerli, som træffes på telefon 82 20 52 05 eller e-mail via borgerraadgiveren@kk.dk.

Eventuelle spørgsmål vedrørende den generelle egen drift-undersøgelse kan rettes til sagsbehandler jurist Daniel Soelberg Bach, som træffes på telefon 82 20 52 11 eller e-mail via borgerraadgiveren@kk.dk.

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Med venlig hilsen

Johan Busse
Borgerrådgiver

BILAG 5 – HØRINGSSVAR FRA KULTUR- OG FRITIDSFORVALTNINGEN OG UDVALGT DOKUMENTATION

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Sekretariat & Presse

16-09-2014

Sagsnr.
2014-0171930

Dokumentnr.
2014-0171930-2

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

Inspektion af Borgerservice Bispebjerg og egen drift-undersøgelse af logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger efter persondataloven

Med henvisning til brev af 8. august 2014 om inspektion af Borgerservice Bispebjerg fremsendes hermed de ønskede oplysninger.

Overordnede retningslinjer for borgerbetjeningen
"Vidensbasen" på intranettet indeholder under punktet "Personlig henvendelse" retningslinjer for de forskellige typer af borgerbetjening: http://kff.kkintra.kk.dk/indhold/sagsbehandling-og-styring. Se også bilag 5. Folderen "Tillidsfuld og effektiv kommunikation".

Øvrige retningslinjer for behandlingen af borgernes henvendelser
Som ovenfor.

Retningslinjer, baggrundsmateriale, politikker eller lignende materiale vedr. digitalisering og borgernes anvendelse af kommunens digitale udstyr, digital sagsbehandling, kanalstrategier og lignende:
Se venligst

- Bilag 1. Citizen 2015. Service- og kanalstrategi for Københavns kommune 2013-2015
- Bilag 4. Folderen "Ny service i praksis"

Nye medarbejdere oplæres i god sagsbehandling, også digital sagsbehandling, og tilmeldes tillige e-læringskurser om god sagsbehandling og den gældende offentlighedslov.

I hvilke it-systemer hos borgerservicecentrene anvendes fortrolige oplysninger?

- Bilag 11. it-systemer, der anvendes i Borgerservice

Hvem er systemejere for de pågældende systemer?

- Bilag 11. it-systemer, der anvendes i Borgerservice

Er de pågældende systemer it-sikkerhedsgodkendt
Ja, se bilag 11.

Foretages der logning af anvendelse af personoplysninger? Og i givet fald hvorledes føres der tilsyn og hvor hyppigt?

- Oplysningerne om logning fremgår af bilag 12-15

Sekretariat & Presse

Rådhuspladsen 1
1550 København V

E-mail
dkrabb@kff.kk.dk

EAN nummer
5798009780515

www.kk.dk

Da fagsystemerne løbende logger transaktioner, er det kun ved konkrete mistanker, at der sammen med leverandøren og KS afdækkes faktiske forløb i enkeltsager. Fx har KMD sag en funktionalitet, hvor der er mulighed for at se logningen for en given sag.

I den forbindelse henledes Borgerrådgiverens opmærksomhed på, at man i KBS og KFF arbejder stringent med medarbejdertyper (jf. bilag 10), som i sig selv er en sikring af, at ansatte kun har adgang til data, som de skal bruge for at udføre deres arbejde.

Derudover er it-sikkerhedslederfunktionen henlagt til KS, hvor der typisk bør foretages stikprøvekontroller.

Hvorledes håndteres eventuelle brud på it-sikkerheden?
I de (ganske få) hændelser, der har været i borgerservicecentrene, er der øjeblikkelig taget kontakt til KS IT-Sikkerhed. På intranettet ligger der vejledning og link til indberetning af en sag.
http://ks.kkintra.kk.dk/indhold/it-sikkerhedsh%C3%A6ndelser

Enhver hændelse vil fremgå af den årlige it-sikkerhedsrapport.

Hvorledes følges der op på log-registreringer om afviste adgangsforsøg til it-systemerne i borgerservicecentrene, hvor der behandles fortrolige eller følsomme personoplysninger?
Der henvises til det ovenfor anførte vedr. it-sikkerhedslederfunktionen i KS..

Hvorledes håndterer borgerservicecentrene anmodninger om indsigt i oplysninger efter persondataloven?

- Bilag 16. Procedure ved anmodning om indsigt iht. PDL

Proceduren for dels håndtering af anmodninger om indsigt fremsat over for Borgerservice, dels for undersøgelse af, om der foreligger oplysninger/registreringer vedr. den pågældende borger

- Bilag 16. Procedure ved anmodning om indsigt iht. PDL

Når borger henvender sig med ønske om indsigt i egne oplysninger afklarer medarbejderen, hvilken type indsigtsanmodning der er tale om. I det omfang borgerne ønsker vejledning i at benytte selvbetjeningsløsningen på kk.dk, bistår medarbejderen til dette efter behov. Hvis borgerne ikke ønsker at benytte selvbetjeningsløsningen, tager medarbejderne imod borgernes henvendelse og formidler den videre til hhv. BR sekretariatet eller KS IT Sikkerhed til videre behandling.

Kopi af eksisterende procedurer, forretningsgange, retningslinjer, rutiner mv. hos borgerservicecentrene vedr. logning af elektronisk

sagsbehandling samt vedr. behandling af anmodninger om indsigt i oplysninger efter persondataloven

- Bilag 12-15

Herudover har Borgerrådgiveren anmodet om en udtalelse med en generel beskrivelse af, hvilke foranstaltninger borgerservicecentrene er ansvarlige for, og hvilke foranstaltninger borgerservicecentrene udfører, i relation til logning af elektronisk sagsbehandling.

I den forbindelse kan det oplyses, at borgerservicecentrene anvender forskellige fagsystemer til elektronisk sagsbehandling. Disse systemer er i forbindelse med ibrugtagning indmeldt i kommunens systemdatabase FISKK. Denne proces, der sker i samarbejde mellem Borgerservice og KS, sikrer, at det enkelte system lever op til gældende regler for it-systemer, herunder logning.

Udover de ovenfor nævnte bilag vedlægges diverse dokumenter under henvisning til Borgerrådgivningens anmodning om andet relevant materiale for inspektionen.

Med venlig hilsen

Thomas Jakobsen
Direktør

Bilag

Bilag 1.	Citizen 2015. Service- og kanalstrategi
Bilag 2.	Forklaring til borgertilfredshedsundersøgelse
Bilag 2a.	Forklaring til borgertilfredshedsundersøgelse
Bilag 3.	Rapport om God Adgang - BSC Bispebjerg
Bilag 4.	Folderen "Ny service i praksis"
Bilag 5.	Folderen "Tillidsfuld og effektiv kommunikation"
Bilag 6.	Oversigt over antal henvendelser og opgaver 2012-2014
Bilag 7.	Gennemsnitlige ventetider - 1. halvår 2014
Bilag 8.	Oversigtstegning BSC Bispebjerg
Bilag 9.	Velkomstbrev til nye it-brugere i KFF
Bilag 10.	Medarbejdertyper
Bilag 11.	Oversigt over it-systemer, der anvendes i Borgerservice
Bilag 12.	Logning KMD Sag
Bilag 13.	Logning CPR
Bilag 14.	Logning Skatekstranet
Bilag 15.	Logning ID-Port
Bilag 16.	Procedure ved anmodning om indsigt iht. PDL
Bilag 17.	Kvitteringssvar ved anmodning om indsigt iht. PDL

KØBENHAVNS KOMMUNE

Procedure for besvarelse af anmodning om indsigt efter persondatalovens § 31

Hvor kommer henvendelsen fra

Anmodningen kommer typisk enten fra BR Sekretariatet, hvor borgeren har henvendt sig på rådhuset eller fra Borgerservice, hvor borgeren har henvendt sig enten personligt, via mail, telefon eller som oftest via den elektronisk blanket, som Borgerservice lancerede i 2010. Når borgeren bruger denne blanket videresendes henvendelsen automatisk fra Borgerservices sikre postkasse til it-sikkerhedsfunktionens sikre postkasse, ksitsikkerhed@ks.kk.dk til videre foranstaltning.

Hvilke typer henvendelser

Der er primært 3 typer af anmodninger fra borgerne:

1. Anmodning om aktindsigt efter forvaltningsloven
   (Denne type drejer sig om indsigt i en eller flere konkrete sager/sagsforløb og skal besvares af den ansvarlige forvaltning, den videresendes til BR Sekretariatets fællespostkasse, brsek@okf.kk.dk til videre foranstaltning.)
2. Anmodning om indsigt efter persondatalovens § 31 fra borger, der er bosiddende i Københavns Kommune.
3. Anmodning om indsigt efter persondatalovens § 31 fra borger, der ikke er bosiddende i Københavns Kommune og ønsker at få slettet KKs dataabonnement på vedkommende.

It-sikkerhedsfunktionen har siden marts 2010 besvaret alle borger henvendelser af type 2 og 3.

Procedure ved besvarelse af Anmodning om indsigt efter persondatalovens § 31 fra borger, der er bosiddende i Københavns Kommune.

Først verificeres borgerens data ved et kontrolopslag i det centrale cpr register, https://webs.cpr.dk, da der kan være fejl i cpr nummer, navn eller andet. Desuden er man nødt til at være sikker på identiteten på borgeren, da andre kan udgive sig for vedkommende, og nogle gange kan der være tale om c/o adresser. Hvis borgeren har angivet et telefonnummer, kan man tit spare meget tid ved at kontakte vedkommende direkte og høre, hvad indsigten konkret drejer sig om, og hvordan den skal overleveres.

Der oprettes en sag på borgeren i e-Doc under den beskyttede sikkerbedsfacet; KS Sikkerhed, og handlingsfacet; A53(Aktindsigtsanmodning) med titlen: "Anmodning om indsigt 06-05-2013" (Eks.), hvor alle dokumenter i besvarelsen journaliseres.

Her efter sendes en kvittering til borgeren, så vedkommende ved, at anmodningen er modtaget samt, hvornår der kan forventes et svar. (Eks. på kvittering se bilag 1).

1

Indsamlingen af materialet om borgerens data fra de kommunale systemer foregår ved, at der udsendes en mail til systemejerne for alle it-systemer, der behandler personfølsomme data. Mailen sendes via postdistribueringslisten, KSDL Indsigt, der løbende vedligeholdes via dialog med systemejere og kontaktpersoner i alle forvaltninger. Nogle forvaltninger foretrækker at have kontorpostkasser på listen i stedet, og nogle foretrækker at have 2 personer pr. system. (Se bilag 2 for en udskrift over alle på listen)Personerne på listen melder altid ind, når der kommer nye systemer i forvaltningen, eller der sker udskiftninger blandt systemejerne. Listen er derfor dynamisk og altid up to date.

I mailen bedes alle svare tilbage med angivelse af, om der behandles data på borgeren i det system, man er ansvarlig for. Hvis svaret er positivt, skal der vedhæftes en udskrift med borgerens data samt et svar på de 4 spørgsmål, der er specificeret i persondatalovens § 31. Der skal også svares tilbage, hvis svaret er negativt. (Se eks. på mail i bilag 3).

Når fristen for personerne på listen til at svare tilbage er udløbet, samles alle svarene, alle de vedhæftede udskrifter skrives ud, og der sendes et samlet svar til borgeren. Dette svar sendes som regel anbefalet via Post DK, da der ifølge persondataloven kun må sendes elektronisk svar til borgeren, hvis denne har en sikker postkasse til at modtage krypteret post, hvilket er meget sjældent. (Se bilag 4 eks. på besvarelse til borgeren).

Til sidst journaliseres samtlige dokumenter og relevante mails i e-Doc under borgerens sag, som derefter lukkes.

Procedure ved besvarelse af Anmodning om indsigt efter persondatalovens § 31 fra borger, der ikke er bosiddende i Københavns Kommune.

Denne type sager adskiller sig ved, at borgeren som regel har henvendt sig til enten Borger.dk eller til cpr registret og har fået oplyst at andre kommuner end bopælskommunen har et aktivt abonnement på vedkommendes cpr nummer.

Borgeren henvender sig derfor til Københavns Kommune og spørger, hvorfor der abonneres på dennes cpr nummer, da vedkommende ikke bor i kommunen, og beder samtidigt om at dette abonnement omgående stoppes.

Proceduren her er fuldstændigt den samme med verificering af personens identitet i CPR 2, oprettelse af journal i e-Doc, afsendelse af kvitteringsskrivelse (Se bilag 5 for eks. på kvitteringsskrivelse)og høring blandt systemejerne via KSDL Indsigt.

I nogle tilfælde viser det sig, at opretholdelse af cpr abonnementet er helt legitimt, eftersom der er sager på borgeren. Det kan være fordi borgeren tidligere har boet i kommunen og har uafsluttede sager i form af restancer eller andet. Det kan også være fordi borgeren har været på besøg i Københavns Kommune og har modtaget en parkeringsbøde og derved er blevet registreret i kommunens systemer.

Hvis borgeren stadig har aktive sager registreret i kommunens systemer vil abonnementet ikke blive opsagt, hvilket borgeren informeres om.

I de fleste tilfælde er det dog ubegrundet, at man har abonnement på udenbys borgere, og det kan bero på enten fejlopslag af kommunens sagsbehandlere, fejl i it-systemerne eller at ældre inaktive sager på borgere, der tidligere har boet i kommunen, ikke er blevet slettet.

2

Her er det så kommunens ansvar at skrive til cpr registret og sikre, at abonnementet på borgeren stoppes (Se Bilag 6 for eks.). Her efter tilskrives borgeren om, at vedkommendes abonnement via cpr registret er opsagt (Se bilag 7 for eks.), og sagen lukkes.

3

KØBENHAVNS KOMMUNE

Anders And
Paradisæblevej 12
9713 Andeby

xx-xx-2013

Bekræftelse på henvendelse vedrørende indsigt

Du har henvendt dig dd-md-år for at få indsigt i de oplysninger, som Københavns Kommune har registreret om dig.

Vi betragter din henvendelse som en "anmodning om indsigt" efter persondatalovens § 31 i Lov nr. 429 af 31/05/2000 om behandling af personoplysninger.

