LOGNING AF ELEKTRONISK SAGSBEHANDLING OG BORGERES ADGANG TIL INDSIGT I OPLYSNINGER

ENDELIG RAPPORT

BORGERRÅDGIVERENS EGEN DRIFT-UNDERSØGELSER

INDHOLDSFORTEGNELSE

1. INDLEDNING

Denne rapport indeholder Borgerrådgiverens endelige vurderinger og bedømmelser i anledning af Borgerrådgiverens undersøgelse vedrørende dels logning af Københavns Borgerservices elektroniske sagsbehandling i it-systemer, hvor der behandles følsomme og fortrolige personoplysninger, og dels borgeres adgang til indsigt i oplysninger efter persondataloven ved Københavns Borgerservice.

Borgerrådgiveren indledte undersøgelsen ved iværksættelsesbrev af 8. august 2014 til Kultur- og Fritidsforvaltningen, idet Københavns Borgerservice organisatorisk hører under Kultur- og Fritidsforvaltningen. Undersøgelsen blev iværksat over for Kultur- og Fritidsforvaltningen, 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 måtte anvende til behandling af følsomme og fortrolige personoplysninger.

Borgerrådgiveren overførte senere 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 Kultur- og Fritidsforvaltningen på daværende tidspunkt oplyste var det eneste it-system, som Københavns Borgerservice anvendte til behandling af følsomme og fortrolige personoplysninger.

Borgerrådgiveren overførte efterfølgende 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 Koncernservice (herefter Koncern IT)[1] til KMD Sag.

Kultur- og Fritidsforvaltningen har i høringsbemærkninger af 28. april 2017 til Borgerrådgiverens foreløbige rapport korrigerende oplyst, at Københavns Borgerservice anvender i alt 14 forskellige it-systemer, hvori der behandles følsomme og fortrolige personoplysninger. Herudover har Kultur- og Fritidsforvaltningen i svar af 15. september 2017 og 2. oktober 2017 på Borgerrådgierens opfølgende spørgmsål tilføjet et yderligere it-system således, at Københavns Borgerservice anvender i alt 15 forskellige it-systemer, hvori der behandles følsomme og fortrolige personoplysninger se afsnit 2 nedenfor.

Undersøgelsen har snitflade dels til Borgerrådgiverens inspektionsrapport med fokus på digitalisering og datasikkerhed ved Borgerservice Bispebjerg under Kultur- og Fritidsforvaltningen[2] og særligt til Borgerrådgiverens generelle egen drift-undersøgelse vedrørende sikring af borgernes personoplysninger ved Koncern IT under Økonomiforvaltningen, hvor Borgerrådgiveren har udtalt kritik af Koncern IT's manglende tilsyn med forvaltningernes kontrol af med afviste adgangsforsøg samt forvaltingernes logopfølgning[3].

Vurderingsgrundlaget for undersøgelsen er lov om behandling af personoplysninger (herefter persondataloven), bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (herefter sikkerhedsbekendtgørelsen), Datatilsynets vejledning til sikkerhedsbekendtgørelsen, Regulativ for it-sikkerhed i Københavns Kom-

[1] Koncernservice blev den 28. april 2016 udskilt til en ny selvstændig forvaltningsenhed under navnet Koncern IT, hvorfor denne betegnelse anvendes herefter i rapporten.

[2] https://www.kk.dk/sites/default/files/Endelig%20rapport%20om%20inspektion%20af%20Borgerservicecenter%20Bispebjerg.PDF

[3] https://www.kk.dk/sites/default/files/Endelig%20rapport%20af%2024.%20august%202015%20%28Sikring%20af%20borgernes%20personoplysninger%29.pdf

mune, uddybende it-sikkerhedsregler for Københavns Kommune samt Datatilsynets udtalelse om datasikkerhed i borgerservice.

Til brug for undersøgelsen har Borgerrådgiveren modtaget høringssvar mv. fra Kultur- og Fritidsforvaltningen, Socialforvaltningen samt Økonomiforvaltningen.

Rapporten har i foreløbige udgaver været sendt til Kultur- og Fritidsforvaltningen, Socialforvaltningen og Økonomiforvaltningen med henblik på forvaltningernes eventuelle bemærkninger til rapportens faktiske oplysninger.

