Koncern IT
Økonomiforvaltningen

Notat

Til Jakob Næsager

Svar på spørgsmål vedr. persondatabeskyttelse

5. februar 2020

Sagsnummer
2020-0001173

Dokumentnummer
2020-0001173-1

Sagsbehandler
Michael Cornelius M Hansson

Resumé af sag
På et møde i Økonomiudvalget d. 10. december 2019 fremsatte Jakob Næsager tre spørgsmål på databeskyttelsesområdet vedrørende 1) persondatabrud, 2) uberettigede opslag i systemer og 3) fjernelse af fratrådte medarbejderes it-adgange.

KIT/Økonomiforvaltningen har herunder udarbejdet en skriftlig besvarelse af spørgsmålene.

Spørgsmål 1
Hvordan kontrolleres det, at brud på persondatasikkerheden indberettes, herunder på områder hvor cpr.nr. er en fast del af arbejdsprocesserne, fx hos Borgerservice?

Svar
Indberetning og anmeldelse af persondatabrud fra Københavns Kommune (KK) til Datatilsynet er beskrevet i *Forretningscirkulære for persondatabeskyttelse – dokumentation og compliance*, der er godkendt af Økonomiudvalget i januar 2019. Selve forretningsgangen, der er obligatorisk at følge for alle forvaltningerne, er formaliseret i *Fællesadministrativ forretningsgang - persondatabrud*.

Denne forretningsgang skal altid følges, således også i Borgerservice, Kultur- og Fritidsforvaltningen.

Hvis en medarbejder i KK opdager et potentielt brud på persondatasikkerheden, har medarbejderen pligt til at indberette dette gennem kommunens it-portal (ServiceNow) eller forvaltningens DPO Business Partner.

Det er et krav, at forvaltningerne sikrer, at alle relevante medarbejdere har gennemgået den obligatoriske uddannelse på databeskyttelsesområdet, hvor der oplyses om, hvordan et potentielt brud på persondatasikkerhedsområdet indmeldes. I hver forvaltning er forvaltningens DPO Business Partner ansvarlig for, at persondatabrud indberettes til Datatilsynet, hvilket sker gennem KK's Databeskyttelsesrådgiver.

KK's Databeskyttelsesrådgiver har central adgang til alle indberetninger og kan herigennem overvåge og føre tilsyn med forvaltningernes behandling af indmeldte brud på persondatasikkerheden.

Spørgsmål 2
Hvordan sikres det, at der ikke foretages opslag i cpr-systemer, som ikke er relevante/berettigede for arbejdets udførelse?

Svar
Sikring mod uberettigede opslag i it-systemer sikres i første omgang gennem korrekt tildeling af brugeradgange. Tildelingen af brugeradgange administreres som udgangspunkt af den centralt placerede brugeradministration i Koncern IT på baggrund af bestilling fra den pågældende medarbejders leder. Denne proces sikrer, at medarbejdere i første omgang kun får tildelt rettigheder til de it-systemer, der er relevante for dem.

Jf. *Forretningscirkulære for informationssikkerhed* er det desuden et krav, at den enkelte leder løbende fører ledelsestilsyn med brugeradgange, hvilket yderligere skal sikre, at medarbejdere ikke har unødvendige adgange. I koordination med Intern Revision er KK desuden ved at implementere en IGA-løsning (Identity Governance and Administration), som skal sikre, at personaleledere i fremtiden automatisk kan danne sig overblik over sine medarbejderes brugeradgange, hvilket vil gøre ledelsestilsyn lettere.

For yderligere sikring mod uberettigede opslag har KK desuden en række foranstaltninger til at dokumentere, opfange og rapportere uberettigede opslag. Eksempelvis følger det af *Forretningscirkulære for informationssikkerhed,* at relevante kommunale it-systemer skal have etableret procedurer for opfølgning på logs, samt at systemerne er integreret til KK's løsning for overvågning af uregelmæssig adfærd (SIEM). Gennem SIEM kan uberettigede opslag opfanges automatisk ud fra en række søgekriterier. Enkelte systemer har desuden tilkoblet relationskontrol, som gør det muligt at opfange, hvis en medarbejder foretager opslag på vedkommendes familie eller personer med samme adresse.

Spørgsmål 3
Hvordan sikres det, at fratrådte medarbejderes it-adgange fjernes?

Svar
Fjernelse af it-adgange og -rettigheder sker som udgangspunkt gennem brugeradministrationen i Koncern IT. Den fratrædende medarbejders leder er ansvarlig for at indberette fratrædelsen gennem kommunens it-portal (ServiceNow), hvorefter en slettesag oprettes og gennemføres af brugeradministrationen.

På systemer, hvor brugeradministrationen varetages lokalt, er der opsat lokale procedurer for sletning af it-adgange jf. *Forretningscirkulære for organisering af informationssikkerhed*. Koncern IT førte i 2018 tilsyn med dette område i alle forvaltningerne. Her vurderede Koncern IT i alle tilfælde, at forvaltningens procedurer for sletning af medarbejderes adgange var forsvarlig.