Du kan forvente at få svar senest 4 uger fra dags dato. Svaret vil bestå af en kort beskrivelse af de systemer du optræder i, systemets navn og formålet med at behandle oplysninger om dig.

Du skal være opmærksom på, at hvis du ønsker indsigt i:

- Behandlingen af dine data i systemer med pas & kørekort skal du henvende dig til politiet
- Dine skattesager skal du henvende dig til Skat
- Dine data i forbindelse med udbetaling af: Børneydelse, underholdsbidrag, barselsdagpenge, boligstøtte eller social pension skal du henvende dig til Udbetaling Danmark.

Pas og kørekort
Rigspolitiet
IT og Tele
Landlystvej 34
2650 Hvidovre

SKAT
Skat
Personkontoret
Østbanegade 123
2100 København Ø

UDK
Udbetaling Danmark
Kongens Vænge 8
3400 Hillerød

Med venlig hilsen

Til systemejere i Københavns Kommune.

Dato: dd-md-år J.nr.: 2013-xxxxxxx
Vedrørende: CPR. nr.: yyyyyy-yyyy

Anders And
Paradisæblevej 1
4678 Andeby

Kommunen har modtaget en anmodning om indsigt efter § 31 i Lov nr. 429 af 31/05/2000 om behandling af personoplysninger.
IT-Sikkerhedsfunktionen skal derfor bede dig om at gå dit system igennem for behandling af den pågældende borger. Borger **skal IKKE have udskrifter fra systemet. Borger skal vide hvilken type oplysninger systemet arbejder med og hvorfor din forvaltning har lagt oplysninger ind i det om borgeren.** Hvis I ikke behandler oplysninger skal du besvare denne mail med et "Vi behandler ikke oplysninger om denne borger i system <systemnavn>".

Hvis I behandler oplysninger om borgeren skal dit svar være et Word dokument på din forvaltnings brevpapir med disse oplysninger om systemet.

1. Navn på it-systemet
2. At der behandles data på borgeren i systemet
3. Du skal på en let forståelig måde beskrive:
    a. Hvilke oplysninger der behandles
    b. Behandlingens formål
    c. Kategorierne af modtagere af oplysningerne /for eksempel:
    d. Tilgængelig information om, hvorfra disse oplysninger stammer

Du skal sende dit resultat til kskpitsikkerhed@ks.kk.dk.

Jeg skal bede dig om at **svare senest dd-md-år**. Vi printer alle de Word dokumenter som vi modtager og sender dem i et samlet svar til borgeren i et anbefalet brev med forklarende følgeskrivelse.

KØBENHAVNS KOMMUNE

Fætter Højben
Gyldenlykkesgade 48 st. tv.
9814 Gåserød

Dato: xx-xx-2013 / j.nr.: 2013-xxxxx

Svar på henvendelse om indsigt

Du har henvendt dig og bedt om indsigt efter persondatalovens § 31 i alle de oplysninger, som Københavns Kommune behandler om dig.

Jeg sender her svar på din anmodning. Svaret indeholder en fortegnelse over alle de IT-systemer i Københavns Kommune, som behandler dine data.

Hvis du senere vil søge om aktindsigt i nogle af sagerne, skal du enten henvende dig på Københavns Rådhus eller i den pågældende forvaltning (se www.kk.dk for adresser)

Jeg skal også henlede din opmærksomhed på, at hvis du ønsker at klage over behandlingen af oplysninger, som vedrører dig, kan du rette henvendelse til Datatilsynet, Borgergade 28, 5., 1300 København K.

Med venlig hilsen

BILAG 6 – OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN

Kultur- og Fritidsforvaltningen - direktionen

26-05-2015

Sagsnr.
2014-0118160

Dokumentnr.
2014-0118160-5

Sendt pr. mail _____ _____ _____ _____ _____

Vedrørende Borgerrådgiverens egen drift-undersøgelse af logning af elektronisk sagsbehandling og borgeres adgang til indsigt i personoplysninger – forvaltningens j. nr. 2014-0171930

Borgerrådgiveren er i færd med at udarbejde den forelobige rapport vedrørende ovenstående undersøgelse.

Med henvisning til Kultur- og Fritidsforvaltningens høringssvar af 16. september 2014 og vedlagte bilag skal jeg bede forvaltningen om at svare på følgende opklarende spørgsmål:

1. Er det korrekt forstået, at forvaltningen alene er ansvarlig for og har udpeget systemejere til følgende it-systemer: CPR2, Notus Kommunal, P-Data, Pas- og Kørekortregisteret samt ID-Port-Admin (jf. bilag 11 med oversigt over it-systemer)?

Forvaltningen har ikke vedlagt dokumentation for logning i it-systemet Notus Kommunal. I bilag 11 med oversigt over it-systemer er der markeret med * ved Notus Kommunal og anført følgende: "Kontaktet CSC pr. telefon 11/9: de har videresendt min mail Oplyser at de kun logger ved ændringer".

2. Kultur- og Fritidsforvaltningen bedes be- eller afkræfte, at det pågældende it-system logger, som påkrævet efter sikkerhedsbekendtgørelsens § 19?

Det er uklart for Borgerrådgiveren, hvorvidt leverandørerne, jf. bilag 11, udfører behandlinger af følsomme personoplysninger, logninger og/eller udfører kontrol med afviste adgangsforsøg og/eller log opfølgning.

3. Kultur- og Fritidsforvaltningen bedes be- eller afkræfte, hvorvidt dette er tilfældet? I tilfælde af et bekræftende svar beder jeg forvaltningen om at svare på følgende:
   3.1. Hvilke it-systemer/leverandører er der tale om?
   3.2. Hvilke opgaver udfører leverandørerne?
   3.3. Har forvaltningen indgået databehandleraftaler med leverandørerne vedrørende opgaverne?

Borgerrådgiveren

Vester Voldgade 2A
1552 København V

Telefon
3366 1400

Telefax
3366 1390

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

www.kk.dk/borgerraadgiveren

3.4. Hvilket tilsyn fører forvaltningen med leverandørernes udførelse af opgaverne?

Borgerrådgiveren beder om svar på spørgsmålene inden 4 uger.

Eventuelle spørgsmål kan rettes til Daniel Soelberg Bach, tlf. nr. 8220 5211.

Med venlig hilsen

Johan Busse
Borgerrådgiver

/Daniel Soelberg Bach
Jurist

BILAG 7 – KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Sekretariat & Presse

05-10-2015

Borgerrådgiveren

Sagsnr.
2014-0171930

Dokumentnr.
2014-0171930-8

Svar til Borgerrådgiveren på supplerende spørgsmål om logning af brug af personoplysninger

Borgerrådgiveren har ved brev af 26. maj 2015 stillet en række supplerende spørgsmål til Kultur- og Fritidsforvaltningens svar af 16. september 2014.

Der blev den 25. august 2015 afholdt et afklarende med jurist Daniel Soelberg Bach om sagen.

Forvaltningens svar på spørgsmålene følger nedenfor.

1. Er det korrekt forstået, at forvaltningen alene er ansvarlig for og har udpeget systemejere til følgende it-systemer: CPR2, Notus Kommunal, P-Data, Pas- og Korekortregisteret samt ID-Port-Admin (jf. bilag 11 med oversigt over it-systemer)?

Svar:
KFF har 137 systemer registreret i FISKK, som er kommunens register over systemer. Alle systemer har en udpeget systemejer.

Heraf er der 5 systemer (bilag 11), som behandler personhenførbare oplysninger (cpr.numre).

*Forvaltningen har ikke vedlagt dokumentation for logning i it-systemet Notus Kommunal. I bilag 11 med oversigt over it-systemer er der markeret med * ved Notus Kommunal og anført følgende: "Kontaktet CSC pr. telefon 11/9: de har videresendt min mail Oplyser at de kun logger ved ændringer".*

2. Kultur- og Fritidsforvaltningen bedes be- eller afkræfte, at det pågældende it-system logger, som påkrævet efter sikkerhedsbekendtgørelsens § 19?

Svar:
Borgerrådgiverens inspektion og spørgsmål har afklaret, at Notus Kommunal desværre ikke lever fuldt op til kravene i § 19, idet CSC oplyser, at systemet ikke logger søgninger. CSC oplyser, at de mod betaling kan udvikle denne facilitet til Notus Kommunal på bestilling fra Københavns Kommune. Systemet er et system, der har været anvendt landsdækkende i en del år.

Sekretariat & Presse

Rådhuspladsen 1
1550 København V

E-mail
dkrabb@kff.kk.dk

EAN nummer
5798009780515

www.kk.dk

Da der af KOMBIT er bestilt og udviklet et nyt system, Praksys, der ultimo 2016 afløser Notus Kommunal, og Notus Kommunal således aktuelt er at betragte som under udfasning, er det på nuværende tidspunkt KFF's vurdering, at udvikling af en logfunktion i forhold til søgninger ikke er hensigtsmæssig. I denne betragtning indgår blandt andet udviklingstid og test.

Det bemærkes, at KFF er i dialog med IT-sikkerhed i KS vedr. manuelle stikprøver af opslag, og at vi i den forbindelse har bedt IT-sikkerhed om hjælp til at udarbejde en procedure, som skal implementeres i indeværende år.

Endelig har KFF – blandt andet på baggrund af erfaringerne fra Borgerrådgiverens inspektion og spørgsmål - rettet henvendelse til KOMBIT's projektleder for Praksys og forespurgt, om man har taget højde for persondataloven i kravspecifikationen. KOMBIT har svaret bekræftende herpå.

Det er uklart for Borgerrådgiveren, hvorvidt leverandørerne, jf. bilag 11, udfører behandlinger af følsomme personoplysninger, logninger og/eller udfører kontrol med afvist adgangsforsøg og/eller log opfølgning.

3. Kultur- og Fritidsforvaltningen bedes be- eller afkræfte, hvorvidt dette er tilfældet? I tilfælde af et bekræftende svar beder jeg forvaltningen om at svare på følgende:
3.1. Hvilke it-systemer/leverandører er der tale om?
3.2. Hvilke opgaver udfører leverandørerne?
3.3. Har forvaltningen indgået databehandleraftaler med leverandørerne vedrørende opgaverne?
3.4. Hvilket tilsyn fører forvaltningen med leverandørernes udførelse af opgaverne?

Svar:
Systemerne i bilag 11 indeholder ikke følsomme personoplysninger, bortset fra KMD Sag, hvor der kan være oplysninger, der kan relatere sig til helbred, fx udlånte hjælpemidler eller handicapbefordring.

Generelt gælder, at der ved enhver anskaffelse af et IT-system over for KS IT-Sikkerhed bl.a. skal redegøres for systemets logning mv.

Det er i øvrigt gældende procedure, at der indgås databehandleraftale, når der anskaffes nye IT-systemer.

For så vidt angår tilsyn med leverandørens udførelse af opgaverne, modtager Københavns Kommune årligt to revisorerklæringer fra

KMD's eksterne revisor, der vurderer KMD's evne til at levere IT-ydelser til KK.

- ISAE 3402-erklæring for generelle IT-kontroller
- ISAE 3000-erklæring vedr. overholdelse af persondataloven

Disse revisioner gennemgås af Koncernservices IT-sikkerheds-funktion, der bidrager, hvis der er observationer, der kræver en indsats for at styrke sikkerheden.

Med venlig hilsen

Dennis Krabbe Sørensen
Specialkonsulent, cand.jur.

BILAG 8 – BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL SOCIALFORVALTNINGEN

KØBENHAVNS KOMMUNE
Borgerrådgiveren

07-07-2016

Til Socialforvaltningen

Sagsnr.
2014-0118160

Sendt dags dato

Dokumentnr.
2014-0118160-15

Overførsel af generel egen drift-undersøgelse om logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag

Borgerrådgiveren iværksatte ved brev af 8. august 2014 til Kultur- og Fritidsforvaltningen en generel egen-drift undersøgelse om logning af Københavns Borgerservices elektroniske sagsbehandling efter persondataloven.

Undersøgelsen er afgrænset til logning af elektronisk sagsbehandling i it-systemer, hvor Københavns Borgerservice behandler følsomme personoplysninger.

Kultur- og Fritidsforvaltningen har ved brev af 5. oktober 2015, herunder ved e-mail af 10. juni 2016, oplyst, at Københavns Borgerservices it-systemer ikke indeholder følsomme personoplysninger, bortset fra KMD Sag, hvor der kan være følsomme personoplysninger, som relaterer sig til helbred.

Det fremgår af materialet, som Borgerrådgiveren har modtaget fra Kultur- og Fritidsforvaltningen, at der er udpeget en systemejer fra Socialforvaltningen til it-systemet KMD Sag, hvor Københavns Borgerservice behandler følsomme personoplysninger.

Det følger af Regulativ for it-sikkerhed i Københavns Kommune, at systemejer til it-systemer skal sikre, at it-systemerne kan logge behandling af data, når dette er påkrævet (se § 11, stk. 7, i regulativet). Det følger af de uddybende it-sikkerhedsregler for kommunen, at systemejer skal foretage log opfølgning på afviste adgangsforsøg samt log opfølgning på data med henblik på at identificere uhensigtsmæssigheder (se afsnit 10.10. om logning i de uddybende regler).

Da der er udpeget en systemejer fra Socialforvaltningen til it-systemet KMD Sag, hvor Københavns Borgerservice behandler følsomme personoplysninger, har Borgerrådgiveren besluttet at overføre generel egen drift-undersøgelsen om logning af Københavns Borgerservices elektroniske sagsbehandling til Socialforvaltningen. Borgerrådgiveren har dags dato orienteret Kultur- og Fritidsforvaltningen herom.

Borgerrådgiveren

Vester Voldgade 2A
1552 København V

Telefon
3366 1400

Telefax
3366 1390

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

www.kk.dk/borgerraadgiveren

Anmodning om udtalelse fra Socialforvaltningen og besvarelse af spørgsmål
Borgerrådgiveren beder om en udtalelse fra Socialforvaltningen vedrørende Socialforvaltningens logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Borgerrådgiveren beder særligt om, at Socialforvaltningen svarer på følgende spørgsmål:

- Hvorledes sker der logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag?

- Foretages tilsyn med logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag? Og i givet fald hvorledes føres der tilsyn og hvor hyppigt?

