SIKRING AF BORGERNES PERSONOPLYSNINGER

BILAG

BORGERRÅDGIVERENS EGEN DRIFT-UNDERSØGELSER

KØBENHAVNS KOMMUNE

INDHOLDSFORTEGNELSE

BILAG 1 – BORGERRÅDGIVERENS OBSERVATIONER OG VURDERINGER 5

BILAG 2 – METODE 7
2.1 GENERELT FOR BORGERRÅDGIVERENS EGEN DRIFT-UNDERSØGELSER 7
2.2 DENNE UNDERSØGELSES METODE 7
2.3 REAKTIONSMIDLER OG BEDØMMELSESGRUNDLAG 7

BILAG 3 – VURDERINGSGRUNDLAG 9
3.1 DET JURIDISKE GRUNDLAG 9
PERSONDATALOVEN 9
SIKKERHEDSBEKENDTGØRELSEN 9
REGULATIV FOR IT-SIKKERHED I KØBENHAVNS KOMMUNE 11
UDDYBENDE SIKKERHEDSREGLER FOR KØBENHAVNS KOMMUNE 14
3.2 DOKUMENTATIONSGRUNDLAGET (DATA) 14

BILAG 4 – BORGERRÅDGIVERENS HØRINGSBREV 15

BILAG 5 – FORVALTNINGENS HØRINGSSVAR 23

BILAG 6 - OPFØLGENDE SPØRGSMÅL OG SVAR 33

BILAG 7 – TELEFONINTERVIEWS 35

BILAG 1 – BORGERRÅDGIVERENS OBSERVATIONER OG VURDERINGER

Københavns Kommune har i medfør sikkerhedsbekendtgørelsens § 5 udstedt Regulativ for it-sikkerhed i Københavns Kommune, som indeholder kommunens interne bestemmelser om sikkerhedsforanstaltninger til beskyttelse af personoplysninger i henhold til gældende lovkrav (dvs. persondataloven og sikkerhedsbekendtgørelsen).

Det følger af Regulativ for it-sikkerhed i Københavns Kommune, at Borgerrepræsentationen vedtager kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ efter indstilling fra Koncernservice i Økonomiforvaltningen. Økonomiudvalget varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it-sikkerhedsforhold. Overborgmesteren og borgmestrene for de enkelte forvaltninger har ansvaret for it-sikkerhedsarbejdet inden for hvert deres forvaltningsområde. Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen. Koncernservice er bl.a. ansvarlig for fællessystemer, drift og it-sikkerhedsfunktionen. It-sikkerhedsfunktionen i Koncernservice fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser. It-sikkerhedsfunktionen har en række opgaver, bl.a. skal funktionen rådgive kommunen om it-sikkerhedsmæssige forhold, fastsætte uddybende sikkerhedsregler, sikre at der sker kontrol af adgangsrettigheder og autorisationer. Herudover kan it-sikkerhedsfunktionen komme med påbud til alle ansatte og enheder i kommunen om, hvorledes man skal forholde sig i relation til it-sikkerhed. It-sikkerhedsfunktionen varetager endvidere opgaven med at sikkerhedsgodkende anskaffelser af nye it-systemer igennem FISKK-proceduren. Herigennem sikres det fra centralt plan, at nye it-systemer opfylder it-sikkerhedskravene, før de tages i brug. Endelig har it-sikkerhedsfunktionen ansvaret for at håndtere it-sikkerhedshændelser/it-sikkerhedsbrud.

Det følger nærmere af Regulativ for it-sikkerhed i Københavns Kommunes bestemmelser om de interne organisatoriske forhold i relation til ansvaret for it-sikkerhedsforanstaltninger, at det er de enkelte forvaltninger, der har ansvaret for at iværksætte og kontrollere sikkerhedsforanstaltninger i forhold til deres egne it-systemer. Forvaltningerne har ansvaret for egne it-systemer, hvis forvaltningerne selv har anskaffet systemet og udpeget en systemejer inden for egen forvaltning. Forvaltningerne har således ikke ansvaret for fælles it-systemer, hvis der er udpeget en systemejer hos Koncernservice for det pågældende system. Ved brug af eksterne leverandører er systemejer ansvarlig for, at der indgås en databehandleraftale, hvor sikkerhedsforanstaltningerne i forbindelse med leverancen er beskrevet. Databehandleraftalen med eksterne leverandører skal sikre, at kommunen kan overholde sikkerhedsforanstaltningerne. Herudover påhviler det den systemansvarlige forvaltning at påse, at sikkerhedsforanstaltningerne overholdes af databehandleren.

Når en forvaltning har ansvaret for et it-system – og dermed ansvaret for iværksættelse af sikkerhedsforanstaltninger – skal forvaltningens direktion inden for eget område fastlægge it-sikkerhedsniveauet, iværksætte foranstaltninger for at opnå et tilstrækkeligt sikkerhedsniveau samt udpege en systemejer for hvert it-system, som forvaltningen har ansvaret for. Systemejerne for det pågældende it-system har ansvaret for at sikre, at it-systemets funktionalitet og anvendelse understøtter it-sikkerhedskravene samt, at anskaffelsen af it-systemet er godkendt via FISKK-proceduren. Herudover er systemejeren bl.a. ansvarlig for it-systemets funktionalitet, opbygning, anvendelse og sikkerhedsløsning, ansvarlig for at it-systemet lever op til kravene i it-sikkerhedshåndborgen samt ansvarlig for, at it-systemet kan logge behandling af data, når dette er påkrævet. Forvaltningernes autorisationsansvarlige (typisk ledere) varetager opgaver i forbindelse med bestilling af autorisationer og rettigheder til medarbejderne (dvs. bestilling af oprettelser, flytning, ændringer og sletninger af medarbejdere). Bestillingen sker normalt hos Koncernservice. Den autorisationsansvarlige har desuden ansvaret for, at der kun bestilles de rettigheder, som medarbejderen har behov for arbejdsmæssigt. Forvaltningernes ledere skal på alle niveauer sikre, at det er muligt for medarbejderne at efterleve ansvaret for at beskytte kommunens personoplysninger. Den personaleansvarlige leder er ansvarlig for, at medarbejderne er informerede om

deres opgaver og ansvar i forhold til it-sikkerheden. Herudover skal den personaleansvarlige leder bl.a. sikre, at der sker inddragelse af medarbejdernes adgangsrettigheder ved fratrædelse mv.

I Koncernservices udtalelse af 30. juni 2014 præciseres de interne organisatoriske forhold i relation til ansvaret for iværksættelse af sikkerhedsforanstaltninger. Det fremgår bl.a. af Koncernservices svar, at den daglige opgave med varetagelse af tilsynet med, at medarbejderne overholder kommunens sikkerhedsbestemmelser, er delegeret til den personaleansvarlige leder, der ved instruktion og ledelsestilsyn skal sikre, at medarbejdernes adfærd og opgaveløsning ligger inden for de gældende regler og retningslinjer. Af Koncernservices svar fremgår desuden, at kontrollen med de tildelte autorisationer på tværs af kommunen er uddeleget til den personaleansvarlige leder. Ledere træffer beslutning om hyppighed, antallet, områder og kriterier for kontrollerne af egne medarbejders autorisationer og afhænger af de autorisationer, der anvendes i enheden. Det fremgår endvidere af svaret, at kontrollen med medarbejdernes adgang til fortrolige oplysninger på tværs af kommunerne er uddelegeret til den personaleansvarlige leder. Ledere og systemejer træffer beslutninger om hyppighed, antallet, områder og kriterier for kontrollerne af egne medarbejderes adgang til fortrolige personoplysninger afhængig af de rettigheder, der er tildelt i enheden. Endelig fremgår det af Koncernservices svar, at opfølgningsopgaven i forhold til logregistreringer vedrørende håndtering af adgangsforsøg er uddelegeret til den enkelte systemejer, der har vide rammer for at definere passende opfølgning på afviste adgangsforsøg.

