From: Mathilde Illum Aastrøm
Sent: 21-02-2014 14:29:25
To: Linea Holm Rasmussen
Subject: 2014-0035173-2 - Samlet scan Vedrørende Borgerrådgiverens generelle egen driftsundersøgelse om sikring af borgernes personoplysninger
Attachments: Vedrørende Borgerrådgiverens generelle egen driftsundersøgelse om sikring af borgernes personoplysninger.PDF

Hej Linea

Håber det er ok ☺ Den kan jo ikke blive en aktiv PDF, fordi jeg har scannet word og PDF sammen til en PDF.

Med venlig hilsen

Mathilde Illum Aastrøm
Chefkonsulent
Digitalisering

KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncernservice

Borups Allé 177 Vær. A2
2400 København NV

Mobil 3052 9258
Email mathilde.illum.aastrom@ks.kk.dk
EAN 5798009809025

KØBENHAVNS KOMMUNE

NOTAT

21-02-2014

Sagsnr.
2014-0035173

Dokumentnr.
2014-0035173-2

Sagsbehandler
Jens Ingemann
Jakob Joensen

Til Økonomiudvalget

Vedrørende Borgerrådgiverens generelle egen driftsundersøgelse om sikring af borgernes personoplysninger

Koncernservice har d. 13. februar 2014 modtaget vedlagte henvendelse fra Borgerrådgiveren vedrørende en driftsundersøgelse om sikring af borgernes personoplysninger.

Borgerrådgiveren kan af egen drift iværksætte undersøgelser af konkrete og generelle forhold samt gennemføre inspektioner i Københavns Kommune.

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

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-sikkerhedsfunktion i Københavns Kommune.

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

Borgerrådgiveren har anmodet Koncernservice om at besvare henvendelsen indenfor en frist på 8 uger.

Københavns Kommunes eksterne revision indeholder hvert år en it-revision, der er primært er rettet mod systemer, der er omfattet af Københavns Kommunes Kasse- og Regnskabsregulativ og dele af it-infrastrukturen, der understøtter disse systemer. På en række områder omhandler it-revisionen de samme forhold, som Borgerrådgiveren her ønsker at undersøge. Det gælder bl.a. i forhold til logning og intern kontrol af adgang til systemerne.

Koncernservice vil snarest afholde et møde med Borgerrådgiveren for nærmere at afklare hvilken dokumentation, Borgerrådgiveren ønsker at modtage fra Koncernservice. På mødet vil den nærmere tidsplan for undersøgelsen også blive drøftet, idet Koncernservice som udgangspunkt forventer at kunne fremsende en besvarelse af Borgerrådgiverens henvendelse indenfor den frist på 8 uger, som Borgerrådgiveren anfører.

Koncernservice vil – med henblik på at besvare de konkrete spørgsmål Borgerrådgiveren stiller i henvendelsen - iværksætte en proces for at indsamle svar og dokumentere, hvordan Koncernservice sikrer borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang til borgernes personoplysninger.

Dokumentationen vil omfatte både informationsmateriale rettet mod medarbejdere og fortrolige dokumenter om Københavns Kommunes håndtering af it-sikkerheden i kommunens it-infrastruktur.

Behovet for at involvere forvaltningerne i besvarelsen, vil blive afklaret på mødet med Borgerrådgiveren.

Bilag
Brev af d. 13. februar 2014: "Vedrørende Borgerrådgiverens generelle egen driftundersøgelse om sikring af borgernes personoplysninger."

KØBENHAVNS KOMMUNE
Borgerrådgiveren

Til Koncernservice i Økonomiforvaltningen

13-02-2014

Sagsnr.
2012-167267

Dokumentnr.
2012-167267-1

Sendt d.d. til: cj@okf.kk.dk; bw@okf.kk.dk; lal@okf.kk.dk; ask@okf.kk.dk; mlm@okf.kk.dk; bn0g@okf.kk.dk

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.

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

Om undersøgelsens formål og tema

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