- Hvorledes håndteres eventuelle brud på it-sikkerheden (jf.*) i forbindelse med Københavns Borgerservices sagsbehandling i it-systemet KMD Sag?

- Hvorledes følger Socialforvaltningen op på log-registreringer om afviste adgangsforsøg til it-systemet KMD Sag i Københavns Borgerservice?

(*Med brud på it-sikkerheden menes her: konstateringer eller formodninger om uberettiget videregivelse af borgernes personoplysninger, og/eller konstateringer eller formodning om, at medarbejdere uberettiget skaffer sig adgang til borgernes personoplysninger).

Anmodning om dokumentation
Borgerrådgiveren beder om at modtage kopi af eksisterende procedurer, forretningsgange, retningslinjer, rutiner mv. hos Socialforvaltningen vedrørende logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Borgerrådgiveren beder om at modtage forvaltningens svar samt dokumentation inden 6 uger fra dags dato.

Kopi af Borgerrådgiverens iværksættelsesbrev af 8. august 2014 vedlægges til Socialforvaltningens orientering (alene side 3-5 er relevant for undersøgelsen).

Kopi af bilag 11 (oversigt over it-systemer hos Københavns Borgerservice) samt bilag 12 (beskrivelse af logning i KMD Sag) modtaget fra Kultur- og Fritidsforvaltningen vedlægges til Socialforvaltningens orientering.

Eventuelle spørgsmål kan rettes til undertegnede.

Med venlig hilsen
For Borgerrådgiveren

/Daniel Soelberg Bach
Jurist

BILAG 9 – HØRINGSSVAR FRA SOCIAL-FORVALTNINGEN

Af mail af 12. august 2016 fra Socialforvaltningen fremgår følgende som svar på Borgerrådgiverens brev af 7. juli 2016:

> ”Det fremgår af din henvendelse af 7. juli 2016, at Kultur- og Fritidsforvaltningen over for Borgerrådgiveren har oplyst, at Socialforvaltningen er systemejer for it-systemet KMD Sag, som Københavns Borgerservice behandler følsomme personoplysninger i.
>
> Vi har undersøgt sagen, og er kommet frem til, at der må være tale om en misforståelse. Socialforvaltningen kan oplyse, at vi er ikke systemejer til it-systemet KMD Sag, men derimod Koncern IT (Økonomiforvaltningen). Dette fremgår af nedenstående link:
> http://fiskk2.ks.kk.dk/systemInfo?id=343”

BILAG 10 – BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL ØKONOMIFORVALTNINGEN

KØBENHAVNS KOMMUNE
Borgerrådgiveren

15-08-2016

Til Økonomiforvaltningen

Sagsnr.
2014-0118160

Sendt dags dato

Dokumentnr.
2014-0118160-24

Overførsel af generel egen drift-undersøgelse om logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag

Borgerrådgiveren iværksatte ved brev af 8. august 2014 til Kultur- og Fritidsforvaltningen en generel egen-drift undersøgelse om logning af Københavns Borgerservices elektroniske sagsbehandling efter persondataloven.

Undersøgelsen er afgrænset til logning af elektronisk sagsbehandling i it-systemer, hvor Københavns Borgerservice behandler følsomme personoplysninger.

Kultur- og Fritidsforvaltningen har ved brev af 5. oktober 2015, herunder ved e-mail af 10. juni 2016 oplyst, at Københavns Borgerservice alene behandler følsomme personoplysninger i it-systemet KMD Sag.

Kultur- og Fritidsforvaltningen har oplyst, at Socialforvaltningen er systemejer til it-systemet KMD Sag, hvorfor Borgerrådgiveren ved brev af 7. juli 2016 overførte generel egen drift-undersøgelsen til Socialforvaltningen.

Socialforvaltningen har efterfølgende ved e-mail af 12. august 2016 oplyst til Borgerrådgiveren, at der er udpeget en systemejer i Koncernservice til it-systemet KMD Sag. Systemejeren i Koncernservice har bekræftet dette ved e-mail af 15. august 2016 til Borgerrådgiveren.

Det følger af Regulativ for it-sikkerhed i Københavns Kommune, at systemejer til it-systemer skal sikre, at it-systemerne kan logge behandling af data, når dette er påkrævet (se § 11, stk. 7, i regulativet).

Det følger af de uddybende it-sikkerhedsregler for Københavns Kommune, at systemejer til it-systemer, skal foretage log opfølgning på afviste adgangsforsøg samt log opfølgning på data med henblik på at identificere uhensigtsmæssigheder (se afsnit 10.10. om logning i de uddybende regler).

Borgerrådgiveren

Vester Voldgade 2A
1552 København V

Telefon
3366 1400

Telefax
3366 1390

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

www.kk.dk/borgerraadgiveren

Da der er udpeget en systemejer fra Koncernservice til it-systemet KMD Sag, hvor Københavns Borgerservice behandler følsomme personoplysninger, har Borgerrådgiveren dags dato besluttet at overføre generel egen drift-undersøgelsen om logning af Københavns Borgerservices elektroniske sagsbehandling til Økonomiforvaltningen.

Borgerrådgiveren har dags dato orienteret Kultur- og Fritidsforvaltningen samt Socialforvaltningen om, at undersøgelsen er overført til Økonomiforvaltningen.

Anmodning om udtalelse fra Økonomiforvaltningen og besvarelse af spørgsmål
Borgerrådgiveren beder om en udtalelse fra Økonomiforvaltningen vedrørende Koncernservices logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Borgerrådgiveren beder særligt om, at Økonomiforvaltningen svarer på følgende spørgsmål:

- Hvorledes sker der logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag?
- Foretages tilsyn med logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag? Og i givet fald hvorledes føres der tilsyn og hvor hyppigt?
- Hvorledes håndteres eventuelle brud på it-sikkerheden (jf.*) i forbindelse med Københavns Borgerservices sagsbehandling i it-systemet KMD Sag?
- Hvorledes følger Koncernservice op på log-registreringer om afviste adgangsforsøg til it-systemet KMD Sag i Københavns Borgerservice?

(*Med brud på it-sikkerheden menes her: konstateringer eller formodninger om uberettiget videregivelse af borgernes personoplysninger, og/eller konstateringer eller formodning om, at medarbejdere uberettiget skaffer sig adgang til borgernes personoplysninger).

Anmodning om dokumentation
Borgerrådgiveren beder om at modtage kopi af eksisterende procedurer, forretningsgange, retningslinjer, rutiner mv. hos Koncernservice vedrørende logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Borgerrådgiveren beder om at modtage Økonomiforvaltningens svar samt dokumentation inden 4 uger fra dags dato.

Kopi af Borgerrådgiverens iværksættelsesbrev af 8. august 2014 til Kultur- og Fritidsforvaltningen vedlægges til Økonomiforvaltningens orientering (alene side 3-5 er relevant for undersøgelsen).

Kopi af bilag 11 (oversigt over it-systemer hos Københavns Borgerservice) samt bilag 12 (beskrivelse af logning i KMD Sag) modtaget fra Kultur- og Fritidsforvaltningen vedlægges til Økonomiforvaltningens orientering.

Eventuelle spørgsmål kan rettes til undertegnede.

Med venlig hilsen
For Borgerrådgiveren

/Daniel Soelberg Bach
Jurist

BILAG 11 – HØRINGSSVAR FRA ØKONOMI-FORVALTNINGEN OG UDVALGT DOKU-MENTATION

KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Direktionen

05-09-2016

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

Sagsnr.
2016-0310076

Dokumentnr.
2016-0310076-11

Svar fra Økonomiforvaltningen på Borgerrådgiverens egen drift-undersøgelse om logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Økonomiforvaltningen har den 15. august 2016 fra Borgerrådgiveren modtaget en anmodning om en udtalelse, herunder besvarelse af en række spørgsmål, samt fremsendelse af kopi af eksisterende procedurer, forretningsgange, retningslinjer, rutiner mv. på området vedrørende logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemet KMD Sag.

Økonomiforvaltningen har i den forbindelse anmodet Koncern IT om bemærkninger til spørgsmålene i undersøgelsen (området hørte tidligere under Koncernservice, men er i forbindelse med en organisationsændring i foråret 2016 overgået til den nyoprettede enhed Koncern IT).

På baggrund af det modtagne svar fra Koncern IT fremsendes hermed Økonomiforvaltningens udtalelse med besvarelse af Borgerrådgiverens spørgsmål. Relevant materiale (procedurer, retningslinjer mv.) er vedlagt som bilag.

Borgerrådgiveren har stillet 4 spørgsmål i henvendelsen:

1) Hvorledes sker der logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag?

2) Foretages tilsyn med logning af Københavns Borgerservices anvendelse af personoplysninger i it-systemet KMD Sag? Og i givet fald hvorledes føres der tilsyn og hvor hyppigt?

3) Hvorledes håndteres eventuelle brud på it-sikkerheden i forbindelse med Københavns Borgerservices sagsbehandling i it-systemet KMD Sag?

4) Hvorledes følger Koncernservice op på log-registreringer om afviste adgangsforsøg til it-systemet KMD Sag i Københavns Borgerservice?

Ad spørgsmål 1:
Måden, der foretages logning i KMD Sag, er som udgangspunkt delt i to.

Direktionen

Københavns Rådhus,
Rådhuspladsen 1
1599 København V

E-mail
Mikkel.Hemmingsen@okf.kk.dk

EAN nummer
5798009800299

www.kk.dk

På borgernes sag i KMD Sag logges følgende:

- Brugere, der er tilgået sagen
- Hvilke sager, der er tilgået
- Hvad brugerne har foretaget sig på sagen, f.eks. indberetninger/ændringer, registrering af journal/notater
- Tidspunktet for seneste anvendelse.

Der henvises til vedlagte bilag 2, "Kopi af bilag 12 Logning KMD Sag". Hertil skal det bemærkes, at det ikke er muligt at foretage direkte udtræk af logninger fra KMD Sag.

I KMD's it-sikkerhedssystem KSP-CICS logges hvilke brugere, der har tilgået hvilke applikationer, hvilke skærmbilleder og hvornår disse er tilgået. Det er via KSP-CICS muligt at foretage udtræk på den givne anvendelse i KMD Sag. Blandt andet kan der vises brugerstatistik over anvendelsen af autoriserede og uautoriserede transaktionskoder, funktioner eller applikationer inden for den pågældende administrative enhed, den enkelte bruger er tilknyttet. Bemærk, at dette blot er én ud af flere måder at foretage udtræk via KSP-CICS. Andre og mere detaljerede beskrivelser af udtræksmulighederne fremgår af det vedlagte bilag 1, "KMD-HDB-086 KMDCICS Administration". Foretaget udtræk lagres desuden i Doc2Archive.

Ad spørgsmål 2:
It-sikkerhedsfunktionen har i 2015 bistået Københavns Borgerservice (KBS) med vejledning med hensyn til, hvorledes KBS kan sikre den ønskede kontrol af logs. It-sikkerhedsfunktionen har herefter, jf. vedlagte Bilag 4, udarbejdet generel vejledning vedr. "Krav om stikprøver af loggen i borgerservicecentre". I denne vejledning blev det specifikt anbefalet, at KMD Sag skulle omfattes af kontrollen.

Senere i 2015 har It-sikkerhedsfunktionen, jf. Bilag 5, udarbejdet mere operationelle planer for gennemførsler af log-kontroller, inkluderende best practices, og endvidere bistået i møder med forvaltningen mm.

På den baggrund gennemførte KBS en række stikprøvekontroller af medarbejderes anvendelse af bl.a. KMD Sag. Kontrolrapporter blev fremsendt til It-sikkerhedsfunktionen 29. december 2015.

It-sikkerhedsfunktionens tilsyn med det fremsendte materiale viste, at stikprøverne var hensigtsmæssigt udført.

Udover gennemførelse af stikprøver som beskrevet i bilagene er det i praksis meget vanskeligt for forvaltningerne at følge op på meget store mængder af logs i fagsystemer.

Derfor blev det med Handlingsplan til forbedring af It-sikkerheden (vedtaget af Borgerrepræsentationen den 28. april 2015) besluttet, at der skulle bevilges anlægsmidler til anskaffelse og drift af en central overvågningsløsning i form af et såkaldt "SIEM-system".

Med denne løsning overdrages ansvaret for opfølgning på logs efter aftale med forvaltningerne til Koncern IT i takt med, at det enkelte system er klargjort til at overføre logs til den centrale SIEM-løsning, og herefter sker der en automatiseret logkontrol, som overvåger forud definerede logevents.

Dette imødekommer problemstillingen, der har været vanskelig at løse for forvaltningerne og disses systemejere.
It-sikkerhedsfunktionens monitoreringsteam, der arbejder med SIEM, har oplyst, at den tekniske afklaring vedr. central overvågning af logs fra både KMD Sag og KMD CICS gennemføres i 2016. Herefter skal systemerne tilpasses, så logs kan overføres. Den endelige tidsplan vil afhænge af den tekniske afklaringsproces.

Ad spørgsmål 3:
Håndtering af brud på sikkerheden i it-systemet KMD Sag følger samme retningslinjer, som alle andre it-systemer er underlagt. Den generelle proces fremgår af de Uddybende it-sikkerhedsregler pkt. 13, samt pkt. 10.10.1 ift. it-sikkerhedsrapporter ved udtræk af data ved begrundet mistanke. Se endvidere bilag 3, "Udtræk af data fra log ved mistanke om misbrug (personalesag) – vejledning", der også fremgår af it-sikkerhedshåndbogen.

Ad spørgsmål 4:
I henhold til Regulativ for it-sikkerhed i Københavns Kommune er forvaltningernes systemejere ansvarlige for at følge op på log-registreringer om afviste adgangsforsøg.

It-sikkerhed har til opgave at sikre, at systemet ved implementeringen er i stand til at leve op til kommunens it-sikkerhedsregler, hvilket bl.a. inkluderer logningskravet på anmeldelsespligtige databehandlerbehandlinger.

Koncern IT udfører efter aftale med Socialforvaltningen systemejeropgaven for KMD Sag. Systemejer på KMD Sag har oplyst, at der bliver foretaget udtræk af loggen ved begrundet mistanke. Sådanne udtræk vil følge de Uddybende it-sikkerhedsregler pkt. 10.10.1 vedr. behandlingen af it-sikkerhedsrapporter.

