KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

Til Borgerrepræsentationens Sekretariat

29. maj 2018

Sagsnr.
2018-0145327

Dokumentnr.
2018-0145327-2

Sagsbehandler
Frederik Siegumfeldt

Brug af egne mobile enheder i arbejdssammenhæng

Baggrund

Et medlem af Borgerrepræsentationen, Karen Melchior, har anmodet om en forklaring på, hvorfor Københavns Kommune har valgt et sikkerhedsniveau for mobile it-enheder, som ikke gør det muligt at tilgå den arbejdsrelaterede kalender og arbejdsmail på f.eks. private mobiltelefoner.

Karen Melchior henviser i den forbindelse til, at denne begrænsning vanskeliggør det daglige arbejde, hvilket bl.a. mangedobler mulighederne for fejl i en travl hverdag med megen kalendergymnastik.

MDM til mobile enheder

Med henblik på at sikre behandlingen af oplysninger på mobile enheder installeres der et program, Mobile Device Management-program (MDM), som giver Københavns Kommune mulighed for at kontrollere de enkelte mobile enheder.

MDM giver bl.a. en sikker adgang til brug af mail, kalender, intranet og selvbetjeningsløsninger. MDM giver også mulighed for, at alle data kan slettes på en bortkommet enhed.

Overvejelser om brug private mobile enheder

Som Københavns Kommunes it-sikkerhedsregler pt. er udformet, er det ikke tilladt for hverken Borgerrepræsentationens medlemmer eller kommunes ansatte at bruge egne mobile enheder i arbejdssammenhæng.
Københavns Kommune behandler i stort omfang meget fortrolige og følsomme informationer, og en del af disse informationer behandles på mobile enheder.

Københavns Kommune har ved fastlæggelsen af sikkerhedsniveauet for mobile enheder foretaget en afvejning af hensyn til:

- At de enkelte forvaltningerne kan tilgå, behandle og gemme oplysninger på den mest fleksible måde
- At de enkelte medarbejdere har en interesse i at kunne varetage både private og arbejdsrelaterede opgaver på en smidig måde
- At den anvendte MDM-løsning er forsvarlig i relation til sikkerhed, drift og økonomi.

IT-sikkerhed og Videnscentre

Borups Allé 177
2400 København NV

EAN nummer
5798009809308

I relation til det fastlagte sikkerhedsniveau har Københavns Kommune særligt lagt vægt på:

- At der i kommunen (herunder BR) i stort omfang behandles fortrolige informationer
- At oplysninger ved transmission til og fra mobile enheder sker på en sikker måde
- At tilgangen til oplysninger, der opbevares på mobiler enheder, sker på en forsvarlig måde
- At kommunen i nødvendigt omfang kan kontrollere de mobile enheder i forhold til f.eks. installation af applikationer og sikkerhedsindstillinger
- At kommunen i tilfælde af bortkomst af mobile enheder kan slette al information på enhederne.

I tilknytning til ovenstående faglige og sikkerhedsmæssige hensyn giver brugen af private mobile enheder også anledning til andre overvejelser, hvoraf nogle er af mere personaleadministrativ karakter, herunder bl.a.:

- Hvorvidt kommunen er berettiget til at kontrollere og tage sig adgang til oplysninger, som alene vedrører den ansattes privatliv (f.eks. i forbindelse med service, backup og sletning)
- Hvorvidt kommunen er berettiget til at forbyde installation af særlige applikationer på private enheder
- Hvorvidt kommunen er ansvarlig for skader på en mobil enhed eller ej
- Hvorvidt kommunen bør sætte grænser for, hvilke typer af private enheder, som kan anvendes i arbejdsrelaterede sammenhænge (idet ikke alle mobile enheder nødvendigvis kan håndteres sikkerhedsmæssigt forsvarligt).

Sammenfatning
Koncern IT er opmærksom, at der er et udbredt ønske blandt borgerrepræsentationens medlemmer og kommunens medarbejdere om at kunne anvende egne mobile enheder i arbejdsmæssig sammenhæng. Koncern IT vurderer derfor også løbende, hvorvidt der for mobile enheder er grundlag for at overgå til eventuelle andre (nye) sikkerhedsløsninger, som kan tilgodese et sådant ønske.

Afslutningsvis skal Koncern IT for en god ordens skyld bemærke, at det fremgår af Københavns Kommunes it-sikkerhedsregler, at arbejdsrelaterede oplysninger skal håndteres og opbevares sikkert og forsvarligt, hvorved der som udgangspunkt sigtes til kommunens mail- og kalendersystemer, lokale fagsystemer, kommunens journalsystem eller på kommunens netværksdrev. Såvel ansatte som borgerrepræsentationens medlemmer bør således sikre sig, at

mødeindkaldelser, der videresendes til private kalendere, ikke i sig selv eller i form af vedhæftet indhold indebærer, at fortrolige informationer opbevares uden for kommunes sikrede it-miljøer i strid med kommunens regler herom.