Rapporten er inddelt i en hoveddel, der indeholder følgende afsnit: Konklusion og sammenfatning, konsekvenser, forslag, henstillinger og anbefalinger, uddybende bistand mv. samt Borgerrådgiverens kritikskala. I rapportens bilag findes følgende: Borgerrådgiverens observationer og vurderinger, metode, vurderingsgrundlag (juridiske regler og dokumentation), Borgerrådgiverens høringsbrev, forvaltningens høringssvar samt opfølgende spørgsmål og svar.

Borgerrådgiveren november 2017

Johan Busse
Borgerrådgiver

2. KONKLUSION OG SAMMENFATNING

Denne rapport handler om logning af Københavns Borgerservices elektroniske sagsbehandling i følgende it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger[4]:

- KMD Sag
- Skat Extranet (kommunal indgang til skat)
- CSC Social
- Notus Kommunal, sygesikring
- CPR
- KMD Social Pension
- Kørekortsregisteret
- Pasregisteret
- Straksudstedelse af NemID (NemID Privat)
- ID-Port (pas og kørekort)
- Køreprøvebookning
- P-Data (KMD udtræk fra CPR)
- Safepay, kasseløsning
- KMD Mainframe
- Fritagelse for digital post

Rapporten omhandler også borgernes adgang til indsigt i oplysninger efter persondataloven ved Københavns Borgerservice.

Rapporten omfatter ikke it-systemer, som Københavns Borgerservice har taget i brug efter tidspunktet for iværksættelse af undersøgelsen.

OPSUMMERING

Københavns Kommune har ifølge persondataloven ansvaret for, at de personoplysninger, som behandles af kommunen, er beskyttet med fornødne sikkerhedsforanstaltninger. Dette er en del af kontrakten med borgerne om, at vi håndterer deres personoplysninger på en betryggende og sikker måde med respekt for privatlivets fred.

En del af disse sikkerhedsforanstaltninger består i, at der skal ske logning af behandling af følsomme og fortrolige personoplysninger (altså en foranstaltning der systematisk dokumenterer hændelser, herunder hvem, der har skaffet sig adgang til eller ændret i data mv.).

I forlængelse heraf skal der foretages registrering af afviste adgangsforsøg til it-systemer, hvor der behandles følsomme og fortrolige personoplysninger, og der skal løbende følges op herpå.

[4] Der har været udpeget en systemejer i Socialforvaltningen til it-systemet KMD Sag frem til den 31. december 2014. Fra den 1. januar 2015 har der været udpeget en systemejer i Koncern IT til it-systemet KMD Sag. Der er udpeget en systemejer i Koncern IT til it-systemet Skat Extranet. Der er udpeget en systemejer i Socialforvaltningen til it-systemet CSC Social. Der er udpeget en systemejer i Kultur- og Fritidsforvaltningen i forhold til de øvrige it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger. It-systemerne KMD Mainframe og fritagelse for digital post har ikke systemejere.

Desuden skal kommunen løbende foretage stikprøvekontrol af loggen af behandlingen af følsomme personoplysninger.

Borgerrådgiveren har overordnet konstateret, at Københavns Borgerservice enten ikke har haft tilstrækkeligt overblik over i hvilke it-systemer, der behandles fortrolige og følsomme oplysninger eller ikke har haft tilstrækelig forståelse for lovens begrebsmæssige afgrænsning af sådanne oplysninger.

Borgerrådgiveren har konstateret, at kommunen på de undersøgte områder ikke har eller ikke har haft de krævede sikkerhedsforanstaltninger i en længere årrække.

Borgerrådgiveren har konkret konstateret, at der igennem en længere årrække ikke er foretaget stikprøvekontroller af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Sag, CPR, KMD Social Pension, kørekortsregisteret og Notus Kommunal.

Borgerrådgiveren har endvidere konkret konstateret, at der ikke er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne Skat Extranet, CSC Social, NemID (NemID Privat), KMD Mainframe, ID-Port (pas og kørekort), køreprøvebookning, P-Data (KMD udtræk fra CPR) og Safepay, kasseløsning.

Borgerrådgiveren udtaler kritik af disse forhold.