Som nævnt ovenfor er systemet KMD Sag endnu ikke blevet klargjort til overførsel af logs til SIEM-løsningen. Arbejdet påbegyndes i efteråret 2016, og når de tekniske forberedelser er gennemført, vil opfølgning på afviste adgangsforsøg via loggen blive foretaget af It-

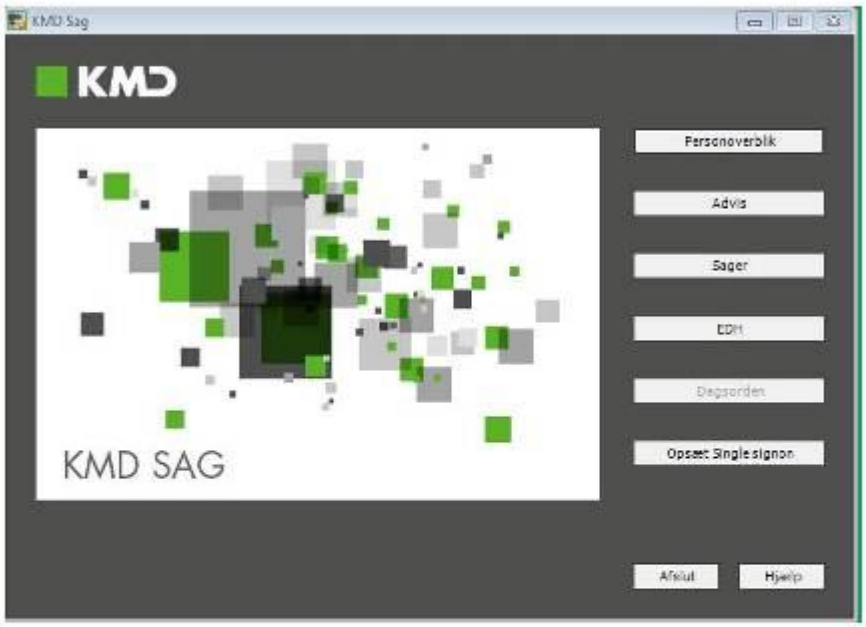
sikkerhed gennem automatiseret kontrol, der vil gøre systemejer opmærksom på mistænkelig trafik eller procesafvikling i dennes system.

Bilag:
Bilag 1: KMD-HDB-086 KMDCICS Administration
Bilag 2: Kopi af Bilag 12 Logning KMD Sag
Bilag 3: Udtræk af data fra log ved mistanke om misbrug (personalesag) – vejledning
Bilag 4: Generel vejledning vedr. krav om stikprøver af loggen i borgerservicecentre
Bilag 5: Best practice for gennemførelse af stikprøvekontrol af loggen

Med venlig hilsen

Mikkel Hemmingsen
Adm. direktør

Logning i KMD Sag



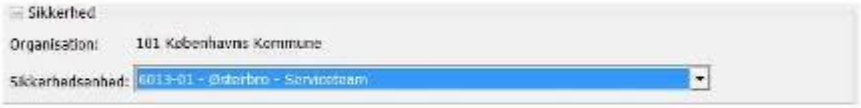
Som det ses af forsiden er KMD Sag opbygget af flere moduler. Derfor gennemgås det enkelte moduls logningsfunktionalitet for sig selv.

Generelt:

KMD Sag logger i henhold til Persondataloven.

For at komme ind i KMD Sag, skal man være autoriseret (via KS). Der logges på med C1+ens egen brugerident. Og Der skal vælges en adgangskode på 8 karakter. Koden skal skiftes efter 3 mdr. sker det ikke bliver brugeren gjort indaktiv og må den vej af KS for at få åbnet for adgangen igen. En kode der engang har været brugt kan ikke anvendes igen før der er gået 12 mdr.

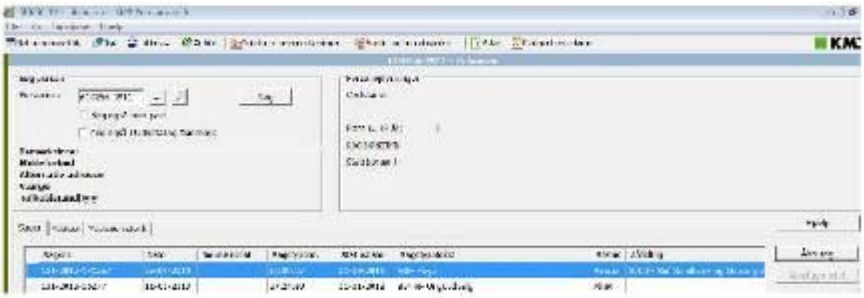
Adgangen til KMD Sag er yderligere begrænset via sikkerhedsenheder:



Den enkelte bruger bliver kun autoriseret til den eller de sikkerhedsenheder der er relevant(e) i forhold til opgavevaretagelsen. Det betyder, at man ikke kan se sager der ligger på andre sikkerhedsenheder end dem man er autoriseret til.

Personoverblikket:

Der logges ikke i selve personoverblikket (Bemærk venligst, at der er brugt et fiktivt cpr.nr.)



Det er først i det øjeblik, at sagsbehandleren vælger at åbne en sag, at der bliver logget i skærmdumpet ovenfor, åbnes den sag, der er markeret med blåt, hvorefter man springer over i Modulet sager.

- 2 -

(…) ” (side 3-6 er udeladt).

KØBENHAVNS KOMMUNE

Udtræk af data fra log ved mistanke om misbrug – vejledning.

Et udtræk af data fra loggen, som viser hvilke transaktioner en medarbejder har udført i et givent system i et givent tidsrum, kaldes en IT-sikkerhedsrapport.

Som personaleleder vil man sandsynligvis kun meget sjældent stå i en situation hvor man har behov for at bestille en IT-sikkerhedsrapport, og typisk sker det i en situation, hvor der er betydeligt internt og eksternt pres på den enkelte leder.
Derfor er formålet med denne vejledning at give den ansvarlige personaleleder og andre interessenter i forvaltningen et overblik over proces og retningslinjer.

Hvornår kan der bestilles IT-sikkerhedsrapporter

Hvis forvaltningens ledelse har begrundet mistanke til en medarbejder om misbrug og strafbare forhold.

Hvilke systemer kan levere udtræk fra log.

Typisk økonomisystemer og fagsystemer der behandler fortrolige og følsomme personoplysninger.
Er der behov kan der leveres udtræk fra mailsystemet, PC log og muligvis printer logs.

Sådan bestilles og udleveres IT-sikkerhedsrapporter

- **Forvaltningen** henvender sig til forvaltningens sagsbehandler hos Personalejura og Forhandling i Koncernservice. Det vil som udgangspunkt være den ansvarlige personaleleder, der tager kontakten, men forvaltningen kan vælge at udpege en anden ansvarlig kontaktperson.
  Forvaltningen skal sende en mail til sagsbehandler med en fyldestgørende begrundelse for anmodningen om udlevering af IT-sikkerhedsrapporter. Anmodningen skal indeholde følgende informationer:

  Info om den berørte medarbejder:
  Forvaltning, Afdeling, Kontor.
  Medarbejders navn og brugerident.
  Navn på system der ønskes udtræk fra.
  Hvilke oplysninger der ønskes.
  Periode der ønskes udtræk for.(der er normalt mulighed for udtræk 6 måneder bagud)
  Begrundelse: *Hvorfor ?*
  Info om bestilleren: *Navn, Stilling*

- **KS** Personalejura & Forhandling vil på baggrund af mail og dialog med forvaltningens kontaktperson vurdere, om der er en tilstrækkelig personalejuridisk begrundelse for at foretage logudtræk. Er det tilfældet videresender Personalejura og Forhandling anmodningen fra forvaltningens kontaktperson til IT-sikkerhed i KS.

- Forvaltningens kontaktperson vil herefter få en kontaktperson hos IT-sikkerhed, Den pågældende varetager den videre kontakt med forvaltningen og står til rådighed, hvis der er spørgsmål eller behov for afklaring i forbindelse med bestillingen. Kontaktpersonen rådgiver om IT-sikkerhedsspørgsmål i sagen, vil sikre forventningsafstemning med forvaltningen og herunder bede forvaltningen meddele, om andre i forvaltningen skal inddrages i den videre proces.

- **KS** IT-sikkerhed sørger nu for at bestiller de nødvendige logudtræk hos de relevante systemejere.
  IT-sikkerhed sender kvittering til forvaltningens kontaktperson når logudtrækkene er bestilt.
  Når IT-sikkerhed modtager IT-sikkerhedsrapporten fra systemejeren, videresendes denne til

forvaltningens kontaktperson, og sagsbehandleren i Personalejura & Forhandling sættes CC på mailen. IT-sikkerhed anfører i mailen, hvem der er systemejer i relation til de(t) system(er), som logudtrækket vedrører.

- **Forvaltningens kontaktperson** modtager IT-sikkerhedsrapporten til brug for det videre sagsforløb, som sker i dialog med KS Personalejura og Forhandling, indtil sagen er afsluttet. Er der behov for hjælp til at læse og tolke indholdet af IT-sikkerhedsrapporten/logudtrækket, skal forvaltningens kontaktperson kontakte systemejeren for det enkelte system. Kontaktpersonen fra IT-sikkerhed medvirker til processen i nødvendigt omfang.

Fortrolighed under opbevaring og håndtering

Kontaktpersonen fra IT-sikkerhed vil i processen informere om hvordan IT-sikkerhedsrapporten skal håndteres, så fortrolige oplysninger ikke kommer til uvedkommendes kendskab.

IT-sikkerhedsrapporten skal opbevares sikkert, og skal destrueres så snart forholdet er endeligt afklaret og/eller der ikke længere af bevismæssige årsager til at opbevare rapporten.

KØBENHAVNS KOMMUNE
Koncernservice
Digitalisering

NOTAT

18-09-2015

Til KFF
Københavns Borgerservice

Sagsnr.
2015-0076634

Dokumentnr.
2015-0076634-2

Sagsbehandler
Kirsten Wenning

Krav om stikprøver af loggen i borgerservicecentre

Datatilsynet stiller krav om at kommuner, der etablerer borgerservicecentre, skal foretage stikprøvekontrol af loggen.

Formålet med en stikprøvekontrol er dels at afsløre eventuelt misbrug, dels at forebygge misbrug.

Datatilsynet har i forbindelse med inspektioner i andre kommuner udtalt at tilsynet finder det meget beklageligt, når en Kommune ikke har levet op til kravene. Dvs. ved ikke på eget initiativ, med jævne mellemrum og med vilkårlige intervaller at have foretaget stikprøvekontroller af loggen.

Det anbefales derfor at Københavns Kommunes Borgerservice foretager stikprøver af loggen efter Datatilsynets henstilling.

Koncept for stikprøver af loggen hos KFF KBS.
På baggrund af Datatilsynets publikation " Datasikkerhed i borgerservicecentre" og informationer fra KFF/KBS anbefaler KS It-sikkerhed:

Borgerservice udpeger 2 tilsynsførende medarbejdere, som har ansvar for at gennemføre stikprøvekontrollerne.

Stikprøverne skal falde med forskellige intervaller, f.eks. 2½ måned, 5 måneder, osv., dog højst 6 måneder. Planlagte datoer for stikprøver fremgår af et bilag, som kun de tilsynsførende medarbejdere har adgang til.
Der udvælges ca. 10 tilfældige medarbejdere pr. kontrol.
Medarbejderne skal naturligvis ikke være bekendt med udvælgelsen.
Stikprøverne foretages af de opslag, som borgerservicecentermedarbejderne foretager i de logningspligtige it-systemer
En stikprøve omfatter 5 – 6 opslag foretaget 1 – 3 dage før, medarbejderen anmodes om at redegøre for årsagen til opslagene.

Log udskrifter bestilles af de tilsynsførende hos de respektive systemejere.
Københavns Borgerservice udpeger på baggrund af de systemer, processer og rettighedstildelinger der anvendes hvilke logningspligtige systemer der er relevante at kontrollere.
Borgerservice har selv tidligere peget på at der foretages opslag i

Digitalisering

Borups Allé 177
2400 København NV

Telefon [redacted]

Mobil [redacted]

EAN nummer
5798009809308

følgende systemer, som vi anbefaler indgår i stikprøvekontrollen: KMD Sag, CPR og Kommunal Sygesikring. Borgerservice identificerer øvrige systemer, som bør indgå.

Stikprøverne forelægges de berørte medarbejdere, som noterer hvad årsagen til opslagene var (evt. journalnumre på de sager, som opslagene vedrørte). Stikprøverne med medarbejderens noteringer lægges til den chef, som har størst indsigt i vedkommendes arbejde. Er der behov for yderligere opklaring, taler chefen med medarbejderen / den tilsynsførende medarbejder.
Giver det ikke anledning til yderligere spørgsmål, betragtes kontrollen som gennemført med tilfredsstillende resultat.
Kontrollen journaliseres fx i eDoc.

Medarbejderne i Borgerservice bør løbende informeres på intranettet om at opslag i kommunens systemer logges, at opslagene til enhver tid kan blive kontrolleret, og at de opslag, som borgerservicecenter-medarbejderne foretager, kontrolleres jævnligt ved stikprøver.

Automatiseret overvågning kan erstatte stikprøver.
Datatilsynet anbefaler at foretage automatiseret overvågning når det er muligt. Løsning kan træde i stedet for stikprøvekontroller.

Automatiseret overvågning er en teknisk løsning, som automatisk finder og giver sikkerhedsmedarbejderne meddelelse om uhensigtsmæssige eller usædvanlige søgemønstre.
Det forudsætter, at der opstilles nogle særlige kriterier for, hvornår søgemønstre er uhensigtsmæssige eller usædvanlige. Ledelsens og systemejerne i Borgerservice opstiller disse kriterier ud fra deres viden om systemerne og Borgerservice medarbejdernes opgaver og arbejdsgange.

Det kan f.eks. være opslag på oplysninger om kendte personer, opslag uden for normal åbningstid, opslag på følsomme sager, der er afsluttet, opslag i samme system på oplysninger om mange forskellige personer inden for et kort tidsrum eller lign. Det skal naturligvis overvejes, hvilke søgemønstre der – med henblik på saglige formål – må formodes at være almindeligt forekommende blandt medarbejdere i borgerservicecentre.