Det er min opfattelse, at det på grund af Koncernservices manglende stillingtagen til, hvorvidt sikkerhedsforanstaltningerne er tilstrækkelige og det manglende tilsyn hermed, er uklart, hvorvidt forvaltningerne på tilstrækkelig vis opfylder sikkerhedsforanstaltningerne, og at der er risiko for et uensartet it-sikkerhedsniveau i de forskellige forvaltninger.

Koncernservice har mulighed for at identificere it-sikkerhedsbrud/it-sikkerhedshændelser i forbindelse med adgang til netværk og computere, idet Koncernservice (brugeradminstrationen) automatisk bliver underrettet igennem fælles alarmfunktioner f.eks. ved forkerte adgangskoder. Dette er imidlertid ikke tilfældet for så vidt angår it-sikkerhedsbrud/it-sikkerhedshændelser, der sker i forvaltningernes egne it-systemer (fagsystemerne), idet systemerne ikke har monitoreringsfunktion, hvorved Koncernservice kun opnår kendskab til it-sikkerhedsbrud i disse systemer, såfremt forvaltningerne selv identificerer it-sikkerhedsbrud og foretager indberetning til Koncernservice. Tilstrækkelige og hensigtsmæssige sikkerhedsforanstaltninger er i den forbindelse helt afgørende for forvaltningernes mulighed for at identificere it-sikkerhedsbrud – og i manglen heraf kan der ske misbrug af personoplysninger uden mulighed for, at det opdages.

Det er min opfattelse, at Koncernservice kan medvirke til at sikre et ensartet sikkerhedsniveau i forvaltningerne i relation til sikkerhedsforanstaltningerne dels ved aktivt at tage stilling til, hvorvidt sikkerhedsforanstaltningerne ude i de enkelte forvaltninger er tilstrækkelige og hensigtsmæssige og dels ved at føre løbende tilsyn (stikprøvekontrol) med forvaltningernes kontrol med afviste adgangsforsøg i it-systemerne samt forvaltningernes kontrol med log-opfølgning.

Det er min opfattelse, at der på grund af uddelegeringen af sikkerhedsforanstaltningerne kan være behov for at tydeliggøre ansvarsfordelingen yderligere med målrettet vejledning og retningslinjer. Det fremgår ikke af materialet, som Borgerrådgiveren har modtaget fra Koncernservice, at Koncernservice har udarbejdet konkrete vejledninger/retningslinjer til de personaleansvarlige ledere vedrørende deres ansvarsopgaver i relation til kontrollen med autorisationer, kontrollen med afviste adgangsforsøg samt kontrollen med medarbejdernes adgang til fortrolige oplysninger (antallet af samt hyppighed, områder og kriterier for kontroller mv.). Det fremgår heller ikke, at Koncernservice har udarbejdet konkrete vejledninger/retningslinjer til de personaleansvarlige ledere om systemejernes ansvar for log-opfølgning med henblik på ledelsesmæssigt tilsyn hermed. Jeg vurderer, at konkrete vejledninger og retningslinjer vedrørende disse forhold kan øge fokus på de personaleansvarlige lederes ansvar for sikkerhedsforanstaltningerne og deres ledelsesmæssige tilsyn med systemejernes log-opfølgning.

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 høringsbrev og forvaltningernes høringssvar er indsat som bilag 4 og 5.

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

Undersøgelsen tager udgangspunkt i følgende regler:

Persondataloven
De overordnede regler for datasikkerheden (behandlingssikkerhed) er fastsat i persondatalovens §§ 41 og 42.

I persondatalovens § 41, stk. 1, stk. stk. 3 og stk. 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 data-ansvarlige, 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.
> …"

I persondatalovens § 42, stk. 1-2, lyder det endvidere:

> "…
> **§ 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.
> *Stk. 2.* Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne
> …"

Sikkerhedsbekendtgørelsen
Justitsministeren har i medfør af persondatalovens § 41, stk. 5, udstedt 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 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 § 5, at den dataanvarlige myndighed skal fastsætte nærmere interne sikkerhedsbestemmelser.

Det lyder således i sikkerhedsbekendtgørelsens § 5:

"…
§ 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.
…"

Det følger af sikkerhedsbekendtgørelsens § 8, at der skal træffes forholdsregler imod uvedkommendes adgang til personoplysningerne. Bestemmelsen lyder således:

"…
§ 8. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.
…"

Det følger af sikkerhedsbekendtgørelsens §§ 11 og 12, at der skal ske autorisation og adgangskontrol i relation til behandlingen af personoplysninger. Bestemmelserne lyder således:

"…
§ 11. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.
Stk. 2. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.
Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.
…"

"…
§ 12. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.
…"

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 § 16 (i kapitel 3), at autorisationer, jf. § 11, skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.

Det følger af sikkerhedsbekendtgørelsens § 17 (i kapitel 3), at der skal ske kontrol med, at de autoriserede personer forsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16. Bestemmelsen lyder således:

"…
§ 17. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16.
Stk. 2. Kontrol heraf skal foretages mindst en gang hvert halve år.
…"

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.
> …"

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 indeholder it-sikkerhedsbestemmelserne for Københavns Kommune. Det følger af regulativet, at Koncernservice bl.a. har ansvaret for drift og it-sikkerhed i Københavns Kommune. Regulativ for it-sikkerhed i Københavns Kommunes § 7, stk. 1-3, har følgende ordlyd:

> "…
> **§ 7.** Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen. It-sikkerhedsfunktionen er for tiden placeret i Koncernservice. Koncernservice er bl.a. ansvarlig for fællessystemer, drift og it-sikkerhedsfunktionen.
> *Stk. 2.* Koncernservice udfører udvalgte myndighedsopgaver i forhold til hele kommunen. Endvidere udføres it-opgaver efter bestilling fra den øvrige del af kommunen.
> *Stk.3.* Koncernservice er ansvarlig for at it-sikkerheden på standardydelser fra Koncernservice ydelseskatalog. Ved forvaltningernes bestilling af andre ydelser hos Koncernservice er forvaltningens bestiller (eller den systemejer/projekt-ejer der er ansvarlig for forvaltningens initiativ på området) ansvarlig for sikkerheden i forbindelse med bestilling af ydelser. herunder at der i nødvendigt omfang indgås aftale om de nærmere vilkår og it-sikkerhedskrav i forbindelse med bestilling af ydelsen. Koncernservice kan rådgive med forslag til sikkerhedsforanstaltninger og aftaler med Den Driftsansvarlige.
> …"

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.
…"

Det følger bl.a. af Regulativ for it-sikkerhed i Københavns Kommune § 10, at direktionerne inden for eget forvaltningsområde har ansvaret for fastsættelse af it-sikkerhedsniveauet samt, at direktionerne inden for eget område skal iværksætte tilstrækkelige it-sikkerhedsmæssige foranstaltninger. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 10, stk. 1-2, samt stk. 5:

"…
§ 10. Direktionen har inden for eget forvaltningsområde ansvar for fastlæggelse af it-sikkerhedsniveauet og for gennemførelse af risikovurderinger. It-sikkerhedsniveauet skal fastlægges indenfor de rammer som er opstillet i It-sikkerhedshåndbogen.
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 systemejerne til kommunens it-systemer skal sikre, at systemerne understøtter it-sikkerhedskravene samt sikre, at it-systemerne lever op til kommunens it-sikkerhedsregler samt gældende lovgivning. Herudover skal systemejerne sikre, at der ved brug af eksterne leverandører indgås en databehandleraftale. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 11, stk. 1-7:

