

SIKRING AF BORGERNES PERSONOPLYSNINGER

ENDELIG RAPPORT



INDHOLDSFORTEGNELSE

1. INDLEDNING	3
2. KONKLUSION OG SAMMENFATNING	4
3. KONSEKVENSER	6
4. FORSLAG, HENSTILLINGER OG ANBEFALINGER	7
5. UDDYBNING, BISTAND MV.	8
BORGERRÅDGIVERENS KRITIKSKALA	9
BILAG – SE SÆRSKILT RAPPORT	10

I. INDLEDNING

Denne rapport indeholder Borgerrådgiverens endelige vurderinger og bedømmelser i anledning af Borgerrådgiverens undersøgelse om sikring af borgernes personoplysninger imod uberettiget videregivelse og imod, at medarbejderne i kommunen skaffer sig uberettiget adgang dertil.

Undersøgelsen er rettet mod Koncernservices overordnede tilsyn, 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.

Undersøgelsen er afgrænset til en gennemgang og vurdering af Københavns Kommunes sikkerhedsforanstaltninger i forhold til følsomme personoplysninger efter kapitel 3 i bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (herefter sikkerhedsbekendtgørelsen) samt Regulativ for it-sikkerhed i Københavns Kommune.

Vurderingsgrundlaget for undersøgelsen er lov om behandling af personoplysninger (herefter persondataloven), sikkerhedsbekendtgørelsen, Regulativ for it-sikkerhed i Københavns Kommune, uddybende it-sikkerhedsregler for Københavns Kommune samt vejledningsmateriale vedrørende it-sikkerhed for Københavns Kommune.

Til brug for undersøgelsen har Borgerrådgiveren modtaget en udtalelse fra Koncernservice samt dokumentation. Herudover har Borgerrådgiveren fra Koncernservice modtaget eksterne revisionsrapporter vedrørende revision af generelle it-kontroller hos Københavns Kommune for 2012 samt for 2013, ekstern konsulentrapport vedrørende modenhedsvurdering af informationssikkerhed hos Københavns Kommune for 2014 samt Koncernservices opfølgende initiativer herpå.

Rapporten har i en foreløbig udgave været sendt til Økonomiforvaltningen med henblik på forvaltningens eventuelle bemærkninger til rapportens faktiske oplysninger.

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

Borgerrådgiveren august 2015



Johan Busse
Borgerrådgiver

2. KONKLUSION OG SAMMENFATNING

Denne rapport handler om det overordnede tilsyn med forvaltningernes tilsynsarbejde, som påhviler Koncernservice. For god ordens skyld bemærkes, at ansvarsfordelingen efter Regulativ for it-sikkerhed i Københavns Kommune, er således, at ansvaret for iværksættelse af sikkerhedsforanstaltninger efter kapitel 3 i sikkerhedsbekendtgørelsen er uddelegeret til de enkelte forvaltninger, som har ansvaret for de it-systemer, hvor der behandles personoplysninger, mens ansvaret for det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser påhviler Koncernservice.

Min undersøgelse viser, at Koncernservice ikke forholder sig aktivt til, hvorvidt forvaltningernes iværksatte sikkerhedsforanstaltninger for så vidt angår kontrol med autorisation, kontrol med afviste adgangsforsøg samt log-opfølgning er tilstrækkelige. Koncernservice foretager stikprøvekontrol med autorisationer, men Koncernservice foretager ikke tilsyn med forvaltningernes kontrol med afviste adgangsforsøg samt forvaltningernes log-opfølgning, hvilket jeg finder utilstrækkeligt. På grund af manglende stillingtagen og tilsyn er det uvist, hvorvidt forvaltningerne opfylder sikkerhedsforanstaltningerne efter kapitel 3 i sikkerhedsbekendtgørelsen samt kommunens it-sikkerhedsbestemmelser.

Ovenstående forhold indebærer efter min opfattelse risiko for, at borgernes følsomme personoplysninger ikke i tilstrækkeligt omfang er sikret imod uberettiget videregivelse samt imod, at medarbejdere uberettiget skaffer sig adgang til disse oplysninger.