Hvis en søgning findes af den automatiserede overvågning, betyder det ikke i sig selv, at der er tale om et misbrug. Det betyder, at der kan være grund til at spørge den pågældende medarbejder om grunden til opslaget.

Kontrol af opslag, som finder sted på baggrund af den automatiserede overvågning, skal ske på samme måde som ved kontrol på baggrund

af stikprøver af loggen med hensyn til forelæggelse for medarbejdere m.v. Medarbejderne bør også informeres om automatisk overvågning.

KS anskaffer i 2015 et system til central overvågning af log fra kritiske systemer og fra 2016 påbegyndes overførsel af ansvaret for overvågnings- og opfølgningsopgaven for sådanne systemer fra forvaltningerne til KS. Det sker på baggrund af aftaler om hvert enkelt system, således at ansvaret overgår når systemet er opsat så central logning og overvågning er mulig. Indtil den tekniske løsning er på plads og overvågningsopgaven overført til KS, er det stadig forvaltningerne der har ansvar for kontrol og opfølgning.

NOTAT

23-10-2015

Sagsnr.
2015-0076634

Dokumentnr.
2015-0076634-4

Sagsbehandler
Kirsten Wenning

Til KFF
Københavns Borgerservice

Best practice for gennemførelse af stikprøvekontrol af loggen

Best practice er udarbejdet på baggrund af kommunens it-sikkerhedsregler, Datatilsynets anbefalinger og erfaringer fra andre kommuner.

Indledning
Formålet med en stikprovekontrol er dels at afsløre eventuelt misbrug, dels at forebygge misbrug.
Stikprøver af loggen skal foretages af de opslag, som borgerservicecentermedarbejderne foretager i de logningspligtige it-systemer. Dvs. systemer der indeholder fortrolige eller følsomme personoplysninger.
Opstart af stikprøvetagning af loggen bør ske i 2 faser.
Fase 1, en pre-test, der skal skabe forståelse for stikprøverne og de opgaver de medfører hos de involverede parter. Samtidig skal eventuelle udfordringer identificeres og løses.
Fase 2, den generelle procedure som bør følges.

Fase 1
Opstart og pre-test

- Informer medarbejdere
  Medarbejderne i Borgerservice informeres på intranettet eller pr. mail om at opslag i kommunens systemer logges, at opslagene til enhver tid kan blive kontrolleret, og at de opslag, som borgerservicecenter-medarbejderne foretager, kontrolleres jævnligt ved stikprøver.

- Systemejere adviseres
  Systemejere, der forventes at skulle bidrage med logudtræk, informeres om at KBS fremadrettet vil foretage stikprøver af loggen. Systemejerne skal vide hvilken log bestilling de vil modtage, hvor ofte, hvad der er for et log udtræk de skal levere og hvor hurtigt. De skal vide at det forventes at de bidrager med hjælp til at tolke loggen hvis der er behov.
  Specifikation af log udtræk. Log udtrækket er det, der typisk kaldes en sikkerhedslog, som skal indeholde: oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrorte, eller det anvendte søgekriterium.

- Start med en pre-test.
  KBS anbefales at starte med at udføre en pre-test, som kan hjælpe dem med at identificere eventuelle udfordringer ved at gennemfører stikprøvekontrollerne. Pre-testen kan bestå i en begrænset test af fx 3 medarbejderes brug af 2 udvalgte systemer (fx: KMD-sag og CPR). Afgiv bestilling til systemejere.

  Eksempel på bestilling:
  Bestilling af sikkerhedslog fra system xxxxx til brug for stikprøve af loggen i Borgerservice
  Periode dd/mm/aa, kl. xx – xx.
  Medarbejders navn xxxx
  Brugerid xxx
  Sikkerhedslog bedes leveret senest dd/mm/aa

  Ved modtagelse af sikkerhedsloggen undersøges det om log udtrækket er forståeligt. Er der behov for hjælp til at forstå loggen kontaktes systemejer.
  Herefter udvælges 5 – 6 opslag pr. medarbejder til kontrol. Medarbejderen noterer hvad årsagen til opslagene var (evt. journalnumre på vedrørende sager). Stikprøver med noteringer lægges til medarbejderens chef til godkendelse og journalisering. Har chefen behov for yderligere opklaring, tales der med medarbejder og evt. anden relevant fagperson.

Fase 2
Generel procedure

- Efter succesfuld gennemført pre-test, anbefales følgende procedure.

  KBS udpeger 2 tilsynsførende medarbejdere (uvildige), som fremover har ansvar for at gennemføre stikprøvekontrollerne.

  Systemer
  Stikproverne foretages af de opslag, som borgerservicecentermedarbejderne foretager i de logningspligtige it-systemer.
  Københavns Borgerservice udpeger på baggrund af de systemer, processer og rettighedstildelinger der anvendes hvilke logningspligtige systemer der er relevante at kontrollere.
  Borgerservice har selv tidligere peget på, at der foretages opslag i følgende systemer, som vi derfor anbefaler indgår i stikprøvekontrollen: KMD Sag, CPR og Kommunal Sygesikring.

Interval for stikprøvetagning
Stikprøverne skal falde med forskellige intervaller, f.eks. 2½ måned, 5 måneder, osv., dog højst 6 måneder. Planlagte datoer for stikprøver skal fremgå af et bilag, som kun de tilsynsførende medarbejdere og deres chef har adgang til.

Antal medarbejdere pr. kontrol
Der udvælges ca. 10 tilfældige medarbejdere pr. kontrol. Medarbejderne skal naturligvis ikke være bekendt med udvælgelsen.

Antal opslag pr. medarbejder
En stikprøve omfatter 5 – 6 opslag

- Stikprøvekontrollen gennemføres
  En stikprøvekontrol bør kunne gennemføres inden for 5-8 arbejdsdage.
  Dag 1 - Log udskrifter bestilles af de tilsynsførende hos de respektive systemejere.
  Dag 3/4 - Stikprøverne forelægges de berørte medarbejdere, som noterer hvad årsagen til opslagene var (evt. journalnumre på de sager, som opslagene vedrørte).
  Dag 5/7 - Stikprøverne med medarbejderens noteringer lægges til den chef, som har størst indsigt i vedkommendes arbejde. Er der behov for yderligere opklaring, taler chefen med medarbejderen / den tilsynsførende medarbejder. Giver det ikke anledning til yderligere spørgsmål, betragtes kontrollen som gennemført med tilfredsstillende resultat. Kontrollen journaliseres fx i eDoc.

Medarbejderne i Borgerservice bør løbende informeres på intranettet eller evt. pr. mail om at opslag i kommunens systemer logges, at opslagene til enhver tid kan blive kontrolleret, og at de opslag, som borgerservicecenter-medarbejderne foretager, kontrolleres jævnligt ved stikprøver.

BILAG 12 – ØKONOMIFORVALTNINGENS HØRINGSBEMÆRKNINGER

KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

30-03-2017

Sagsnr.
2017-0125348

Dokumentnr.
2017-0125348-1

Sagsbehandler
Tom John Fischer Jensen

Til Borgerrådgiveren

Svar på Borgerrådgiverens foreløbige rapport vedr. logning

Vedr. Borgerrådgiverens sag nr. 2014-0118160.

Borgerrådgiveren har foretaget en undersøgelse af logning i Københavns Borgerservices elektroniske sagsbehandlingssystem, *KMD Sag* og har fremsendt udkast til rapport. Borgerrådgiveren anfører, at der eksisterer en række mangler ift. den elektroniske sagsbehandling, der angives til at være følgende:

1. At der i perioden hvor *KMD Sag* har haft en systemejer, enten i Socialforvaltningen eller i Koncernservice, ikke er sket kontrol med afviste adgangsforsøg, hvilket strider mod Bek. nr. 528 af 15. juni 2000 (sikkerhedsbekendtgørelsen) § 18.

2. At der i perioden hvor *KMD Sag* har haft en systemejer, enten i Socialforvaltningen eller i Koncernservice, ikke er fulgt op på den maskinelle log vedr. adgang til følsomme personoplysninger, hvilket strider mod Datatilsynets udtalelse af 26. juni 2006.

3. At It-sikkerhedsfunktionen i Koncernservice først har fulgt op med en vejledning om stikprøvekontrol til Borgerservice Centre i 2015, og at vejledningen ikke var formuleret som bindende retningslinje.

4. At It-sikkerhedsfunktionen i Koncernservice ikke har foretaget stikprøvekontrol af loggen for Københavns Borgerservices behandling af følsomme personoplysninger i *KMD Sag*.

5. At *KMD Sag* ikke logger i funktionen *personoverblikket* og at der således kan tilgås følsomme personoplysninger ved søgninger på personer i *KMD Sag* uden logning.

Københavns Kommunes It-sikkerhedsfunktion har gennemgået *KMD Sag* med dets nuværende systemejer i Koncern IT og har følgende bemærkninger til rapportens faktuelle oplysninger:

Ad 1) Det kan oplyses, at *KMD Sags* understøttende it-sikkerhedsløsning *KMD CICS* registrerer afviste adgangsforsøg, og at systemet låser den pågældende bruger ude efter tre afviste loginforsøg. Der sker dermed en automatisk registrering af afviste adgangsforsøg, og systemet udviser samtidigt en passende reaktion ved blokeringen for yderligere forsøg på adgang. It-sikkerhedsfunktionen vurderer, at denne løsning lever op til kravene i sikkerhedsbekendtgørelsens § 18.

IT-sikkerhed, Systemejere og Videnscentre

Borups Allé 177
2400 København NV

Mobil [redacted]

EAN nummer
5798009809308

Ad 2) Opfølgning på logoplysninger om adgang til følsomme persondata er systemejers ansvar. Den nuværende systemejer på *KMD Sag* har haft ansvar for opgaven siden 2015, hvor systemejeropgaven overgik fra Socialforvaltningen til Koncernservice/Koncern IT. Systemejer har oplyst, at det er korrekt, at der ikke er blevet fulgt op på loggen i *KMD Sag*. *KMD Sag* er et paraplysystem for en række underliggende systemer. Systemets kompleksitet gør det praktisk umuligt manuelt at gennemgå de meget store datamængder. Det er bl.a. årsagen til, at Borgerrepræsentationen i 2015 på baggrund af indstilling fra Økonomiforvaltningen besluttede, at der skulle anskaffes en fælles maskinel logopfølgningsløsning, og at ansvaret for opfølgning på logs skulle overgå til It-sikkerhedsfunktionen i KIT efter konkret aftale, når det enkelte system var klargjort til overførsel af logs.

Det er en teknisk meget kompleks opgave at overføre logs korrekt, og i forhold til *KMD Sag* har arbejdet med at forberede adgang til overførsel af logs fra *KMD Sag* og de tilhørende logs i *KMD CICS* været i gang siden medio 2016. Opgaven er nu næsten afsluttet, og det forventes, at en automatiseret logopfølgning for *KMD Sag* kan etableres i 2. kvartal 2017.

Ad 3) I marts 2010 oprettede man It-sikkerhedsfunktionen i det daværende KS. I den forbindelse blev det forudsat, at Datatilsynets udtalelse af 26. juni 2006 var fulgt af Københavns Kommunes Borgerservice Centre, idet ansvaret for efterlevelse af reglerne i hele perioden har ligget i de pågældende forvaltninger.

Den udstedte vejledning fra It-sikkerhedsfunktionen blev udarbejdet for bl.a. at sikre forenelighed mellem interne regler og Datatilsynets udtalelse af 26. juni 2006. Vejledningen blev udstedt 18. september 2015 og blev derfor udformet som en anbefaling, der supplerede Datatilsynets regler og praksis.

Ad 4) Det er korrekt, at *KMD Sag* ikke hidtil har været udtaget til stikprøve af It-sikkerhedsfunktionen. It-sikkerhedsfunktionen planlægger ikke at gennemføre en stikprøve på nuværende tidspunkt, idet *KMD Sag* jf. ovenfor vil overgå til automatiseret overvågning af logs indenfor få måneder.

Ad 5) Det er korrekt, at der ikke logges direkte i funktionen personoverblikket i *KMD Sag*. It-sikkerhedsfunktionen vurderer, at dette ikke er nødvendigt, idet systemejer oplyser, at relevante oplysninger om de handlinger, en bruger foretager i personoverblikket, bliver logget i KMDs sikkerhedsløsning *KMD CICS*. Dermed vurderer It-sikkerhedsfunktionen, at loggen opfylder

sikkerhedsbekendtgørelsens § 19, stk. 1, hvorefter al behandling af følsomme personoplysninger bliver logget.

Sammenfatning
Koncern IT vurderer, at *KMD Sag* i sammenhæng med den integrerede sikkerhedsløsning *KMD CICS* lever op til sikkerhedsbekendtgørelsens § 18 om håndtering af afviste adgangsforsøg og § 19 om logning.

Koncern IT udsendte d. 18. september 2015 en vejledning om stikprøvekontroller som supplement til Datatilsynet udtalelse fra 2006 for at sikre forenelighed mellem eksterne og interne regler. Vejledningen blev på den baggrund udformet som en anbefaling. Koncern IT tager til efterretning, at Borgerrådgiveren kritiserer, at vejledningen ikke er udsendt tidligere, og at Borgerrådgiveren vurderer, at vejledningen skulle have været udformet som en bindende retningslinje.

Koncern IT overtog systemejerskabet i 2015. I perioden siden 2015 har der ikke været fulgt op på logfiler. Årsagen er, at logfilerne er så omfattende og komplekse, at det ikke har været muligt at følge op manuelt. I stedet har Koncern IT arbejdet på at klargøre *KMD Sag* til automatiseret opfølgning på logfiler.

Der vil være etableret automatiseret opfølgning på logfiler fra *KMD Sag* og *KMD CICS* med udgangen af 2. kvartal 2017. På den baggrund har Koncern IT ikke udtaget systemet til stikprøvekontrol.

BILAG 13 – OPFØLGENDE SPØRGSMÅL TIL KONCERN IT

[redacted]

Fra: Borgerrådgiveren
Sendt: 5. april 2017 14:51
Til: Taghi Cheraghi
Emne: Fra hvornår har KSP CICS registreret afviste adgangsforsøg i Københavns Kommune til KMD Sag, herunder logget i KMD Sags personoverblik?