Borgerrådgiveren har endvidere konstateret, at It-sikkerhedsfunktionen i Koncern IT først i december 2015 begyndte at føre tilsyn med stikprøvekontrollerne i Københavns Borgerservice.

Borgerrådgiveren udtaler også kritik af dette.

Endelig udtaler Borgerrådgiveren kritik af Koncern IT's vejledning om stikprøvekontrol.

Borgerrådgiveren konstaterer, at der er foretaget opfølgning på registrering af afviste adgangsforsøg til it-systemerne KMD Sag, CPR, KMD Mainframe og ID-Port, som der skal.

Borgerrådgiveren kan ikke på grundlag af det modtagne materiale fra forvaltningerne vurdere, om der er foretaget opfølgning på registrering af Københavns Borgerservices afviste adgangsforsøg til de øvrige it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger.

LOGNING AF KØBENHAVNS BORGERSERVICES ELEKTRONISKE SAGSBEHANDLING

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

Min undersøgelse viser, at der er foretaget opfølgning på registrering af afviste adgangsforsøg til it-systemerne KMD Sag, CPR, KMD Mainframe og ID-Port, i overensstemmelse med sikkerhedsbekendtgørelsens § 18.

Jeg kan ikke på grundlag af det modtagne materiale fra forvaltningerne vurdere, om der er foretaget opfølgning på registrering af Københavns Borgerservices afviste adgangsforsøg til de øvrige it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger.

Logning af søgninger i it-systemet Notus Kommunal, sygesikring
Kultur- og Fritidsforvaltningen har i supplerende høringssvar af 5. oktober 2015 oplyst, at it-systemet Notus Kommunal, sygesikring, ikke logger søgninger.

Det er min opfattelse, at søgninger på personer i Notus Kommunal, sygesikring, kan resultere i fremsøgning af 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 Fritidsforvaltningen i notat af 15. september 2017 har oplyst, at forvaltningen nu har anskaffet et logningsmodul, som kan logge søgninger i it-systemet Notus Kommunal, sygesikring.

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

Min undersøgelse viser, at Kultur- og Fritidsforvaltningen generelt ikke har haft fornødent overblik over, hvilke it-systemer Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger.

Jeg har noteret mig, at Kultur- og Fritidsforvaltningen 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 først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag fra december 2015.

Min undersøgelse viser, at det er uklart, hvor hyppigt der er foretaget stikprøvekontrol fra december 2015 og indtil eftersommeren 2017, hvor det er blevet muligt at foretage automatisk lopfølgning (SIEM løsning) i it-systemet KMD Sag. Der er uoverensstemmelse mellem Kultur- og Fritidsforvaltningens og Økonomiforvaltningens oplysninger om hyppigheden af stikprøvekontroller i it-systemet KMD i den ovenfor anførte periode.

Den igennem en længere årrække manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet KMD Sag er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg finder, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandlingen af fortrolige og følsomme personoplysninger i it-systemet KMD Sag indtil december 2015 er kritisabel.

CPR
Min undersøgelse viser, at der først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CPR fra 2015.

Den igennem en længere årrække manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CPR er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg finder, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandlingen af fortrolige og følsomme personoplysninger i it-systemet CPR indtil 2015 er kritisabel.

KMD Social Pension og kørekortsregisteret
Min undersøgelse viser, 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.

Den igennem en længere årrække manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Social Pension og kørekortsregisteret er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg finder, 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 kritisabel.

Notus Kommunal, sygesikring
Min undersøgelse viser, at der først er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Notus Kommunal, sygesikring, fra 2017.

Den igennem en længere årrække manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Notus Kommunal, sygesikring, er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg finder, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandlingen af fortrolige og følsomme personoplysninger i it-systemet Notus Kommunal, sygesikring indtil 2017 er kritisabel.

Skat Extranet
Min undersøgelse viser, at der ikke er foretaget stikprøvekontrol af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet.

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 finder, at den manglende stikprøvekontrol af loggen af behandlingen af fortrolige og følsomme personoplysninger i it-systemet Skat Extranet er kritisabel.

CSC Social
Min undersøgelse viser, at der ikke er foretaget stikprøvekontrol af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemet CSC Social.

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 finder, at den manglende stikprøvekontrol af loggen af behandlingen af fortrolige og følsomme personoplysninger i it-systemet CSC Social er kritisabel.