"…
§ 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.5. Systemejer er ansvarlig for, at dokumentationen af systemer og processer er ajourført og tilgængelig for relevante medarbejdere. Endvidere har systemejer ansvar for, at der indgås aftale om it-beredskab efter kriterier og retningslinjer fastlagt i it-sikkerhedshåndbogen, og systemejeren skal endvidere bidrage til kommunens it-beredskabsplan.
Stk. 6. Ved brug af eksterne samarbejdspartnere/leverandører er systemejer ansvarlig for, at der indgås en databehandler-/it-sikkerhedsaftale, hvor sikkerhedsforanstaltninger i forbindelse med samarbejdet/leverancerne er beskrevet. Nye aftaler baseres på den standard, der er fastlagt i it-sikkerhedshåndbogen
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 § 14, at ledere på alle niveauer i kommunen skal sikre, at det er muligt for kommunens medarbejdere at beskytte kommunens personoplysninger samt, at den personaleansvarlige leder er ansvarlig for, at medarbejderne er informeret om sine opgaver og ansvar i forhold til it-sikkerheden. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 14, stk. 1:

"…
§ 14. Ledere skal på alle niveauer sikre, at det er muligt for medarbejderne at efterleve deres ansvar for at beskytte kommunens person- og værdioplysninger.
Den personaleansvarlige er ansvarlig for, at medarbejderen er informeret om sine opgaver og ansvar i forhold til it-sikkerheden, inden medarbejderen får adgang til kommunens it-systemer og oplysninger.
…"

Herudover følger det bl.a. af Regulativ for it-sikkerhed i Københavns Kommune § 16, at direktionen inden for eget forvaltningsområde har ansvaret for fastlæggelse af passende it-sikkerhedsniveau, samt hvordan der skal ske underretning i tilfælde af brud eller formodning om brud på it-sikkerheden. Det lyder således i Regulativ for it-sikkerhed i Københavns Kommune § 16, stk. 1-2, samt stk. 12:

"…
§ 16. It-sikkerhed skal afvejes med hensynet til effektiviteten i opgaveløsningen i forvaltningerne.
Stk. 2. Direktionen har inden for eget forvaltningsområde ansvar for at fastlægge et passende itsikkerhedsniveau ud fra en risikovurdering. For så vidt angår Intern Revision og Borgerrådgiverinstitutionen og Brandvæsnet påhviler ansvaret henholdsvis Revisionschefen, Borgerrådgiveren og Beredskabschefen.
[…]
Stk. 12. Styring af it-sikkerhedshændelser: Ved konstatering af brud eller formodning om brud på itsikkerhedsbestemmelserne eller andre væsentlige it-sikkerhedshændelser,
skal den, der konstaterer disse sikre, at it-sikkerhedsfunktionen underrettes herom. Hvis itsikkerhedshændelsen har relation til et bestemt system, skal systemejeren også underrettes. Systemejer skal endvidere i relevant omfang orientere den lokale ledelse i forvaltningen.
[…]
…"

Det følger af Regulativ for it-sikkerhed i Københavns Kommune §§ 17-18, at de enkelte direktioner, Revisionschefen og Borgerrådgiveren inden for eget område skal sikre, at specifik lovgivning af betydning for it-sikkerheden overholdes, og at det daglige ansvar for overholdelse af persona-

taloven i forbindelse med behandling af personoplysninger påhviler disse. Det lyder således i §§ 17-18:

"…
§17. De respektive direktioner henholdsvis Revisionschefen og Borgerrådgiveren 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 henholdsvis Revisionschefen og Borgerrådgiveren…"

Uddybende sikkerhedsregler for Københavns Kommune

Det fremgår af Koncernservices seneste uddybende sikkerhedsregler af 15. januar 2015 for Københavns Kommune, 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 og overvågning:

"…
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 DOKUMENTATIONSGRUNDLAGET (DATA)

Borgerrådgiveren iværksatte nærværende egen drift-undersøgelse ved brev af 13. februar 2014 til Koncernservice. Til brug for undersøgelsen modtog Borgerrådgiveren udtalelse af 30. juni 2014 fra Koncernservice samt dokumentation i form af procedurer, vejledninger, retningslinjer mv. i relation til behandling af personoplysninger. Herudover har Borgerrådgiveren fra Koncernservice modtaget eksterne revisionsrapporter for 2012 samt for 2013 vedrørende revision af generelle it-kontroller hos Københavns Kommune. Herudover har Borgerrådgiveren fra Koncernservice modtaget ekstern revisionsrapport for 2014 vedrørende modenhedsvurdering af informationssikkerhed hos Københavns Kommune samt Koncernservices opfølgende initiativer herpå.

Endelig har Borgerrådgiveren modtaget Koncernservices svar af 20. januar 2015 på Borgerrådgiverens skriftlige opfølgende spørgsmål.

BILAG 4 – BORGERRÅDGIVERENS HØRINGSBREV

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Til Koncernservice i Økonomiforvaltningen

13-02-2014

Sagsnr.
2012-167267

Sendt d.d. pr. e-mail

Dokumentnr.
2012-167267-1

Vedrørende Borgerrådgiverens generelle egen driftundersøgelse om sikring af borgernes personoplysninger

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.
> …"

På mødet i Borgerrådgiverudvalget den 26. oktober 2012 drøftede Borgerrådgiveren og udvalget plan for udmøntningen af egen driftskompetencen i 2013 for så vidt angår generelle undersøgelser og inspektioner.

Af planen fremgår, at Borgerrådgiveren i 2013 indleder en skriftlig undersøgelse vedrørende sikring af borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang dertil.

Undersøgelsen er rettet mod Koncernservice, idet det følger af regulativ for it-sikkerhed i Københavns Kommune, at Koncernservice bl.a. er ansvarlig for drift og it-sikkerhedsfunktionen i Københavns Kommune.

Om undersøgelsens formål og tema

Borgerrådgiveren

Vester Voldgade 2A
1552 København V

Telefon
33 66 14 00

Telefax
3366 1390

E-mail
borgerraadgiveren@kk.dk

EAN nummer
5798009800053

www.borgerraadgiver.kk.dk

Formålet med undersøgelsen er at belyse, hvorledes Koncernservice sikrer borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang til dem.

Undersøgelsen vil have fokus på Koncernservices procedurer, rutiner mv. (f.eks. logning, sikkerhedssystemer og intern kontrol) i relation til sikring af borgernes personoplysninger.

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

Regelgrundlag

Persondataloven

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

Persondatalovens § 41, stk. 1, stk. 2 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 dataanvarlige myndighed skal fastsætte nærmere interne sikkerhedsbestemmelser.

Det lyder således i sikkerhedsbekendtgørelsens § 5:

"…
§ 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.
…"

Det følger af sikkerhedsbekendtgørelsens § 8, at der skal træffes forholdsregler imod uvedkommendes adgang til personoplysningerne. Bestemmelsen lyder således:

"…
§ 8. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.
…"

Det følger af sikkerhedsbekendtgørelsens §§ 11 og 12, at der skal ske autorisation og adgangskontrol i relation til behandlingen af personoplysninger. Bestemmelserne lyder således:

"…

> **§ 11.** Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.
> *Stk. 2.* Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.
> *Stk. 3.* Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.
> …"
>
> "…
> **§ 12.** Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.
> …"

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.
> ..."

Regulativ for it-sikkerhed i Københavns Kommune

Københavns Kommune har i medfør af sikkerhedsbekendtgørelsens § 5 udstedt regulativ for it-sikkerhed i Københavns Kommune (herefter regulativet).

Regulativet indeholder it-sikkerhedsbestemmelserne for Københavns Kommune.

Det følger af regulativet, at Koncernservice bl.a. har ansvaret for drift og it-sikkerhed i Københavns Kommune.

Regulativets § 7, stk. 1, har følgende ordlyd:

> "…
> **§ 7.** Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen. It-sikkerhedsfunktionen er for tiden placeret i Koncernservice. Koncernservice er bl.a. ansvarlig for fællessystemer, drift og It-sikkerhedsfunktionen.
> …"

Regulativets § 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.
…"

Anmodning om udtalelse og besvarelse af spørgsmål

Jeg beder om en udtalelse fra Koncernservice med en generel beskrivelse af, hvilke foranstaltninger Koncernservice er ansvarlige for – og hvilke foranstaltninger Koncernservice udfører – i henseende til sikring af borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang dertil.