Kære Taghi

Som aftalt telefonisk dag dato en mail med mine spørgsmål.

Borgerrådgiveren ønsker svar på, fra hvornår KSP CICS (som jeg går ud fra er identisk med KMD CICS) har registreret afviste adgangsforsøg i Københavns Kommune til it-systemet KMD Sag, herunder fra hvornår KSP CICS har logget i KMD Sags personoverblik i forhold til Københavns Kommunes søgninger mv. Dette til brug for Borgerrådgiverens generelle egen drifts-undersøgelse om logning i Københavns Borgerservices it-system KMD Sag.

Jeg går ud fra, at du som nævnt retter henvendelse til KMD, hvis det er nødvendigt for at svare på spørgsmålet.

På forhånd mange tak.

Har du spørgsmål mv. er du velkommen til at ringe eller skrive.

Med venlig hilsen
for Borgerrådgiveren

Daniel Soelberg Bach
Jurist

BORGER RÅDGIVEREN

KØBENHAVNS KOMMUNE

Vester Voldgade 2A
1552 København V

Telefon 33 66 14 00
Telefax 33 66 13 90
E-mail borgerraadgiveren@kk.dk
www.kk.dk/borgerraadgiveren

Følg os på Facebook
www.facebook.com/borgerraadgiveren

1

[redacted]

Fra: Borgerrådgiveren
Sendt: 5. april 2017 15:44
Til: Taghi Cheraghi
Emne: Supplerende spørgsmål - Fra hvornår har KSP CICS registreret afviste adgangsforsøg i Københavns Kommune til KMD Sag, herunder logget i KMD Sags personoverblik?

Kære Taghi

Borgerrådgiveren stiller dig supplerende spørgsmål vedrørende registrering og loggen i KSP CICS, som jeg sender til dig allerede nu med henblik på ikke at skulle følge unødigt op over for dig på et senere tidspunkt.

I det omfang et andet it-system har registreret afviste adgangsforsøg i Københavns Kommune til KMD Sag og/eller logget i KMD Sags personoverblik, før dette er sket med KSP CICS, ønsker Borgerrådgiveren at få oplyst it-systemets navn, og hvilken periode it-systemet har registreret afviste adgangsforsøg i KMD Sag og/eller logget i KMD Sags personoverblik?

Endelig ønsker Borgerrådgiveren svar på, hvilke oplysninger KSP CICS loggen indeholder i forhold til Københavns Kommunes søgninger mv. i KMD Sags personoverblik?

Med venlig hilsen
for Borgerrådgiveren

Daniel Soelberg Bach
Jurist

BORGER RÅDGIVEREN

KØBENHAVNS KOMMUNE

Vester Voldgade 2A
1552 København V

Telefon 33 66 14 00
Telefax 33 66 13 90
E-mail borgerraadgiveren@kk.dk
www.kk.dk/borgerraadgiveren

Følg os på Facebook
www.facebook.com/borgerraadgiveren

Fra: Borgerrådgiveren
Sendt: 5. april 2017 14:51
Til: Taghi Cheraghi
Emne: Fra hvornår har KSP CICS registreret afviste adgangsforsøg i Københavns Kommune til KMD Sag, herunder logget i KMD Sags personoverblik?

Kære Taghi

Som aftalt telefonisk dag dato en mail med mine spørgsmål.

Borgerrådgiveren ønsker svar på, fra hvornår KSP CICS (som jeg går ud fra er identisk med KMD CICS) har registreret afviste adgangsforsøg i Københavns Kommune til it-systemet KMD Sag, herunder fra hvornår KSP CICS har logget i KMD Sags personoverblik i forhold til Københavns Kommunes søgninger mv. Dette til brug for Borgerrådgiverens generelle egen drifts-undersøgelse om logning i Københavns Borgerservices it-system KMD Sag.

Jeg går ud fra, at du som nævnt retter henvendelse til KMD, hvis det er nødvendigt for at svare på spørgsmålet.

På forhånd mange tak.

Har du spørgsmål mv. er du velkommen til at ringe eller skrive.

Med venlig hilsen
for Borgerrådgiveren

Daniel Soelberg Bach
Jurist

BORGER
RÅDGIVEREN

KØBENHAVNS KOMMUNE

Vester Voldgade 2A
1552 København V

Telefon 33 66 14 00
Telefax 33 66 13 90
E-mail borgerraadgiveren@kk.dk
www.kk.dk/borgerraadgiveren

Følg os på Facebook
www.facebook.com/borgerraadgiveren

BILAG 14 – ØKONOMIFORVALTNINGENS SVAR PÅ BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL

NOTAT

28-04-2017

Sagsnr.
2017-0125348

Dokumentnr.
2017-0125348-3

Sagsbehandler
Brian Thordarson

Til Borgerrådgiveren

Supplerende besvarelse til Borgerrådgiverens generelle egen drifts-undersøgelse om logning i Københavns Borgerservices it-system KMD Sag.

Borgerrådgiveren har i to e-mails af 5. april 2017 til systemejer Taghi Cheraghi fremsendt en række opfølgende spørgsmål vedr. logning af transaktioner i KMD Sag i sikkerhedsløsningen KSP CICS.

Det sker på baggrund af KITs oprindelige besvarelse af Borgerrådgiverens egen drifts-undersøgelse jf. eDoc sag 2017-0125348.

Borgerrådgiveren stiller fem spørgsmål i henvendelserne.

1. Er KSP CICS samme system som KMD CICS?
2. Fra hvilket tidspunkt har KSP CICS registreret afviste adgangsforsøg i Københavns Kommune til it-systemet KMD Sag?
3. Fra hvilket tidspunkt har KSP CICS logget KMD Sags personoverblik i forhold til Københavns Kommunes søgninger mv?
4. I det omfang et andet it-system har registreret afviste adgangsforsøg i Københavns Kommune til KMD Sag og/eller logget i KMD Sags personoverblik, før dette er sket med KSP CICS, ønsker Borgerrådgiveren at få oplyst it-systemets navn, og hvilken periode it-systemet har registreret afviste adgangsforsøg i KMD Sag og/eller logget i KMD Sags personoverblik.
5. Hvilke oplysninger indeholder KSP CICS loggen i forhold til Københavns Kommunes søgninger mv. i KMD Sags personoverblik?

Svar
Det skal indledende oplyses, at der kun kan søges på personnummer i KMD Sag Personoverblik. Desuden er det kun muligt at anvende KMD Sag Personoverblik, såfremt KMD Sag er installeret på medarbejderens pc og medarbejderen er blevet autoriseret til at bruge KMD Sag Personoverblik. Autorisation af medarbejdere sker i KSP-CICS via Brugeradministrationen.

Når en bruger vil anvende KMD Sag, skal brugeren først logge på ved angivelse af brugernavn og adgangskode. Alle afviste adgangsforsøg bliver logget i KSP-CICS.

Ad spørgsmål 1
Nej. KMD CICS-miljøet er hele KMD´s mainframe-miljø, hvor KSP-CICS er KMD´s autorisations- og sikkerhedsløsning.

Ad spørgsmål 2
KSP CICS er anvendt til at registrere afviste adgangsforsøg i Københavns Kommune til it-systemet KMD Sag siden ibrugtagelse. Iflg. KK systemoverblik "Fiskk" er KMD sag ibrugtaget 1. januar 2009. Det er oplyst, at KMD sag er en videreførelse af KMD S&A (KMD Sags- og Advis system).

Ad spørgsmål 3
KSP CICS er anvendt til at logge KMD Sags Personoverblik i forhold til Københavns Kommunes søgninger mv. siden ibrugtagen af KMD Sag pr. 1. januar 2009.

Ad spørgsmål 4
Der har ikke været anvendt andre systemer end KSP CICS til logning af brugernes anvendelse af KMD Sag Personoverblik.

Ad spørgsmål 5
KSP CICS har siden idriftsættelse logget følgende oplysninger om brug af KMD Sag Personoverblik:

- Brugerident, medarbejdernavn og forvaltning
- Dato
- Klokkeslæt
- At brugeren har anvendt KMD Sag Personoverblik
- Personnummeret på den borger, der er slået op.

Logon-kontrollen oplyser om fem forskellige forløb, som et Logon kan have:

- Logon ok
- Logon afvist – kendeord er forkert
- Logon afvist – kendeord er udløbet
- Logon afvist – nyt kendeord er forkert
- Logon afvist – bruger uautoriseret til adresse.

Logon-kontrollen kan både bestilles for et tidsinterval tilbage i tiden og frem i tiden, og det kan bestilles for udvalgte brugere.

Loggen gemmes i seks måneder.

Der henvises i øvrigt til tidligere fremsendt materiale om logning i KSP CICS, hvori ovenstående er uddybet.

KIT deltager gerne i afklaringsmøde, såfremt Borgerrådgiveren har yderligere spørgsmål i sagen.

BILAG 15 – KULTUR- OG FRITIDSFORVALTNINGENS HØRINGSBEMÆRKNINGER

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Center for Digitalisering og Innovation

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

28-04-2017

Sagsnr.
2017-0194178

Dokumentnr.
2017-0194178-3

Høringsbemærkninger til Borgerrådgiveren vedr. Borgerrådgiverens foreløbige rapport af 28. februar 2017 om logning af elektronisk sagsbehandling og borgernes adgang til indsigt i oplysninger

Borgerrådgiveren har ved skrivelse af 28. februar 2017 anmodet KFF (og KIT) om at fremkomme med eventuelle bemærkninger til de faktiske oplysninger i den foreløbige rapport om logning af Københavns Borgerservices elektroniske sagsbehandling i KMD Sag.

Borgerrådgiverens undersøgelse af KMD Sag er sket som opfølgning på Borgerrådgiverens ved skrivelse af 8. august 2014 iværksatte undersøgelse vedr. logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemer, hvor der behandles følsomme personoplysninger, og borgeres adgang til indsigt i oplysninger efter persondataloven ved Københavns Borgerservice.

Nærværende skrivelse udgør KFFs bemærkninger til Borgerrådgiveren.

I sin foreløbige rapport af 28. februar 2017 har Borgerrådgiveren anført, at Borgerrådgiveren: "... finder det bemærkelsesværdigt, at Københavns Borgerservice alene skulle behandle følsomme personoplysninger i KMD Sag, men foretager for nu ikke yderligere end at påpege dette, og jeg har i undersøgelsen lagt forvaltningens oplysning til grund.".

På baggrund af det af Borgerrådgiveren anførte har KFF valgt på ny at gennemgå den af KFF i den oprindelige sag (sagsnr. 2014-0171930) udarbejdede liste over systemer i Københavns Borgerservice. Endvidere har KFF valgt at gennemgå det ved skrivelse af 5. oktober 2015 fra KFF til Borgerrådgiveren om samme liste over systemer i Københavns Borgerservice oplyste (ligeledes sagsnr. 2014-0171930).

Ved gennemgangen har KFF konstateret, at der beklageligvis er fejl i det af KFF om systemerne oplyste.

KFF burde rettelig have oplyst, at der udover KMD Sag er flere systemer, hvor der behandles følsomme personoplysninger. KFF har derfor udarbejdet ny systemoversigt, som er indsat nederst i dette brev som tabel 1. I tabellen er angivet kategorien af de i systemerne behandlede persondata. For god ordens skyld er systemoversigten opda-

Systemhåndtering
Nyropsgade 1
1602 København V
Mobil [redacted]
E-mail [redacted]
EAN nummer
5798009781697

teret således, at den indeholder alle persondataindeholdende systemer, der pr. dags dato anvendes i Københavns Borgerservice.

Ved udarbejdelsen af tabel 1 har KFF anvendt Københavns Kommunes Intern Revisions opdeling af persondatakategorier, hvorfor kategorisering er foretaget ud fra følgende opdelinger: Almindelige, fortrolige og følsomme personoplysninger.

Med venlig hilsen

Thomas Jakobsen
Direktør

Tabel 1

FISKK id	Systemnavn	Almindelige personoplysninger	Fortrolige personoplysninger	Følsomme personoplysninger
343	Kmd Sag	x	X	x
512	Notus Kommunal, sygesikring	x	X	x
423	CPR	x	X	x
244	Pasregisteret	x	x	
244	Kørekortregisteret	x	x	x
	Fritagelse for digital post	x	x	x
469	Straksudstedelse af NemID (NemID Privat)	x	x	
	KMD Mainframe	x	x	x
712	ID-Port (pas og kørekort)	x	x	
383	Køreprøvebooking	x	x	
247	P-Data (KMD udtræk fra CPR)	x	x	x
729	CSC Social	x	x	x
1017	Skat Extranet (kommunal indgang til skat)	x	x	
518	SafePay, kasseløsning		x	

Side 2 af 2

BILAG 16 – ØKONOMIFORVALTNINGENS HØRINGSBEMÆRKNINGER II

KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

06-07-2017

Sagsnr.
2017-0125348

Dokumentnr.
2017-0125348-6

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

Svar fra Koncern IT på Borgerrådgiverens foreløbige rapport II om logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger

Borgerrådgiveren har i brev af 23. juni 2017 anmodet Økonomiforvaltningen om at fremsende eventuelle bemærkninger til Borgerrådgiverens foreløbige rapport II om logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger hos Koncernservice.

Borgerrådgiveren har følgende bemærkninger, der vedrører Økonomiforvaltningen/Koncern IT i rapporten:

1. Borgerrådgiveren finder det meget beklageligt, at it-sikkerhedsfunktionen først fulgte op over for Københavns Borgerservice med vejledningen "Krav om stikprøver af loggen i borgerservicecentre" og best practice "for gennemførelse af stikprøvekontrol af loggen" mere end 9 år efter Datatilsynets udtalelse af 26. juni 26. juni 2006.
2. Ydermere finder Borgerrådgiveren det "beklageligt, at it-sikkerhedsfunktionens vejledning er udformet som en anbefaling, og ikke som et pålæg om at foretage stikprøvekontrol i samarbejde med systemejeren."
3. Borgerrådgiveren finder, "at det manglende tilsyn med hensyn til foretagelse af stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme oplysninger i it-systemerne er kritisabel(t)".