Koncernservice udgør et selvstændigt it-sikkerhedsområde under Økonomiforvaltningen. Koncernservice er bl.a. ansvarlig for fællessystemer, drift og it-sikkerhedsfunktionen. Det følger af Regulativ for it-sikkerhed i Københavns Kommune, at It-sikkerhedsfunktionen i Koncernservice fører det daglige tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser. Alle anskaffelser af nye it-systemer skal sikkerhedsgodkendes via FISKK-proceduren hos it-sikkerhedsfunktionen, hvilket sikrer, at systemerne opfylder it-sikkerhedskravene til sikkerhed.

Ansvaret for iværksættelse af sikkerhedsforanstaltninger i henhold til Regulativ for it-sikkerhed i Københavns Kommune er, som nævnt, uddelegeret til de enkelte forvaltninger, som har ansvaret for it-systemerne. Når forvaltningerne har ansvaret for it-systemer, skal direktionerne i forvaltningerne fastsætte et passende sikkerhedsniveau og udpege en systemejer til hvert enkelt it-system. Systemejer skal sikre, at it-systemet efterlever it-sikkerhedskravene og sikre, at der løbende sker log-opfølgning i forhold til afviste adgangsforsøg mv. De personaleansvarlige ledere skal mindst en gang hvert halve år kontrollere tildelte autorisationer og i øvrigt føre ledelsesmæssigt tilsyn med systemejerens samt medarbejderes opfyldelse af sikkerhedsforanstaltningerne.

Koncernservice forholder sig ikke aktivt til, hvorvidt forvaltningernes sikkerhedsforanstaltninger er tilstrækkelige, og fører ikke tilsyn med forvaltningernes kontrol af afviste adgangsforsøg eller forvaltningernes log-opfølgning. Det må antages, at Koncernservice har mulighed herfor inden for rammerne i det gældende Regulativ for it-sikkerhed i Københavns Kommune.

På grund af den manglende stillingtagen og det manglende tilsyn er det uvist, hvorvidt forvaltningerne på tilstrækkelig vis opfylder sikkerhedsforanstaltningerne efter kapital 3 i sikkerhedsbekendtgørelsen samt kommunens it-sikkerhedsbestemmelser. Herudover er der risiko for et uensartet sikkerhedsniveau i de forskellige forvaltninger i forhold til sikkerhedsforanstaltningerne. Tilstrækkelige og hensigtsmæssige sikkerhedsforanstaltninger i de enkelte forvaltninger er en afgørende forudsætning for, at brud på it-sikkerheden kan identificeres, idet der ikke forefindes fælles alarmfunktioner i forvaltningernes it-systemer, som underretter Koncernservice i tilfælde af it-sikkerhedshændelser i forvaltningernes egne it-systemer. Koncernservices kan kun opnå kendskab til it-sikkerhedshændelser i forvaltningernes egne it-systemer, såfremt forvaltningerne selv identificerer disse og indberetter til Koncernservice.

3. KONSEKVENSER

De konstaterede fejl kan have betydning for sikkerhedsniveauet for kommunens opbevaring og behandling af borgernes følsomme personoplysninger, idet det er uvist, hvorvidt forvaltningerne på tilstrækkelig vis opfylder sikkerhedsforanstaltningerne efter kapitel 3 i sikkerhedsbekendtgørelsen samt kommunens it-sikkerhedsbestemmelser. Herudover er der risiko for et uensartet sikkerhedsniveau i forvaltningerne samt risiko for, at brud på it-sikkerheden ikke identificeres.

4. FORSLAG, HENSTILLINGER OG ANBEFALINGER

Borgerrådgiveren anbefaler, at Koncernservice foretager en aktiv stillingtagen til, hvorvidt forvaltningernes iværksatte sikkerhedsforanstaltninger er tilstrækkelige. Borgerrådgiveren anbefaler samtidig, at Koncernservice fører tilsyn (stikprøvekontrol) med forvaltningernes kontrol med afviste adgangsforsøg samt med forvaltningernes log-opfølgning i it-systemer, hvor der behandles følsomme personoplysninger.