Jeg beder desuden om, at Koncernservice i udtalelsen beskriver, hvilke foranstaltninger, forvaltningerne måtte være ansvarlige for i henseende til ovennævnte sikring af personoplysninger, herunder eventuelle snitflader og/eller overlap mellem Koncernservice og forvaltningerne i relation til ansvaret for sikring af borgernes personoplysninger.

Jeg beder endvidere om, at Koncernservice svarer på følgende spørgsmål:

- Hvorledes fører Koncernservice i det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser?

- Hvorledes sikrer Koncernservice, at medarbejderne i Københavns Kommune overholder it-sikkerhedsbestemmelserne?

- Hvilken kontrol foretager Koncernservice af tildelte autorisationer? Hvor hyppigt foretages kontrol? Hvor mange autorisationer kontrolleres? På hvilke forvaltningsområder og sagsområder sker der kontrol? Og på baggrund af hvilke kriterier bliver autorisationer udvalgt til kontrol?

- Hvilken kontrol foretager Koncernservice af de medarbejdere, der har adgang til fortrolige personoplysninger? Hvor hyppigt foretages kontrol? På hvilke sagsområder og forvaltningsområder sker der kontrol? Hvor mange medarbejdere bliver kontrolleret? Og på baggrund af hvilke kriterier sker der udvælgelse til kontrol?

- Hvorledes sikrer Koncernservice, at brud på it-sikkerheden (jf.*) kan identificeres såvel af Koncernservice som i forvaltningerne?

- Hvorledes følger Koncernservice op på eventuelle brud på it-sikkerheden (jf.*)?

- Hvordan registrer og statistikfører Koncernservice eventuelle brud på it-sikkerheden (jf.*)?

- Hvorledes følger Koncernservice op på log-registreringer om afviste adgangsforsøg til kommunens it-systemer, 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).

Anmodning om dokumentation

Jeg beder om kopi af Koncernservices procedurer, forretningsgange, retningslinjer, rutiner mv., herunder eventuelle forretningsgange mv. vedrørende snitfladen og/eller overlap mellem forvaltningerne og Koncernservice, i relation til ovennævnte sikring af borgernes personoplysninger.

Jeg beder så vidt muligt om at modtage Koncernservices udtalelse, svar på spørgsmål og den nævnte dokumentation inden 8 uger fra dags dato. Hvis dette ikke kan lade sig ske, beder jeg om underretning om, hvornår Koncernservice forventer at kunne svare.

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

Jeg forbeholder mig ret til at stille yderligere spørgsmål til Koncernservice, herunder ret til at anmode om yderligere dokumentation, såfremt dette måtte være relevant for nærværende undersøgelse.

Jeg vil via Borgerrådgiverens hjemmeside www.borgerrådgiveren.kk.dk orientere offentligheden om, at jeg har iværksat denne undersøgelse.

Eventuelle spørgsmål vedrørende undersøgelsen kan rettes til jurist Daniel Soelberg Bach, som kan kontaktes på telefon 33 66 14 00 eller e-mail za6n@okf.kk.dk.

Med venlig hilsen

Johan Busse
Borgerrådgiver

/Daniel Soelberg Bach
Jurist

BILAG 5 – FORVALTNINGENS HØRINGSSVAR

KØBENHAVNS KOMMUNE
Koncernservice
Digitalisering

30-06-2014

Sagsnr.
2014-0110609

Dokumentnr.
2014-0110609-1

Borgerrådgiveren
Vester Voldgade 2A
1552 København V

Besvarelse af Borgerrådgiverens henvendelse

Borgerrådgiveren har med mail til Koncernservice af 13. februar 2014 (Dok.nr. 2012-167267-1) iværksat en egen driftsundersøgelse om sikring af borgernes personoplysninger.

Undersøgelsen er rettet mod Koncernservice som bl.a. er ansvarlig for drift og IT-sikkerhedsfunktionen i Københavns kommune.

A. Borgerrådgiveren beder om en udtalelse fra Koncernservice med en generel beskrivelse af, hvilke foranstaltninger Koncernservice er ansvarlige for – og hvilke foranstaltninger Koncernservice udfører – i henseende til sikring af borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang dertil.
B. Borgerrådgiveren beder desuden om, at Koncernservice i udtalelsen beskriver, hvilke foranstaltninger, forvaltningerne måtte være ansvarlige for i henseende til ovennævnte sikring af personoplysninger, herunder eventuelle snitflader og/eller overlap mellem Koncernservice og forvaltningerne i relation til ansvaret for sikring af borgernes personoplysninger.

Borgerrådgiveren beder herudover om, at Koncernservice svarer på følgende spørgsmål:

1. Hvorledes fører Koncernservice i det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser?

2. Hvorledes sikrer Koncernservice, at medarbejderne i Københavns Kommune overholder it-sikkerhedsbestemmelserne?

3. Hvilken kontrol foretager Koncernservice af tildelte autorisationer? Hvor hyppigt foretages kontrol? Hvor mange autorisationer kontrolleres? På hvilke forvaltningsområder og sagsområder sker der kontrol? Og på baggrund af hvilke kriterier bliver autorisationer udvalgt til kontrol?

4. Hvilken kontrol foretager Koncernservice af de medarbejdere, der har adgang til fortrolige personoplysninger? Hvor hyppigt foretages kontrol? På hvilke sagsområder og forvaltningsområder sker der

Digitalisering

Borups Allé 177
2400 København NV

Telefon
2673 1102

Mobil
2673 1102

EAN nummer
5798009809025

kontrol? Hvor mange medarbejdere bliver kontrolleret? Og på baggrund af hvilke kriterier sker der udvælgelse til kontrol?

5. Hvorledes sikrer Koncernservice, at brud på it-sikkerheden (jf.*) kan identificeres såvel af Koncernservice som i forvaltningerne?

6. Hvorledes følger Koncernservice op på eventuelle brud på it-sikkerheden (jf.*)?

7. Hvordan registrer og statistikfører Koncernservice eventuelle brud på it-sikkerheden (jf.*)?

8. Hvorledes følger Koncernservice op på log-registreringer om afviste adgangsforsøg til kommunens it-systemer, 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).

Svar på A:

Generel beskrivelse af hvilke foranstaltninger Koncernservice er ansvarlig for og udfører.

Københavns kommune har fastsat nærmere interne bestemmelser om sikkerhedsforanstaltninger til beskyttelse af personoplysninger i kommunens IT-sikkerhedsregler, her beskrives tillige de organisatoriske forhold, fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger samt kontrol med autorisationer.

IT-sikkerhedsreglerne består af tre elementer, der under ét kaldes IT-sikkerhedshåndbogen:

- IT-sikkerhedspolitikken, der fastlægger mål og rammer for IT-sikkerhed
- IT-sikkerhedsregulativet, der beskriver organisering af arbejdet samt rolle- og ansvarsfordeling
- IT-sikkerhedsreglerne, der uddyber og fortolker sikkerhedsregulativet gennem konkrete anvisninger.

IT-sikkerhedsreglerne er baseret på ISO 27001 - 2 (international standard), som er anbefalet af staten.
IT-sikkerhedshåndbogen er publiceret på kommunens Intranet.

IT-sikkerhedsorganisation i Koncernservice

Borgerrepræsentationen vedtager kommunens IT-sikkerhedspolitik og IT-sikkerhedsregulativ.

Overborgmesteren og de enkelte borgmestre har ansvaret for IT-sikkerhedsarbejdet inden for de enkelte forvaltningsområder.

Myndighedsopgaverne på IT-sikkerhedsområdet varetages i Koncernservice af IT-sikkerhedsfunktionen, Driftorganisationen og Brugeradministrationen. Arbejdsgrundlaget for myndighedsudøvelsen er IT-sikkerhedsregulativet jf.ovenfor.

IT-sikkerhedsfunktionen er placeret i enheden Digitalisering. Funktionen fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser og koordinerer kommunens it-sikkerhedsarbejde.