Ad 1.
I marts 2010 oprettede man It-sikkerhedsfunktionen i det daværende KS, og det er først fra det tidspunkt at it-sikkerhedsfunktionen har haft mandat til at gå ind i sagen. I forbindelse med oprettelsen blev det forudsat, at Datatilsynets udtalelse af 26. juni 2006 var fulgt af Københavns Kommunes Borgerservice, idet ansvaret for efterlevelse af reglerne i hele perioden har ligget i de ansvarlige forvaltninger.

IT Sikkerhedsfunktionen havde inden udstedelsen af vejledningen i 2015 en længere og konstruktiv dialog med Kultur- og Fritidsforvaltningen om, hvordan forvaltningen bedst muligt lever op til kravene, og denne dialog mundede ud i, at den omtalte vejledning blev udarbejdet.

Ad 2.

IT-sikkerhed, Systemejere og Videnscentre

Borups Allé 177
2400 København NV

Mobil [redacted]

EAN nummer
5798009809308

www.kk.dk

Koncern IT tager til efterretning, at Borgerrådgiveren finder, at vejledningen skulle have været udsendt tidligere, og at Borgerrådgiveren finder, at vejledningen skulle have været udformet som en bindende retningslinje.

Ad 3.
It-sikkerhedsfunktionen har udført tilsyn med de stikprøver, som Københavns Borgerservice gennemførte i 2015 og efterfølgende dokumenterede i kontrolrapporter, som er fremsendt til it-sikkerhedsfunktionen.

Det skete i forlængelse af at it-sikkerhedsfunktionen i 2015 rådgav Københavns Borgerservice med hensyn til, hvordan KBS kunne sikre den ønskede kontrol af logs. I samme forbindelse udarbejdede it-sikkerhedsfunktionen mere operationelle planer for gennemførelse af logkontroller samt best practices.

Tilsynet viste, at stikprøverne var hensigtsmæssigt gennemført.

Koncern It har tidligere orienteret Borgerrådgiveren om, at KMD Sag tilknyttes kommunens SIEM løsning, således at logopfølgningen automatiseres fremadrettet. Den tekniske løsning er nu i stabil drift, og regelmæssig opfølgning med rapporter til systemejer vil blive iværksat i eftersommeren 2017.

BILAG 17 – SOCIALFORVALTNINGENS HØRINGSBEMÆRKNINGER II

KØBENHAVNS KOMMUNE
Socialforvaltningen
Adm. direktør

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

11. august 2017

Sagsnr.
2017-0111188

Dokumentnr.
2017-0111188-17

Vedrørende Borgerrådgiverens foreløbige rapport II om logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger, jf. Borgerrådgiverens sagsnr. 2014-0118160

Borgerrådgiveren har den 23. juni 2017 fremsendt foreløbig rapport II om logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger til høring hos Kultur- og Fritidsforvaltningen, Økonomiforvaltningen og Socialforvaltningen.

Rapporten drejer sig om logning af elektronisk sagsbehandling i 14 forskellige it-systemer, såsom KMD Sag og CSC Social, og om borgeres indsigt i oplysninger efter persondataloven. Borgerrådgiveren anmoder alene om eventuelle bemærkninger til faktuelle oplysninger i rapporten.

Socialforvaltningen kan oplyse, at forvaltningen har følgende bemærkninger til de faktuelle oplysninger i rapporten vedrørende it-system CSC Social:

Københavns Borgerservice har 50 autoriserede brugere i CSC Social, som siden den 17. januar 2017 har haft læse-adgang til borgere på myndighedsniveau. Brugerne kan bl.a. se borgerens stamdata, hvilke indsatser borgeren er tilknyttet, og de handleplaner, notater og breve der er knyttet til de specifikke indsatser.

SOF IT og Københavns Borgerservice (Center for Innovation og Digitalisering) har i august 2017 været i dialog omkring en arbejdsgang for opfølgning på afviste adgangsforsøg. CSC Social kræver loginoplysninger ved adgang til systemet og at, disse loginoplysninger kun tildeles af Koncernservice Brugeradministration til medarbejdere, som Københavns Borgerservice autorisationsansvarlige har bestilt adgang til – efter forudgående godkendelse fra pågældende medarbejders nærmeste leder.

Således kan brugere uden autorisation aldrig få adgang til CSC Social. Kun med korrekt personlig loginkode og medarbejdernes brugerID kan der opnås adgang til systemet.

Derfor er det SOF IT og Københavns Borgerservices opfattelse, at loggen over afviste loginforsøg ikke direkte giver indikation af "forsøg på uretmæssig adgang til kritiske data" jf. stk.10.10 i kommunens uddybende it-sikkerhedsregler, idet afviste adgangsforsøg jo blot viser, at;

Direktionen

Rådhuset
1599 København V.

Telefon
33 66 33 66

Direkte telefon
[redacted]

E-mail
[redacted]

www.kk.dk

- systemet ikke genkender et givent brugernavn (uden et genkendeligt brugernavn er det ikke muligt at fastslå, om det var en medarbejder i Københavns Borgerservice, som uretmæssigt forsøgte at tilgå systemet, eller en allerede autoriseret medarbejder, som blot tastede sit brugernavn forkert)

- systemet ikke genkender en given loginkode (idet en autoriseret medarbejders loginkode kun er kendt af medarbejderen selv, er det ikke muligt at fastslå, om det var en anden medarbejder i Københavns Borgerservice, som uretmæssigt forsøgte at tilgå systemet, eller den allerede autoriserede medarbejder, som blot tastede sin loginkode forkert).

På baggrund af ovenstående har SOF IT og Københavns Borgerservice sammen besluttet ikke at gå videre med at etablere en arbejdsgang for overbringelse af logs til brug for Københavns Borgerservice opfølgning på afviste adgangsforsøg. SOF IT arbejder til gengæld med et SIEM-projekt sammen med Koncern IT. I regi af projektet bliver der lavet log på forskellige typer af afviste adgangsforsøg, f.eks. på overhyppigheder i afviste adgangsforsøg fra enkelte IP-adresser eller forsøg på login fra tidligere medarbejdere.

Det blev aftalt, at Københavns Borgerservice til enhver tid skal kontakte SOF IT, hvis der opleves anormaliteter ved login og SOF IT kan til en hver tid fremskaffe en log over mislykkede login-forsøg.

Med venlig hilsen

Nina Eg Hansen

BILAG 18 – KULTUR- OG FRITIDSFORVALTNINGS HØRINGSBEMÆRKNINGER II

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Direktionen

Borgerrådgiveren

09-08-2017

Sagsnr.
2017-0194178

Dokumentnr.
2017-0194178-9

Vedr. Borgerrådgiverens foreløbige rapport af 23. juni 2017 om logning af elektronisk sagsbehandling og borgernes adgang til indsigt i oplysninger

Borgerrådgiveren har den 23. juni 2017 anmodet Kultur- og Fritidsforvaltningen om at fremkomme med eventuelle bemærkninger til de faktiske oplysninger i den foreløbige rapport II om logning af elektronisk sagsbehandling og borgernes adgang til indsigt i oplysninger.

På baggrund af det af Borgerrådgiveren anførte vedrørende loggen af Københavns Borgerservices behandling af personoplysninger i it-systemerne, rapportens s. 6, ønsker Kultur- og Fritidsforvaltningen supplerende at bemærke, at forvaltningen fra december 2015 har foretaget stikprøvekontroller.

Proceduren og rammerne for stikprøvekontroller er aftalt med og godkendt af Koncernservice, IT–sikkerhed, som vi er i løbende dialog med.

Med venlig hilsen

Thomas Jakobsen
Direktør

Rådhuset
1. sal, vær. 83
1599 København V

Telefon
[redacted]

www.kk.dk

BILAG 19 – BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN (UDKLIP AF REFERATARK, DOK.NR. 2014-0118160-11)

”**11. sept. 2017: Opkald fra Malte Harrishøj i KFF**
Jeg gentager spørgsmålet, om forvaltningen kan bekræfte, at de hidtil foretagne stikprøvekontroller af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i henhold til Datatilsynets udtalelse og Koncern IT's vejledning og best practice alene er sket i it-systemerne KMD Sag, Notus Kommunal, sygesikring og CPR. Jeg præciserer, at vores spørgsmål er afgrænset til *foretagne* stikprøvekontroller.

/DAB

8. sept. 2017: Opkald til Anette L. Hansen (ALH) i KFF
Med henvisning til Borgerrådgiverens foreløbige rapport II og forvaltningens seneste bemærkninger hertil, spørger jeg, om forvaltningen kan bekræfte, at de hidtil foretagne stikprøvekontroller af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i henhold til Datatilsynets udtalelse og Koncern IT's vejledning og best practice alene er sket i it-systemerne KMD Sag, Notus Kommunal, sygesikring og CPR.

ALH beder it-ansvarlig Malte H om at give mig svar.

/DAB”

BILAG 20 – KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ OPFØLGENDE SPØRGSMÅL (NOTAT AF 15. SEPTEMBER 2017)

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Center for Digitalisering og Innovation

NOTAT

15. september 2017

Sagsnr.
2017-0194178

Dokumentnr.
2017-0194178-13

Sagsbehandler
Anders C. S. Larsen

Svar til Borgerrådgiveren i forlængelse af KFF's kommentarer af 9. august 2017 til Borgerrådgiverens foreløbige rapport II af 23. juni 2017

Stikprøvekontrol i KFF

Som nævnt i forvaltningens bemærkning til den foreløbige rapport har forvaltningen allerede fra december 2015 foretaget stikprøvekontroller, hvis procedurer og rammer er aftalt med og godkendt af Koncernservice, IT–sikkerhed.

Koncernservice, IT–sikkerhed, har modtaget ansøgning og givet accept til at KFF foretager stikprøvekontroller i følgende systemer i 2017:

- CPR Web
- Notus kommunal
- Kørekortregisteret
- KMD Social Pension
- Bibprint

Status for stikprøvekontroller i 2017

CPR Web:
1 stikprøve er afsluttet i marts 2017
1 stikprøve er iværksat og forventes afsluttet primo uge 40

Notus kommunal:
1 stikprøvekontrol er iværksat og forventes afsluttet ultimo uge 39

Kørekortregisteret:
1 stikprøve er afsluttet i marts 2017
1 stikprøve er planlagt og forventes afsluttet ultimo uge 42

KMD Social Pension:
1 stikprøve er afsluttet i marts 2017
1 stikprøve er iværksat og forventes afsluttet primo uge 39

Bibprint:
KFF arbejder på retningslinjer for stikprøver.
1 stikprøve iværksættes og forventes afsluttet ultimo uge 40

Systemhåndtering

Nyropsgade 1
1602 København V

EAN nummer
5798009781697

CallGuide, recording:
KFF har supplerende fået accept fra Koncernservice, IT–sikkerhed, til at tilføje CallGuide, recording til porteføljen af stikprøvekontroller. 1 stikprøve er iværksat og forventes afsluttet ultimo uge 38

Logning af søgninger i Notus Kommunal

KFF oplyste i supplerende høringssvar til Borgerrådgiveren af 5. oktober 2015, at it-systemet Notus Kommunal, ikke loggede søgninger, hvilket har ført til kritik fra Borgerrådgiverens side i den foreløbige rapport II.

På baggrund af et ønske om at kunne imødekomme Borgerrådgiverens kritik og i øvrigt om til enhver tid at være compliant, har KFF anskaffet et af leverandøren udviklet logningsmodul, der opfylder sikkerhedsbekendtgørelsens § 19. Modulet gør systemejer i stand til at logge både brug og søgninger, og forvaltningen påbegynder med udgangspunkt i dette modul stikprøvekontrol i systemet. Stikprøvekontrollen forventes afsluttet i uge 39.

BILAG 21 – BORGERRÅDGIVERENS MAIL AF 27. SEPTEMBER 2017 MED OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN

Fra: Borgerrådgiveren
Sendt: 27. september 2017 16:59
Til: Anette Lund Hansen; Malte Harrishøj
Emne: Vedrørende Borgerrådgiverens generelle egen driftsundersøgelse om logning af elektronisk sagsbehandling og borgeres adgang til indsigt i oplysninger

Prioritet: Høj

Kære begge

Borgerrådgiveren ses ikke at have modtaget et svar på sit spørgsmål stillet henholdsvis den 8. september 2017 samt den 11. september 2017 om udstrækningen af den stikprøvekontrol, som forvaltningen har foretaget siden 2015, hvorfor Borgerrådgiveren umiddelbart må konkludere, at forvaltningen alene har foretaget stikprøvekontroller af it-systemerne KMD Sag, Notus Kommunal, sygesikring og CPR (siden 2015), mens forvaltningen til dato ikke har fortaget stikprøvekontroller af andre systemer bortset fra de anførte systemer i Kultur- og Fritidsforvaltningens notat af 15. september 2017 til Borgerrådgiveren.

Er denne konklusion korrekt?

Spørgsmålet bedes besvaret med et "ja" eller et "nej" og inden 8 dage, idet Borgerrådgiveren ellers vil lægge denne konklusion til grund for sin endelige rapport, som herefter vil blive fremsendt og offentliggjort. Hvis spørgsmålet besvares med et "nej" bedes forvaltningen oplyse i hvilke andre it-systemer end de ovenfor anførte, der er foretaget stikprøvekontrol?

Med venlig hilsen
for Borgerrådgiveren

Daniel Soelberg Bach
Jurist

BORGER RÅDGIVEREN

KØBENHAVNS KOMMUNE

Vester Voldgade 2A
1552 København V

Telefon 33 66 14 00
Telefax 33 66 13 90
E-mail borgerraadgiveren@kk.dk
www.kk.dk/borgerraadgiveren

Følg os på Facebook
www.facebook.com/borgerraadgiveren

1

BILAG 22 – KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ OPFØLGENDE SPØRGSMÅL II (NOTAT AF 2. OKTOBER 2017)

KØBENHAVNS KOMMUNE
Kultur- og Fritidsforvaltningen
Center for Digitalisering og Innovation

NOTAT

2. oktober 2017

Sagsnr.
2017-0194178

Dokumentnr.
2017-0194178-14

Sagsbehandler
Anders C. S. Larsen

Svar til Borgerrådgiveren i forlængelse af mail af 27. september 2017

Borgerrådgiveren fremsender 27. september mail med følgende ordlyd:

"Borgerrådgiveren ses ikke at have modtaget et svar på sit spørgsmål stillet henholdsvis den 8. september 2017 samt den 11. september 2017 om udstrækningen af den stikprøvekontrol, som forvaltningen har foretaget siden 2015, hvorfor Borgerrådgiveren umiddelbart må konkludere, at forvaltningen alene har foretaget stikprøvekontroller af it-systemerne KMD Sag, Notus Kommunal, sygesikring og CPR (siden 2015), mens forvaltningen til dato ikke har fortaget stikprøvekontroller af andre systemer bortset fra de anførte systemer i Kultur- og Fritidsforvaltningens notat af 15. september 2017 til Borgerrådgiveren.