Øvrige it-systemer
De øvrige it-systemer, som Københavns Borgerservice anvender til behandling af fortrolige og følsomme personoplysninger, omfatter 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.

Min undersøgelse viser, at der ikke er foretaget stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i de ovenfor øvrige anførte it-systemer.

Den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i de ovenfor øvrige anførte it-systemer er i strid med Datatilsynets udtalelse af 26. juni 2006 og Københavns Kommunes it-sikkerhedsregler.

Jeg finder, at den manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i de ovenfor øvrige anførte it-systemer er kritisabel.

It-sikkerhedsfunktionens vejledning om stikprøvekontrol

Min undersøgelse viser, at It-sikkerhedsfunktionen i Koncern IT først i efteråret 2015 udarbejdede vejledningen "Krav om stikprøver af loggen i borgerservicecentre" og best practice "for gennemførelse af stikprøvekontrol af loggen".

Jeg finder det beklageligt, at It-sikkerhedsfunktionen i Koncern IT ikke fulgte op over for Københavns Borgerservice med vejledning og best practice tidligere. Jeg lægger vægt på, at It-sikkerhedsfunktionen blev oprettet i marts 2010, hvorved It-sikkerhedsfunktionen fik kompetence til at vejlede mv. om it-sikkerhedsspørgsmål.

Min undersøgelse viser, at vejledningen "Krav om stikprøver af loggen i borgerservicecentre" er formuleret som en anbefaling til Københavns Borgerservice om at foretage stikprøvekontrol.

Jeg finder det beklageligt, at It-sikkerhedsfunktionens vejledning er formuleret som en anbefaling og ikke som et pålæg om at foretage stikprøvekontrol i samarbejde med systemejeren. Jeg lægger vægt på, at Datatilsynets udtalelse forpligtiger kommuner, der etablerer borgerservicecentre, til at foretage stikprøvekontrol af loggen jf. sikkerhedsbekendtgørelsens § 4, og at It-sikkerhedsfunktionen i Koncern IT har adgang til give pålæg 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

Min undersøgelse viser, at It-sikkerhedsfunktionen i Koncern IT først i december 2015 førte tilsyn med hensyn til foretagelse af stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemer ved Københavns Borgerservice.

Jeg finder, at It-sikkerhedsfunktionens manglende tilsyn med hensyn til foretagelse af stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger er kritisabelt. Jeg lægger vægt på, at It-sikkerhedsfunktionen efter min opfattelse på et langt tidligere tidspunkt end sket burde have foretaget tilsyn i overensstemmelse med Datatilsynets udtalelse.

Lovreglerne følger af persondataloven og sikkerhedsbekendtgørelsen.

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

De nærmere sikkerhedsforanstaltninger er udmøntet i sikkerhedsbekendtgørelsen. Ifølge sikkerhedsbekendtgørelsens § 18 skal der foretages registrering af afviste adgangsforsøg til it-systemer, hvor der behandles følsomme personoplysninger, og der skal løbende følges op. Ifølge sikkerhedsbekendtgørelsens § 19 skal der ske logning af behandling af følsomme personoplysninger.

Udover ovenstående lovregler har det siden Datatilsynets udtalelse af 26. juni 2006 om datasikkerhed i borgerservicecentre været et krav, at kommuner, der etablerer borgerservicecentre, løbende skal foretage stikprøvekontrol af loggen af behandlingen af følsomme personoplysninger.

Kommunens it-sikkerhedsregler følger af Regulativ for it-sikkerhed i Københavns Kommune, herunder af uddybende it-sikkerhedsregler for Københavns Kommune.

I Regulativ for it-sikkerhed i Københavns Kommune er de interne organisatoriske forhold i relation til ansvaret for it-sikkerhedsforanstaltninger fastlagt. Det påhviler bl.a. It-sikkerhedsfunktionen i Koncern IT at føre dagligt tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser. Herudover har It-sikkerhedsfunktionen en rådgivning- og vejledningsfunktion i relation til it-sikkerhed. It-sikkerhedsfunktionen i Koncern IT har haft den daglige tilsynspligt, herunder rådgivnings- og vejledningsfunktionen, siden Borgerrepræsentationen den 16. december 2010 godkendte det daværende Regulativ for it-sikkerhed i Københavns Kommune.