Eksempler på IT-sikkerhedsfunktionens myndighedsopgaver:

- Rådgiver om IT-sikkerhedsmæssige forhold. Det sker ved at udarbejde og vedligeholde forskrifter og vejledninger og derudover løbende ved konkrete henvendelser.
- Godkender sikkerhedsløsningen ved anskaffelse af nye systemer. Det sker ved at IT-sikkerhedsfunktionen deltager i It-anskaffelsesprocessen og derved får forelagt alle nye it-systemer til godkendelse.
- Sikrer kontrol af medarbejdernes adgangsrettigheder og autorisationer. Det sker konkret efter henvendelse fra systemejere eller forvaltninger. Det daglige arbejde udføres i Brugeradministrationen og af den enkelte systemejer.
- Udarbejder procedurer som sikrer tværorganisatorisk styring af it-beredskabet. Det sker ved at der er udarbejdet procedurer både for KS og for forvaltningernes It-beredskab og ved at bistå forvaltningerne med at udpege de mest kritiske systemer og sikre udarbejdelse af beredskabsplaner for evt. nedbrud.
- Håndterer IT-sikkerhedshændelser og IT-sikkerhedsbrud. Det sker konkret efter henvendelse eller hvis It-sikkerhedsfunktionen i øvrigt bliver opmærksom på en hændelse.
- Ansvar for fælles informations- og uddannelsesmateriale, herunder opbygning og opdatering af kommunens IT-sikkerhedshåndbog og supplerende vejledninger. Det sker ved at opbygge og vedligeholde et omfattende materiale på kknet, der frit står til alle forvaltningers disposition og ved at udarbejde og distribuere løbende awareness-kampagner.

Driftsorganisationen er placeret i enhederne IT Infrastruktur, IT Rådgivning og Udvikling, IT Support og Logistik samt Serviceindgang IT.

Eksempler på driftsorganisationens myndighedsopgaver:

- Ansvaret for sikkerheden på kommunens IT-platforme.
- Det IT-sikkerhedsmæssige ansvar for opbygning og anvendelse af it-driftsmiljø og kommunikationsforbindelser samt for de fysiske sikringsforanstaltninger i forhold til kommunens netværk, netværksudstyr og servere m.v.
- Udarbejder it-sikkerhedsforskrifter eller retningslinjer for it-installationer/driftsmiljø og de benyttede netværk.
- IT-infrastruktur administrerer Koncernservice netværk, servere, datalagring, back-up og telefoni så opsætning og anvendelse overholder sikkerhedsbestemmelserne.

Brugeradministrationen er placeret i enheden Serviceindgang. Brugeradministrationen har det IT-sikkerhedsmæssige ansvar for administrationen af kommunens brugeradgange.

Eksempler på Brugeradministrationens myndighedsopgaver:

- Ansvar for aftaler om og udførelse af brugeradministration af de systemer kommunens medarbejdere benytter.
- Sikre at der findes retningslinjer for adgangsstyringen af de enkelte systemer (dvs. hvilke medarbejdergrupper skal benytte systemet, hvilke rettigheder herunder dataadgang og funktioner må tildeles).
- Ansvar for den løbende opbygning og vedligeholdelse af medarbejdertyper.
- Sikre at der i forbindelse med brugeradministrationen altid er et gyldigt revisionsspor.
- Support af autorisationsansvarlige .
- Tildeling af rettighedere i it-systemer.

KS Direktion udpeger inden for eget område systemejere for IT-systemer, som KS har ansvaret for.

- Systemejerne sikrer, at systemets funktionalitet og anvendelse løbende tilpasses og bedst muligt understøtter It-sikkerhedskravene samt forretningens og brugernes behov.

Det er således systemejer, som i hele systemets livscyklus sikrer at systemer, som indeholder personoplysninger understøtter reglerne i Kommunens IT sikkerhedshåndbog.

Alle ledere i KS skal sikre at det er muligt for medarbejdere at efterleve ansvaret for at beskytte Kommunens personoplysninger herunder:

- Sikre at medarbejdere er bekendt med Kommunens it-sikkerhedsregler.
- Tildele og kontrollere at medarbejdere til en hver tid kun har autorisationer til systemer, som er relevante for udførelse af deres arbejde.

Koncernservice har etableret et IT-kriseberedskab med klart definerede roller og ansvarsområder, som skal sikre effektiv håndtering af kritiske it-nedbrud.

Svar på B:

Beskrivelse af hvilke foranstaltninger forvaltningerne er ansvarlige for i henseende til sikring af personoplysninger, herunder eventuelle snitflader og/eller overlap mellem Koncernservice og forvaltningerne i relation til ansvaret for sikring af borgernes personoplysninger.

Forvaltningernes ansvar er beskrevet i Københavns kommunes It-sikkerhedshåndbog (IT-sikkerhedsregulativet) jf. ovenfor.

Det er Overborgmesteren og de enkelte borgmestre som har ansvaret for It-sikkerhedsarbejdet inden for den enkelte forvaltning.

Forvaltnings direktion har ansvaret for fastlæggelse af It-sikkerhedsniveauet og for gennemførelse af risikovurderinger inden for eget forvaltningsområde. Forvaltningens direktion skal udpege systemejere og sikre at det er muligt for medarbejdere at efterleve ansvaret for at beskytte personoplysninger jf. beskrivelsen af KS ovenfor.

Direktionen for Børne- og ungdomsforvaltningen har jf. it-sikkerhedsregulativet udpeget en driftsansvarlig for forvaltningens eget pædagogiske netværk, netværksudstyr og servere m.v. I forbindelse med Børne- og Ungdomsforvaltningens snitflader/deling af it-ressourcer med Koncernservice og kommunens administrative net er det den driftsansvarlige i Koncernservice der har ansvaret. Ligeledes har ledelsen for Brandvæsenet udpeget en Driftsansvarlig for Brandvæsnets eget netværk, netværksudstyr og servere m.v.

Koncernservice svar på Borgerrådgiverens konkrete spørgsmål.

Generelt svar i forhold til de konkrete spørgsmål:

Kommunens eksterne revision gennemfører årlig revision af generelle it-kontroller. Der er i meget høj grad tale om revision af de samme forhold som er genstand for Borgerrådgiverens undersøgelse og som besvares nedenfor. Der er i de seneste år sket en reduktion i antallet af revisionsanbefalinger og en reduktion i disses kritikalitet. Seneste revisionsrapporter vedlægges som bilag jf. bilagslisten sidst i denne besvarelse.

Datatilsynet gennemfører stikprøvevis inspektion af Københavns Kommunes overholdelse af persondataloven. I november 2013 inspicerede Datatilsynet kommunens håndtering af persondata i forhold til TV-overvågning, og i maj 2014 har Datatilsynet været på inspektion i forhold til behandling af persondata i et konkret system i Socialforvaltningen. Datatilsynets udtalelse i forbindelse inspektionen i november 2013 vedlægges som bilag jf. bilagslisten sidst i denne besvarelse. Koncernservice har endnu ikke modtaget tilbagemelding fra Datatilsynet i forbindelse med inspektionen i maj 2014.

Koncernservice har i juni 2014 anmodet konsulentfirmaet PWC om at foretage en analyse af sikkerhedsniveauet i Københavns Kommune. Analysen skal vurdere om kommunen har tilstrækkelige procedurer og kontroller på it-området samt om disse er tilstrækkeligt indarbejdede i den daglige praksis. På baggrund af analysen skal PWC desuden give anbefalinger til hvilke indsatser Københavns Kommune fremadrettet kan iværksætte for at styrke it-sikkerheden.

PWCs rapport med vurdering af status og forslag til evt. ændringer vil foreligge i august 2014 og Koncernservice vil efterfølgende fremlægge forslag vedr. opfølgende initiativer.

Koncernservice vil fremsende PWCs rapport og forslag til opfølgende initiativer til Borgerrådgiveren, når disse foreligger.

1 Hvorledes fører Koncernservice i det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser?

Koncernservice daglige tilsyn med overholdelsen af it-sikkerhedsbestemmelserne håndteres på flere niveauer. Nye it-systemer vurderes og it-sikkerhedsgodkendes i en proces der er fælles for alle forvaltninger. It-systemerne håndteres i et register over it-systemer i Københavns Kommune (FISKK).