Herudover anbefaler Borgerrådgiveren, at Koncernservice iværksætter målrettet vejledning til de personaleansvarlige ledere om deres ansvar for så vidt angår kontrollen med autorisationer samt målrettet vejledning til de personaleansvarlige ledere om systemejeneres ansvar for løbende log-opfølgning for at skabe øget fokus på det ledelsesmæssige tilsyn hermed.

Borgerrådgiveren anbefaler endvidere, at Koncernservice overvejer mulighederne for at etablere monitoreringsfunktion i it-systemer, som forvaltningerne selv har ansvaret for, med henblik at opnå et fælles overblik over it-sikkerhedshændelser.

Borgerrådgiveren er opmærksom på, at Koncernservice på baggrund af PWC ekstern konsulentrapport vedrørende modenhedsvurdering af informationssikkerhed har iværksat en række initiativer, som bl.a. forsøger at imødekomme en del af ovennævnte problemstillinger.

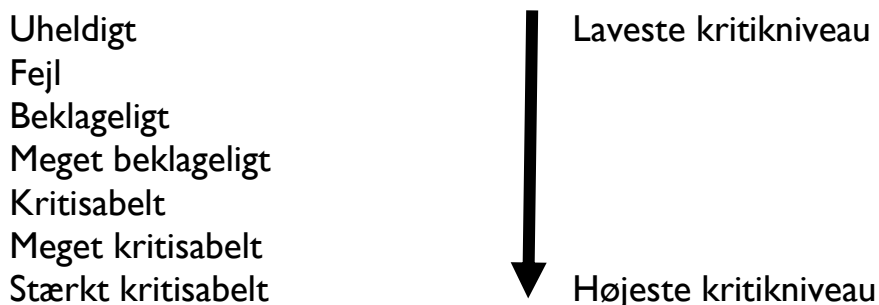
Borgerrådgiveren henstiller Koncernservice til at inddrage Borgerrådgiverens vurderinger og anbefalinger i det videre arbejde med disse initiativer.

5. UDDYBNING, BISTAND MV.

Borgerrådgiveren uddyber gerne undersøgelsen samt vurderinger mv. på et møde, såfremt det ønskes. Forvaltningen bedes i givet fald kontakte Daniel Soelberg Bach, za6n@okf.kk.dk, tlf. 3366 1400, for nærmere aftale.

Borgerrådgiveren hjælper også meget gerne til med intern opfølgning på sagen, herunder i form af undervisning, vejledning om reglernes anvendelse i praksis mv. Forvaltningen bedes i givet fald kontakte Daniel Soelberg Bach, za6n@okf.kk.dk, tlf. 3366 1400, for nærmere aftale.

BORGERRÅDGIVERENS KRITIKSKALA



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

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

BILAG – SE SÆRSKILT RAPPORT

BILAG 1 – BORGERRÅDGIVERENS OBSERVATIONER OG VURDERINGER

BILAG 2 – METODE

BILAG 3 – VURDERINGSGRUNDLAG

BILAG 4 – BORGERRÅDGIVERENS HØRINGSBREV

BILAG 5 – FORVALTNINGENS HØRINGSSVAR

BILAG 6 – OPFØLGENDE SPØRGSMÅL OG SVAR

BILAG 7 – TELEFONINTERVIEWS

SIKRING AF BORGERNES PERSONOPLYSNINGER

ENDELIG RAPPORT

Redaktion

Borgerrådgiveren

Kontakt

Københavns Kommune
Vester Voldgade 2A
1552 København V

Foto

Borgerrådgiveren

Tryk

Oplag

ISBN

Udgiver

Borgerrådgiveren

KØBENHAVNS KOMMUNE

Borgerrådgiveren

Vester Voldgade 2A

1552 København V

Telefon: 33 66 14 00

Telefax: 33 66 13 90

E-mail: borgerraadgiveren@kk.dk

www.kk.dk/borgerraadgiveren