Systemejernes ansvar i relation til it-sikkerhedsforanstaltninger følger ligeledes af Regulativ for it-sikkerhed i Københavns Kommune. Systemejerne har bl.a. ansvaret for, at it-systemerne efterlever it-sikkerhedskravene, og at systemejer kan logge, når det er påkrævet. Efter de uddybende it-sikkerhedsregler for Københavns Kommune skal der ske opfølgning på registrering af afviste adgangsforsøg og opfølgning på loggen af behandling af personfølsomme oplysninger. Ifølge ansvarsuddelegeringen efter Regulativ for it-sikkerhed i Københavns Kommune påhviler det den til enhver tid værende systemejer i forhold til de enkelte it-systemer, som anvendes til behandling af følsomme personoplysninger, at foretage opfølgning på registrering af afviste adgangsforsøg og opfølgning på loggen af behandling af følsomme personoplysninger.

ADGANG TIL INDSIGT I PERSONOPLYSNINGER EFTER PERSONDATALOVEN

Jeg finder, at proceduren ved Københavns Borgerservice ved anmodning af indsigt i personoplysninger efter persondataloven 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.

3. KONSEKVENSER

De konstaterede fejl med hensyn til den i gennem en længere årrække manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne KMD Sag, CPR, KMD Social Pension, kørekortsregisteret og Notus Kommunal, sygesikring kan betyde, at eventuelt misbrug af fortrolige og følsomme personoplysninger i disse it-systemer ved Københavns Borgerservice ikke er blevet identificeret igennem en årrække, fordi der alene er sket logopfølgning i tilfælde af konkret mistanke om misbrug.

Den manglende log på søgninger af personer i it-systemet Notus Kommunal, sygesikring, frem til Københavns Borgerservice anskaffede et logningsmodul, som kan logge søgninger, kan betyde, at eventuelt misbrug af fortrolige og følsomme personoplysninger i forbindelse med søgninger af personer i it-systemet, ikke er blevet identificeret igennem en længere årrække.

Den konstaterede fejl med hensyn til manglende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i it-systemerne Skat Extranet, CSC Social, 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, kan betyde, at eventuelt misbrug af fortrolige og følsomme personoplysninger i disse it-systemer ved Københavns Borgerservice ikke identificeres, fordi der alene sker logopfølgning i tilfælde af konkret mistanke om misbrug.

De konstaterede fejl med hensyn til den manglende stikprøvekontrol i it-systemerne Skat Extranet, CSC Social, 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, herunder It-sikkerhedsfunktionens manglende tilsyn med logopfølgning, kan betyde, at Københavns Kommune, som dataansvarlig i forhold til behandling af fortrolige og følsomme personoplysninger, ikke lever op til artikel 5, nr. 1, litra f, i den nye persondataforordning, som træder i kraft den 25. maj 2018.

4. FORSLAG, HENSTILLINGER OG ANBEFALINGER

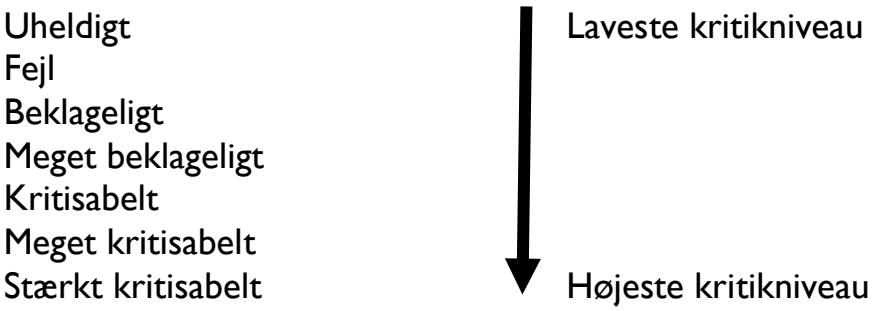
Borgerrådgiveren henstiller, at It-sikkerhedsfunktionen i Koncern IT sikrer, at der foretages løbende stikprøvekontrol af loggen af Københavns Borgerservices behandling af fortrolige og følsomme personoplysninger i de it-systemer ved Københavns Borgerservice, hvor der ikke aktuelt foretages stikprøvekontol, indtil eventuel automatiseret logopfølgning kan erstatte manuel stikprøvekontrol.