Er denne konklusion korrekt?

Spørgsmålet bedes besvaret med et "ja" eller et "nej" og inden 8 dage, idet Borgerrådgiveren ellers vil lægge denne konklusion til grund for sin endelige rapport, som herefter vil blive fremsendt og offentliggjort. Hvis spørgsmålet besvares med et "nej" bedes forvaltningen oplyse i hvilke andre it-systemer end de ovenfor anførte, der er foretaget stikprøvekontrol?"

Spørgsmålet besvares med et **"nej"**.

Nedenfor følger en liste over systemer, hvor systemejerskabet ligger i KFF, med angivelse af hvilket år, KFF har foretaget stikprøvekontroller:

2015	CPR (systemnavn CPR Web)
2016	CPR (systemnavn CPR Web) Kørekortregisteret KMD Social Pension
2017	CPR (systemnavn CPR Web) Kørekortregisteret KMD Social Pension Notus kommunal (sygesikring)

Der ud over er der planlagt følgende stikprøvekontroller i KFF i **nye** systemer, hvor systemejerskabet ligger i KFF, i efteråret 2017:
Bibprint

Systemhåndtering

Nyropsgade 1
1602 København V

EAN nummer
5798009781697

CallGuide, recordings

For de systemer, hvor systemejerskabet ligger i KFF, foretages der stikprøvekontroller på alle brugere, der har adgang til systemerne, hvad enten de er ansat i KFF eller andre steder.

Specifikt med hensyn til KMD Sag skal det oplyses, at systemejerskabet tidligere har ligget i SOF, men nu er flyttet til KIT, og at det derfor ikke er KFF, der er forpligtiget til at foretage stikprøvekontroller.

Der ud over kan det, i forlængelse af Borgerrådgiverens liste over it-systemer som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger fra den foreløbige rapport II side 5, oplyses, at KFF udelukkende har systemejerskabet for følgende af systemerne på listen:

- Notus Kommunal, sygesikring
- CPR
- Pasregisteret
- Kørekortsregisteret
- Straksudstedelse af NemID (NemID Privat)
- ID-Port (pas og kørekort)
- Køreprøvebookning
- P-Data (KMD udtræk fra CPR)
- Safepay, kasseløsning

I forbindelse med Legal Compliance Projektet gennemgår KFF hele systemporteføljen, herunder ovenstående systemer, med henblik på at sikre at forvaltningen fremadrettet er compliant på stikprøvekontrolområdet.

BILAG 23 – DATATILSYNETS UDTALELSE AF 26. JUNI 2006

DATATILSYNET

Forside / Afgørelser

Udtalelse om datasikkerhed i borgerservice

Brevdato: 26.06.06

Journalnummer: 2006-329-0022

I forbindelse med lovforslaget om kommunale borgerservicecentre tilkendegav Indenrigs- og Sundhedsministeriet, at ministeriet i samarbejde med KL ville udarbejde vejledningsmateriale vedrørende oprettelse og anvendelse af borgerservicecentre.

I forlængelse heraf sendte Indenrigs- og Sundhedsministeriet den 25. januar 2006 Datatilsynet et udkast til et kapitel om datasikkerhed, som skulle indgå i en vejledning/guide om etablering af borgerservicecentre. Guiden blev udarbejdet sammen med KL.

Udkastet gav Datatilsynet anledning til en række bemærkninger, som tilsynet fremsendte den 10. februar 2006.

Bl.a. af tidsmæssige grunde valgte Indenrigs- og Sundhedsministeriet og KL at udskille kapitlet om datasikkerhed til en selvstændig vejledning.

Datatilsynet har herefter været i løbende dialog med Indenrigs- og Sundhedsministeriet, og der blev den 4. maj 2006 afholdt et møde med deltagelse af ministeriet, KL og Datatilsynet.

Indenrigs- og Sundhedsministeriet har den 1. juni 2006 fremsendt udkast til publikationen "Datasikkerhed i borgerservicecentre – regler og praksis" med anmodning om Datatilsynets bemærkninger. Det er planen, at publikationen skal udgives i et samarbejde mellem ministeriet, KL og Datatilsynet.

Der er i udkastet til publikationen stillet en række mindre spørgsmål, som Datatilsynet vil besvare telefonisk. I denne udtalelse vil alene blive behandlet spørgsmålet om, hvilke yderligere sikkerhedsforanstaltninger der skal iværksættes i borgerservicecentre.

Det fremgår af vejledningen, at kommunerne kan vælge mellem forskellige ordninger, som styrker sikkerheden, f.eks. give medarbejderne særlig instruktion i datasikkerhed, foretage stikprøver af loggen fra anmeldelsespligtige systemer og give borgerne adgang til en overordnet log via en elektronisk selvbetjeningsløsning.

Datatilsynet skal – efter at sagen har været behandlet i Datarådet – udtale følgende:

1. Generelle bemærkninger om styrkelse af behandlingssikkerheden

Efter persondatalovens § 41, stk. 3, skal der træffes de fornødne tekniske og organisatoriske 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.

Pligten til at træffe fornødne sikkerhedsforanstaltninger påhviler efter persondatalovens § 41, stk. 3, såvel den dataansvarlige som en eventuel databehandler.

Bestemmelsen er for den offentlige forvaltning nærmere udmøntet i sikkerhedsbekendtgørelsen.

Datatilsynet har flere gange i forbindelse med strukturreformen udtalt sig om behandlingssikkerhed. F.eks. Datatilsynets høringssvar af 7. april 2004 over Strukturkommissionens betænkning nr. 1434/2004, tilsynets høringsvar af 7. januar 2005 over forslaget til lov om kommunale borgerservicecentre og tilsynets brev af 30. marts 2005 med bidrag til besvarelse af spørgsmål 1 til L 72 (forslag til borgerservicecenterloven).

I Datatilsynets høringssvar af 7. januar 2005 over forslaget til lov om kommunale borgerservicecentre tilkendegav tilsynet, at den pågældende brug af medarbejdere til løsning af forskellige opgaver gør det påkrævet, at der i forbindelse med servicecenterkonstruktionen og IT-understøttelsen af centrene sker en forøgelse af behandlingssikkerheden, herunder med hensyn til styring af brugerrettigheder og interne kontrolordninger i forhold til medarbejdernes anvendelse af IT-systemerne.

Datatilsynet tilkendegav samtidig, at etablering af servicecentre medfører, at kommunerne må styrke uddannelse og vejledning af medarbejderne om behandlingen af personoplysninger, herunder navnlig under hvilke betingelser en medarbejder lovligt kan behandle personoplysninger, som vedkommende er autoriseret til.

Tilsynet udtalte desuden, at det herudover kan være relevant at supplere adgangskontrol og autorisationsordninger med andre løsninger.

2. De tre foreslåede ordninger

Indledningsvis bemærkes, at tilsynets krav til datasikkerheden ikke alene har karakter af anbefalinger. Det følger således af § 4 i sikkerhedsbekendtgørelsen, at Datatilsynet kan komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger. Tilsynet skal derfor anmode om, at det på side 3 præciseres, at der er tale om tilsynets **henstillinger** til styrkelse af datasikkerheden og ikke tilsynets **anbefalinger**.

Datatilsynet finder endvidere, at det skal fremgå af vejledningen – f.eks. som et nyt afsnit 2 på side 17 – at kommunens udmøntning af de i publikationen beskrevne krav så vidt muligt skal udformes som bindende tjenestebefalinger til medarbejderne.

I det følgende vil Datatilsynet kommentere de tre forslag til ordninger til styrkelse af behandlingssikkerheden, som er nævnt i vejledningen.

Det skal understreges, at der efter tilsynets opfattelse **ikke** – som anført på side 7 i publikationen – er valgfrihed for kommunerne mellem de tre foreslåede ordninger.

2.1. Instruktion af medarbejdere

Efter sikkerhedsbekendtgørelsens § 6 skal den dataansvarlige myndighed give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder

gøres bekendt med de regler, der er fastsat i medfør af § 5 (myndighedens uddybende sikkerhedsregler).

Datatilsynet skal generelt bemærke, at den øgede adgang til fortrolige og følsomme personoplysninger i borgerservicecentre selvsagt gør instruktionen af medarbejderne helt central. Tilsynet finder det positivt, at der lægges op til at højne medarbejdernes viden om datasikkerhed med kurser mv.

Selv en skærpet instruktion til medarbejderne kan imidlertid efter Datatilsynets opfattelse ikke **i sig selv** udgøre en tilstrækkelig styrkelse af behandlingssikkerheden. Tilsynet lægger i den forbindelse vægt på, at forpligtelsen til at give fornøden instruktion allerede påhviler kommunerne efter sikkerhedsbekendtgørelsens § 6.

Datatilsynet finder, at behovet for styrkelse af uddannelse og vejledning af medarbejderne gælder **ved siden af** behovet for forøgelsen af behandlingssikkerheden. Der skal således **under alle omstændigheder** gives medarbejderne den instruktion, der er fornøden under hensyn til medarbejderens opgaver. Tilsynet forudsætter, at medarbejderne i borgerservicecentre får særlig instruktion i datasikkerhed.

Det bemærkes, at overskriften i boksen på side 17 i vejledningen bør være "Medarbejderne skal især vejledes i:" og ikke "Medarbejderne bør…".

2.2. Borgernes adgang til log-oplysninger

Efter persondatalovens § 31 er der ikke ret til indsigt i den log, der efter sikkerhedsbekendtgørelsens § 19 skal foretages ved behandling af oplysninger omfattet af anmeldelsespligten til Datatilsynet.

Datatilsynet har imidlertid ved flere lejligheder udtalt, at det som led i styrkelsen af behandlingssikkerheden kan overvejes at gøre oplysninger om, hvem der har set oplysninger om en borger, tilgængelige i en elektronisk selvbetjeningsløsning. Dette kendes fra den medicinprofil, som Lægemiddelstyrelsen er dataansvarlig for.

I vejledningen er anført en række forhold, som kommunerne skal være opmærksomme på ved etablering af sådanne løsninger.

Det er Datatilsynets opfattelse, at muligheden for adgang til sådanne oplysninger er værdifuld for borgerne. Tilsynet skal således opfordre til, at der under alle omstændigheder arbejdes videre med denne løsning. Datatilsynet skal anmode om at blive orienteret om, hvad der foretages vedrørende denne løsning, samt det tidsmæssige perspektiv herfor.

Datatilsynet skal i den forbindelse påpege, at angivelsen af, hvem der har indhentet oplysninger om en borger, må ske på et niveau, der er relevant og tilstrækkeligt præcist til, at løsningen kan tjene sit formål.

Tilsynet skal opfordre til, at kommuner, der påtænker at etablere sådanne løsninger, kontakter Datatilsynet med henblik på nærmere drøftelser om udformningen, sikkerhedsniveauet osv.

Datatilsynet må samtidig understrege, at en borgeradgang til log-oplysninger ikke afskærer retten til indsigt efter persondatalovens § 31.

2.3. Stikprøvekontrol af loggen

Datatilsynet finder, at den øgede adgang til personoplysninger i borgerservicecentre gør det påkrævet, at der foretages stikprøvekontrol af loggen. Dette gælder dog alene systemer, hvori der indgår anmeldelsespligtige behandlinger af personoplysninger, dvs. systemer, hvor der efter sikkerhedsbekendtgørelsen allerede er krav om logning.

Ifølge udkastet til publikationen skal stikprøverne foretages på kommunens eget initiativ, med jævne mellemrum og med vilkårlige intervaller.

Der er i den forbindelse givet et eksempel på, hvordan ordningen kan være beskrevet i kommunens uddybende sikkerhedsregler.

Datatilsynet finder, at det i eksemplet anførte, hvorefter kontrollen foretages med forskellige intervaller, dog højst 6 måneder, er udtryk for en passende afvejning af de bagvedliggende hensyn.

Datatilsynet skal herefter **henstille**, at kommuner, der etablerer borgerservicecentre, som minimum foretager stikprøvekontrol af logfiler i et omfang, der svarer til det anførte i eksempelboks 8 i udkastet til publikationen. Tilsynet finder, at det bør fremgå af selve teksten (og ikke blot som eksempel), at kontrollen skal foretages som anført.

Det tilføjes, at Datatilsynet vil være indstillet på at lade den manuelle stikprøvekontrol af loggen erstatte af en automatiseret overvågning, der bl.a. afdækker uhensigtsmæssige eller usædvanlige søgemønstre og dermed er bedre egnet end stikprøvekontrol til at afsløre misbrug.

3. Afsluttende bemærkninger

Datatilsynet forventer at blive hørt over den vejledning til medarbejderne i borgerservicecentre, som er under udarbejdelse. Tilsynet forudsætter, at forslaget om, at medarbejderne skal notere, hvorfor oplysningerne er indhentet, overvejes i forbindelse med udarbejdelsen af vejledningen til medarbejderne i borgerservicecentrene.

Tilsynet vil snarest kontakte Indenrigs- og Sundhedsministeriet med henblik på besvarelse af de øvrige spørgsmål, som er rejst i udkastet til publikationen.

Tilbage til alle afgørelser

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk

BILAGSRAPPORT

Redaktion
Borgerrådgiveren

Kontakt
Københavns Kommune
Vester Voldgade 2A
1552 København V

Foto
Borgerrådgiveren

Tryk

Oplag

ISBN

Udgiver
Borgerrådgiveren

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Vester Voldgade 2A
1552 København V
Telefon: 33 66 14 00
Telefax: 33 66 13 90
E-mail: borgerraadgiveren@kk.dk
www.kk.dk/borgerraadgiveren