Den daglige opgave med at varetage tilsynet med at medarbejderne overholder kommunens it-sikkerhedsbestemmelser er delegeret til den

personaleansvarlige leder, der ved instruktion og ledelsestilsyn skal sikre at medarbejdernes adfærd og opgaveløsning ligger indenfor de gældende regler og retningslinjer.

Enhedscheferne i Koncernservices driftsenheder varetager ledelsestilsynet indenfor eget driftsområde.

Kommunens eksterne revision gennemfører årligt en revision af kommunens generelle It-kontroller i samarbejde med Koncernservice.

2 Hvorledes sikrer Koncernservice, at medarbejderne i Københavns Kommune overholder it-sikkerhedsbestemmelserne?

Koncernservice sikrer at medarbejderne i Københavns Kommune overholder it-sikkerhedsbestemmelserne ved flere tiltag:

- Alle medarbejdere og ledere gøres ved ansættelsen bekendt med tavshedspligtsreglerne efter straffeloven og forvaltningsloven.
- Alle it-brugere modtager ved oprettelse i kommunens it-systemer et instruktionsbrev om retningslinjerne for anvendelsen af kommunens it-systemer og kommunens data der kan indeholde personfølsomme oplysninger.
- Alle medarbejdere henvises løbende til Københavns Kommunes It-sikkerhedshåndbog hvor materiale om it-sikkerhed er samlet og ligger tilgængelig for alle it-brugere på kommunens administrative it-netværk. It-sikkerhedshåndbogen indeholder kommunens It-sikkerhedspolitik, It-sikkerhedsregulativet, uddybende vejledninger, pjecer og andre skriftlige informationer om It-sikkerhedsbestemmelser.
- Koncernservice kommunikerer løbende via kommunens intranet til medarbejdere og ledere, både via nyhedsbreve og på egne sider om it-sikkerhed.
- Direktionen og It-sikkerhedsfunktionen iværksætter awareness kampagner indenfor it-sikkerhedsområdet på enhedschefernes fællesmøde for at sikre et bredt kendskab i hele Koncernservice og tilbyder løbende awareness-kampagner til alle forvaltninger.

3 Hvilken kontrol foretager Koncernservice af tildelte autorisationer? Hvor hyppigt foretages kontrol? Hvor mange autorisationer kontrolleres? På hvilke forvaltningsområder og sagsområder sker der kontrol? Og på baggrund af hvilke kriterier bliver autorisationer udvalgt til kontrol?

Kontrollen af de tildelte autorisationer er på tværs af kommunen uddelegeret til den personaleansvarlige leder. Ledere og udpegede

autorisationsansvarlige kan bestille oprettelse, ændringer og nedlæggelse af brugernes autorisationer via Brugeradministrationens selvbetjeningsløsning. I selvbetjeningsløsningen kan lederen søge information om medarbejdernes autorisationer. Beslutningen om hyppighed, antallet, områder og kriterier for kontrollerne af egne medarbejderes autorisationer træffes af ansvarlig leder og afhænger af de autorisationer der anvendes i enheden.

4 Hvilken kontrol foretager Koncernservice af de medarbejdere, der har adgang til fortrolige personoplysninger? Hvor hyppigt foretages kontrol? På hvilke sagsområder og forvaltningsområder sker der kontrol? Hvor mange medarbejdere bliver kontrolleret? Og på baggrund af hvilke kriterier sker der udvælgelse til kontrol?

Kontrollen med medarbejdernes adgang til fortrolige personoplysninger, er på tværs af kommunen uddelegeret til den personaleansvarlige leder. Ledere og systemejer træffer beslutninger om hyppighed, antallet, områder og kriterier for kontrollerne af egne medarbejderes adgang til fortrolige personoplysninger afhængig af de rettigheder der er tildelt i enheden.

5 ***Hvorledes sikrer Koncernservice, at brud på it-sikkerheden kan identificeres såvel af Koncernservice som i forvaltningerne?***

Koncernservice har udarbejdet vejledninger og herunder en kort pjece om "Sikker adfærd på nettet", så det er tydeligt for medarbejdere hvilken adfærd og behandling af data der er acceptabel. It-sikkerhedsfunktion har desuden præsenteret It-sikkerhedsbestemmelserne for medarbejderne i Koncernservice serviceindgange så disse er i stand til at identificere medarbejderes brud på it-sikkerheden. På KKintra ligger en kort indmeldelsesformular til indmeldelse af it-sikkerhedshændelser til efterforskning.

6 ***Hvorledes følger Koncernservice op på eventuelle brud på it-sikkerheden?***

Alle it-sikkerhedshændelser, som It-sikkerhedsfunktionen observerer eller modtager som indberetninger, følges op af en intern redegørelse og dokumentation af forløbet. Redegørelsen udarbejdes som hovedregel i samarbejde med impliceret leder og personalejurister fra enheden for Personalejura og Forhandling i Koncernservice. Afhængig af redegørelsens observationer kontaktes medarbejder, ledere og andre implicerede så fremtidige hændelser eller brud på it-sikkerheden kan undgås. I det tilfælde der er tale om brud på forvaltnings- eller straffelovens regler kan dokumentation overdrages til politiet og videre efterforskning. Evt. beslutning om sigtelse og

personale juridiske foranstaltninger træffes af ansvarlig leder og personale jurist hos Koncernservice,

7 Hvordan registrer og statistikfører Koncernservice eventuelle brud på it-sikkerheden?
It-sikkerhedshændelser der observeres eller modtages som indberetninger i It-sikkerhedsfunktionen registreres i eDoc og bearbejdes i en manuel statistisk opgørelse.

8 ***Hvorledes følger Koncernservice op på log-registreringer om afviste adgangsforsøg til kommunens it-systemer, hvor der behandles fortrolige eller følsomme personoplysninger?***

I anskaffelsesprocessen for it-systemer vejledes systemejere i bl.a. de logningskrav, der skal implementeres for et system ud fra de data, der behandles i systemet. Opfølgningsopgaven vedr. håndtering af adgangsforsøg er uddelegeret til den enkelte systemejer, der har vide rammer for at definere passende opfølgning på afviste adgangsforsøg.

Vedlagt relevant dokumentation af procedurer, vejledninger m.v., sammen med undersøgelse fra ekstern revision og svar på henvendelse fra Datatilsynet.

Oversigt over vedhæftet materiale

IT-sikkerhedspolitik
IT-sikkerhedsregulativ
Uddybende IT-sikkerhedsregler
Ekstern revision – IT-kontroller 2012 (Fortrolig), fremsendes særskilt
Ekstern revision – IT-kontroller 2013 (Fortrolig), fremsendes særskilt
Datatilsynet inspektion vedr. tv-overvågning
e-mail og internet politik
Guide til ledere om IT-sikkerhed
Sikker adfærd på nettet – vejledning til medarbejdere
Awareness kampagne 2014 – Følgebrev til forvaltningerne
IT-sikkerhedshændelser – Rapportering og håndtering
Anmeldelser til Datatilsynet – vejledning
Autorisationer – den daglige leders ansvar
Autorisationsansvarlig - ansvar og opgaver
Databehandleraftale
Identifikation ved tildeling af adgangskoder
Logningskrav til dokumenter og 30 dages reglen
Logning udvidet vejledning (under revision)
Mobile enheder – sådan skal du sikre dem
Mobile enheder teknisk sikring
Opbevaring og fysisk transport af ind- og uddata
Passwordopsætning i IT-systemer
Sikkerhedskrav til systemer – vejledning til systemejer

Tavshedspligtserklæringer – vejledning
Tavshedspligtserklæring virksomhed ekstern samarbejdspart
Tavshedspligtserklæring ekstern konsulent vikar
TV- og videoovervågning – retningslinjer
Udlevering af IT-sikkerhedsrapporter
Undgå skjulte oplysninger i digitalt materiale
Infobrev til nye medarbejdere
Autorisationsvejledning for Brugeradministrationen
Krav til implementering af nyt IT-system i Brugeradminstrationen
Rettighedsskema for Brugeradministrtionen
Retningslinjer i Brugeradministrationen for tildeling af adgangskoder

BILAG 6 - OPFØLGENDE SPØRGSMÅL OG SVAR

Borgerrådgiveren stillede ved e-mail af 7. januar 2015 opfølgende spørgsmål til Koncernservice. I e-mailen fremgår bl.a. følgende:

"…
For det første beder Borgerrådgiveren om Koncernservices estimat på antallet af it-systemer uden for Koncernservices område (dvs. it-systemer som KS ikke har ansvaret for og hvor KS ikke har udpeget en systemejer), hvor der bliver behandlet følsomme persondataoplysninger (dvs. behandling af personoplysninger som er omfattet af reglerne i kapitel 3 i bekendtgørelse nr. 528 af 15. juni 2000). Borgerrådgiveren beder også om Koncernservices estimat på it-systemernes antalsmæssige fordeling ift. de forskellige forvaltninger.