5. UDDYBNING, BISTAND MV.

Borgerrådgiveren uddyber gerne undersøgelsen samt vurderinger mv. på et møde, såfremt det ønskes. Forvaltningen bedes i givet fald kontakte Daniel Soelberg Bach på tlf. 33 66 14 00 eller pr. e-mail borgerraadgiveren@kk.dk for nærmere aftale.

Borgerrådgiveren hjælper også meget gerne til med intern opfølgning på sagen, herunder i form af undervisning, vejledning om reglernes anvendelse i praksis mv. Forvaltningen bedes i givet fald kontakte samme medarbejder for nærmere aftale.

BORGERRÅDGIVERENS KRITIKSKALA



Kritikskalaen spænder fra konstatering af forhold, der ikke er, som de bør være, uden at nogen konkret bebrejdes herfor (uheldigt) over kritik af forhold, der er mere eller mindre almindeligt forekommende i offentlig forvaltning, men ikke bør forekomme og til kritik af helt utilstedelige og uacceptable forhold (stærkt kritisabelt). Konstateringer af, at noget er uheldigt, registreres ikke som en egentlig kritik i Borgerrådgiverens statistik.

Det bemærkes, at Borgerrådgiveren ud over ovennævnte kritikskala naturligvis supplerende kan uddybe og kvalificere sin kritik i almindeligt sprog.

BILAG – SE SÆRSKILT RAPPORT

BILAG 1 BORGERRÅDGIVERENS OBSERVATIONER OG VURDERINGER
BILAG 2 METODE
BILAG 3 VURDERINGSGRUNDLAG
BILAG 4 BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL KULTUR- OG FRITIDSFORVALTNINGEN
BILAG 5 HØRINGSSVAR FRA KULTUR- OG FRITIDSFORVALTNINGEN OG UDVALGT DOKUMENTATION
BILAG 6 OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN
BILAG 7 KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL
BILAG 8 BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL SOCIALFORVALTNINGEN
BILAG 9 HØRINGSSVAR FRA SOCIALFORVALTNINGEN
BILAG 10 BORGERRÅDGIVERENS IVÆRKSÆTTELSESBREV TIL ØKONOMIFORVALTNINGEN
BILAG 11 HØRINGSSVAR FRA ØKONOMIFORVALTNINGEN OG UDVALGT DOKUMENTATION
BILAG 12 ØKONOMIFORVALTNINGENS HØRINGSBEMÆRKNINGER
BILAG 13 OPFØLGENDE SPØRGSMÅL TIL KONCERN IT
BILAG 14 ØKONOMIFORVALTNINGENS SVAR PÅ BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL
BILAG 15 KULTUR- OG FRITIDSFORVALTNINGENS HØRINGSBEMÆRKNINGER
BILAG 16 ØKONOMIFORVALTNINGENS HØRINGSBEMÆRKNINGER II
BILAG 17 SOCIALFORVALTNINGENS HØRINGSBEMÆRKNINGER II
BILAG 18 KULTUR- OG FRITIDSFORVALTNINGENS HØRINGSBEMÆRKNINGER II
BILAG 19 BORGERRÅDGIVERENS OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN (UDKLIP AF REFERATARK, DOK.NR. 2014-0118160-11)
BILAG 20 KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ OPFØLGENDE SPØRGSMÅL (NOTAT AF 15. SEPTEMBER 2017)
BILAG 21 BORGERRÅDGIVERENS MAIL AF 27. SEPTEMBER 2017 MED OPFØLGENDE SPØRGSMÅL TIL KULTUR- OG FRITIDSFORVALTNINGEN
BILAG 22 KULTUR- OG FRITIDSFORVALTNINGENS SVAR PÅ OPFØLGENDE SPØRGSMÅL II (NOTAT AF 2. OKTOBER 2017)

BILAG 23 DATATILSYNETS UDTALELSE AF 26. JUNI 2006

LOGNING AF ELEKTRONISK SAGSBEHANDLING OG BORGERES ADGANG TIL INDSIGT I OPLYSNINGER

ENDELIG RAPPORT

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