Det fremgår af Koncernservices besvarelse af 30. juni 2014, at Datatilsynet har gennemført inspektion ift. behandling af persondata i et konkret it-system i Socialforvaltningen. Hvis Koncernservice har modtaget Datatilsynets tilbagemelding herpå, beder Borgerrådgiveren om en kopi heraf. Hvis Koncernservice endnu ikke har modtaget tilbagemeldingen, beder Borgerrådgiveren om en kopi, når Koncernservice modtager tilbagemeldingen fra tilsynet.

Det fremgår af indstilling af 10. oktober 2014, at Digitalisering bl.a. indstiller, at direktionen tiltræder handlingsplan for styrkelse af it-sikkerheden. Borgerrådgiveren beder om en status på, hvorvidt indstillingen blev tiltrådt?

Det fremgår af indstillingens side 5 midtfor, at Koncernservice fremlægger en revideret rollebeskrivelse på et kommende møde i Digitaliseringschefkredsen. Borgerrådgiveren beder om en kopi af denne beskrivelse, såfremt den er udarbejdet og fremlagt. Herudover beder Borgerrådgiveren om en status på, hvorvidt Koncernservice på nuværende tidspunkt har fundet det nødvendigt at foreslå tilpasninger af It-sikkerhedsregulativet?

I bilaget 1 til Digitaliserings indstilling er oplistet forslag til 21 konkrete initiativer. Borgerrådgiveren skal venligst bede om en status på følgende punkter: 1.1., 1.5., 1.7., 2.1., 5.2., samt 5.3.

…"

Koncernservice svarede ved e-mail af 20. januar 2015 på Borgerrådgiverens opfølgende spørgsmål. Det fremgår bl.a. følgende af svaret:

"…
Koncernservice giver her et estimat på antallet af systemer indeholdende fortrolige/følsomme personoplysninger, som ligger uden for KS ansvarsområde og fordelingen af disse på forvaltninger.
Estimatet bygger på udtræk fra FISKK. FISKK systemoversigten indeholder kommunens systemer og vedligeholdes af forvaltningerne.

Antal uden for KS ansvarsområde: 44
BIF: 13
BUF: 6
KFF: 7
SOF: 9
SUF: 7
TMF: 0
ØKF: 2

Vedr. Datatilsynets inspektion af It-system i Socialforvaltningen.
Nej Koncernservice har endnu ikke modtaget tilbagemeldingen. Vi fremsender en kopi til Borgerrådgiveren så snart vi har modtaget tilbagemeldingen fra Datatilsynet.

Vedr. handlingsplan for styrkelse af it-sikkerheden.
Ja – Direktionen tiltrådte handlingsplanen d. 20 oktober og den er umiddelbart iværksat. Handlingsplanen har dannet grundlag for orientering af økonomiudvalget d. 12 december og der vil blive fremlagt forslag til økonomiudvalget i løbet af foråret 2015.

Vedr. tilpasning af sikkerhedsregulativet og revideret rollebeskrivelse (ansvar og organisering).
Koncernservice har ikke p.t. fundet det nødvendigt at foreslå ændringer af It-sikkerhedsregulativet.
Koncernservice har ikke fremlagt en revideret rollebeskrivelse.
På digitaliseringschefkredsens mødet d. 19 november blev samarbejde og snitflader mellem Koncernservice og forvaltningerne drøftet. Diskussionen mundede ud i en aftale om nedsættelse af en arbejdsgruppe. Koncernservice har udarbejdet forslag til kommissorium for arbejdsgruppen, se vedhæftede "kommissorium"

Status på initiativ punkter.
1.1 Løsningen "Konsulentadgang" i Basis er tæt på at være færdigudviklet. Herefter mangler test inden endelig implementering der forventes 1. kvartal 2015.
1.5 Oprydning i medarbejdertyper (faste entydige roller) – status: afventer
1.7 Business case IAM/IDM-løsning: et udkast er under udarbejdelse. Koncernservice foreslår udarbejdelse af en foranalyse hvor endelig business case skal indgå.
Vil indgå i indstilling til Økonomiudvalget foråret 2015
2.1 SIEM løsning forventes at indgå i indstilling til Økonomiudvalget foråret 2015
5.2 Oplæg forventes klar 1. kvartal 2015
5.3 Oplæg til model forventes klar 1. kvartal 2015
…"

BILAG 7 – TELEFONINTERVIEWS

Borgerrådgiveren udførte den 15. januar 2015 et telefoninterview med Koncernservice for afklaring af en række forhold. Referatet fra telefoninterviewet gengives i det følgende (svar er angivet i kursiv):

"…
Emne: KK's interne organisatoriske forhold – som følger af regulativet for it-sikkerhed i KK- i henseende til ansvaret for sikkerhedsforanstaltninger (i relation til opfyldelse af lovkravene i sikkerhedsbekendtgørelsens § 17 (kontrol med autorisation – mindst én gang hvert halve år) § 18 (løbende opfølgning ift. afviste adgangsforsøg) samt § 19 (logning) samt overholdelse af KK interne understøttende regler (uddybende it-sikkerhedsregler om opfølgning på logning samt fejllogs).

Vedrørende formuleringerne i Koncernservices udtalelse på side 4, punkt 11: "KS udpeger *inden for eget område* systemejere for IT-systemer, som KS har ansvaret for", udtalelsens s. 7, nederst: "kontrollen af de tildelte autorisationer er *på tværs af kommunen* uddelegeret til den personaleansvarlige leder".

Spørgsmål 1
Er det korrekt forstået, at ansvaret for de ovenfor nævnte sikkerhedsforanstaltninger overordnet afgrænses af, hvorvidt it-systemer hører *inden for* eller *uden for* en forvaltnings område? Og i givet fald hvad er bestemmende/udslagsgivende for, om et it-system er inden for en forvaltnings eget område?

Svar:

Ja.

Udslagsgivende er hvilken forvaltning, der har ansvaret, hvilket er tilfældet, hvis forvaltningen har bestilt og betalt for systemet og udpeget systemejer inden for egen forvaltning.

Det er KS, der styrer rettighederne til systemerne.

Det er cheferne ude i enheder i hver enkelt forvaltning, som giver og tjekker om autorisation er korrekt.

Spørgsmål 2
Er det korrekt forstået, at de nærmere opgaver i relation til ansvaret for sikkerhedsforanstaltningerne inden for hver enkelt forvaltnings område er fordelt på direktionen inden for den pågældende forvaltning, systemejeren som direktionen har udpeget, samt personalelederen inden for den pågældende forvaltning samt medarbejderne i den pågældende forvaltning?

Svar:

Ja.

Spørgsmål 3
Når et it-system hører inden for Koncernservices område, er det i så fald direktionen i Koncernservice eller direktionen i ØKF, som skal opfylde de givne sikkerhedsforanstaltninger som er pålagt direktionerne i henhold regulativ for it-sikkerhed i KK.

Svar:

Direktionen i KS

Emne: uddybende it-sikkerhedsregler – periodisk review

Spørgsmål 4
Det følger af uddybende sikkerhedsregler under overskriften periodisk review, at it-sikkerhedsfunktionen sikrer, at der foretages stikprøvekontrol af de tildelte autorisationer. Hvorledes sikres dette af Koncernservices?

Svar

Det foretages af ekstern revision en gang om året.

Herudover er det ledernes daglige ansvar at sikre kontrol.

Ved omrokeringer, omorganiseringer og lign. foretager KS også stikprøvekontrol.

KS har ført stikprøvekontrol med de enkelte forvaltninger, men processen er tung, idet der bl.a. er en lav svarprocent.

KS er pt. i færd med at føre opgaven med stikprøvekontrol over på det almindelige ledelsestilsyn i de enkelte forvaltninger på lige fod med andre ledelsesopgaver.

Spørgsmål 5
Det følger ligeledes under overskriften periodisk review, at it-sikkerhedsfunktionen især skal sikre, at der sker kontrol af de medarbejdere, der har adgang til fortrolige personoplysninger. Hvorledes sikres dette af Koncernservice?

Svar

Samme svar som ovf. grundet, at de fleste medarbejdere i KK har adgang til fortrolige personoplysninger.

Uddybende it-sikkerhedsregler - opfølgning på logning

Spørgsmål 6
Det følger af uddybende sikkerhedsregler, at der skal ske opfølgning på logning. Hvilken logdata skal der følges op på? Hvordan afgrænses logdata, som der skal ske opfølgning i forhold til? Og hvad ligger der i de uddybende sikkerhedsreglers begreb i form af "kritiske data" (er dette f.eks. følsomme personoplysninger)?

Svar:

Der er mange varianter af log dels fra system, database og brugerhandlinger. Det er systemejerne der selv skal fastsætte kriterier for, hvilken log der skal ske (bl.a. afhængig i lex specialis).

Hvis KS har ansvaret, er der et team, der fører log opfølgning (KS har også i nogle tilfælde lavet aftale med KMD om, at et team dér foretager log opfølgning – dette er f.eks. også tilfælde vedr. aftale med CSC).

På "fagsystemerne" (altså de it-systemer, som de enkelte forvaltninger har ansvaret for) er det systemejerne selv, der skal foretage logning og lave log opfølgning.

Det er et KS initiativ på baggrund af PWC rapporten, at det skal være mere præcist, hvordan systemejerne i fagsystemer skal føre log opfølgning

Emne: Koncernservices eventuelle kontrol med overholdelsen af sikkerhedsforanstaltningerne

Spørgsmål 7
Fører Koncernservice nogen kontrol med overholdelsen af sikkerhedsforanstaltningerne, som er udelegeret efter regulativets regler om det interne organisatoriske forhold/ansvarsfordelingen (dvs. fører Koncernservice tilsyn med, om de, som har fået delegeret ansvaret, overholder kontrol med autorisation, jf. § 17, kontrol med afviste adgangsforsøg, jf. § 18, samt opfølgning på logning i henhold til uddybende it-sikkerhedsregler s. 15)? Og i givet fald præciser venligst hvorledes Koncernservice udfører kontrol/tilsyn, herunder stikprøvekontrol? Hvad regler kontrollerer Koncernservice om der bliver overholdt? (både ift. §§ 17 og 18 i sikkerhedsbekendtgørelsen samt i forhold til opfølgning på logning i henhold til uddybende sikkerhedsregler s. 15? Herunder hvilke systemer (it-systemer og/eller netværk) er genstand for Koncernservices kontrol/tilsyn?

Svar:

KS har på eget område tilsyn

Forvaltningerne har inden for eget område eget tilsyn

Det er et KS initiativ på baggrund af PWC rapporten, at der skal ske en tydeliggørelse af ansvarsområder i relation til sikkerhedsforanstaltningerne.

Emne: it-sikkerhedsbrud

Koncernservices svar af 30. juni 2014
Vedrørende formuleringen: Håndtering af it-sikkerhedshændelser/it-sikkerhedsbrud "sker konkret efter henvendelse eller hvis it-sikkerhedsfunktionen i øvrigt bliver opmærksom på en hændelse", jf. side 3, punkt 5.

Spørgsmål 8
Hvordan kan it-sikkerhedsfunktionen blive opmærksom på en hændelse, hvis der ikke modtages en konkret henvendelse (uddyb gerne med eksempler og f.eks. i hvilke situationer og hvilke it-systemer det kan ske)?

Svar:

Kun ved KS på logning inden for eget område samt ved KS logning på netværket, kan KS selv blive opmærksomme på it-sikkerhedshændelser.

Hændelser i fagsystemer, som andre forvaltninger har ansvaret for, beror helt på, om det bliver identificeret i forvaltningerne.

Det er et KS initiativ på baggrund af PWC rapporten, at der skal anskaffes et system, der giver mulighed for øget fælles monitorering.

Emne: eventuelle alarmsystemer/funktioner i it-systemer, hvor der behandles følsomme personoplysninger

Spørgsmål 9
Findes der alarmsystemer/funktioner i it-systemer, som automatisk alarmerer i tilfælde af it-sikkerhedshændelser/it-sikkerhedsbrud? Og i givet fald i hvilke it-systemer? Og hvilke forvaltninger hører it-systemerne under?

Svar

Ja, for så vidt angår enhver adgang til netværket og kommunens computere – og adgang hertil er en forudsætning for at kunne anvende ethvert system samt fagsystemer. Adgangen til netværk og kommunens computere har således alarmfunktion til brugeradministrationen i KS.

Når man først er inden i fagsystemerne, er der er adgangsbegrænsninger i forhold til, hvordan autorisationen er sat op – dvs. hvilke rettigheder hver medarbejder har, hvilket systemejerne har sat op. I de enkelte alarmsystemer er der også sat alarmfunktioner op, hvis brugere forsøger at få adgang til noget, som de ikke har rettigheder til.

Koncernservice foretager kun overvågning af Netværkstrafik samt driftscentre.

Men overvågning af brugerlogs i de enkelte systemer er ikke fælles. På nogle it-systemer, som forvaltningerne har ansvaret for, er der indgået databehandleraftaler med it-udbydere som f.eks. KMD om logning og opfølgning herpå. Dette er f.eks. tilfældet i KMD systemer og for Exchange.

Det er et KS initiativ på baggrund af PWC rapporten, at der skal skabes bedre styring af hændelsesoverblik samt logning i fællessystemer.

Spørgsmål 10
Hvis ovenstående spørgsmål er svaret bekræftende: har de pågældende it-systemer en centralalarmfunktion således, at Koncernservice (it-sikkerhedsfunktionen) automatisk bliver gjort opmærksom i tilfælde af it-sikkerhedshændelse/it-sikkerhedsbrud?

Svar

Svaret er indeholdt i svar 9.
…"

Borgerrådgiveren udførte den 3. februar 2015 et yderligere telefoninterview med Koncernservice for afklaring af et enkelt forhold. Referatet fra telefoninterviewet gengives i det følgende (svar er angivet i kursiv):

"…
Emne: it-systemer i KK, som er blevet taget i brug inden kravet om, at anskaffelser af nye it-systemer skal sikkerhedsgodkendes via FISKK proceduren.

Spørgsmål

Har KS lavet en opfølgende indsats i forhold til sådanne it-systemer med henblik på at sikre, at it-systemerne opfylder sikkerhedskravene efter kap. 3 i sikkerhedsbekendtgørelsen og kommunens interne it-sikkerhedsregler?

Svar:

KS har indsamlet materiale fra alle forvaltninger i kommunen vedrørende brugen af sådanne it-systemer i de forskellige forvaltninger, og derefter er forvaltningernes it-systemer blevet registeret i FISKK, hvor det vurderes, om systemerne opfylder it-sikkerhedskravene. Der er udpeget systemejere til disse it-systemer.
…"

BILAG

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