

Bilag 1

INFORMATIONSSIKKERHEDSPOLITIK

1. Ramme for politikken

Informationssikkerhedspolitikken, det tilhørende Informationssikkerhedsregulativ og underliggende regelsæt følger den til enhver tid gældende lovgivning og regulering, herunder Lov om kommunernes styrelse, Styrelsesvedtægt for Københavns Kommune, persondatareguleringen, samt forvaltningsretlige krav af betydning for informationssikkerheden og sikringen af borgernes rettigheder i bred forstand.

Politikken, det tilhørende Informationssikkerhedsregulativ og underliggende regelsæt gælder for alle juridiske enheder under Københavns Kommune, hvor Københavns Kommune enten er dataansvarlig eller databehandler, og omfatter værdioplysninger samt personoplysninger fra alle borgere, medarbejdere og andre personer, hvis personoplysninger registreres af kommunen (herefter registrerede).

Politikken træder i kraft, når den er godkendt af Borgerrepræsentationen.

Økonomiforvaltningen har ansvar for vedligeholdelse af politikken, herunder for forelæggelse og godkendelse for Økonomiudvalget og Borgerrepræsentationen. Økonomiforvaltningen inddrager relevante tværgående fora, hvor alle forvaltninger er repræsenteret på direktionsniveau.

2. Vision

Visionen for informationssikkerhed i Københavns Kommune er: *Lovlig forvaltningsvirksomhed og tryghed for borgerne og virksomhederne i mødet med Københavns Kommune.*

3. Strategi

Trygheden opnås ved efterlevelse af gældende lovgivning og ansvarlig behandling af personoplysninger, værdioplysninger og øvrige oplysninger, som modtages og behandles i forbindelse med kommunens opgaveløsning.

Den konkrete strategi for at udmønte visionen baserer sig på en række styringsprincipper, der med udgangspunkt i en risikobaseret tilgang skal medføre et optimalt og ensartet sikkerhedsniveau i alle kommunens forvaltninger. Sikkerhedsniveauet er udtryk for en afvejning af hensynet til sikkerhed, brugervenlighed og økonomi. Strategien skal løbende vurderes og tilpasses efter behov.

4. Mål

Strategien lægger den overordnede ramme for at opfylde Københavns Kommunes mål om:

- *at sikre et vedvarende, ensartet og passende niveau for lovmedholdelighed, fortrolighed, integritet og tilgængelighed, når kommunen modtager, behandler, opbevarer og transmitterer data, herunder person- og værdioplysninger.*

Med lovmæthed menes, at love og regler for behandling af personoplysninger udmøntes korrekt og beskytter de registreredes rettigheder.

Med fortrolighed menes, at person- og værdioplysninger i alle tilfælde kun er tilgængelig for de medarbejdere, systemer eller eksterne parter, der har et lovligt arbejdsbetinget behov for at have adgang til disse.

Med integritet menes, at person- og værdioplysninger i alle tilfælde er valide og med garanti for, at data ikke er manipulerede.

Med tilgængelighed menes, at det skal være muligt at tilgå systemer og data for autoriserede personer, når det er nødvendigt.

5. Risikovillighed

Informationssikkerhedsniveauet skal være stabilt og bestemt ud fra Københavns Kommunes aktuelle risikoniveau for henholdsvis databeskyttelse og informationssikkerhed. Dog går hensynet til overholdelse af gældende lovgivning, herunder den registreredes retsstilling og rettigheder, forud for hensynet til kommunens økonomiske og ressourcemæssige indsats for opnåelse af tilstrækkelig informationssikkerhed.

Den konkrete risiko skal løbende følges og omfanget af den ressourcemæssige og økonomiske indsats for at nedbringe risici skal disponeres ud fra det besluttede risikoniveau.

6. Ansvar og organisering

Informationssikkerheden skal udmøntes gennem tydelige regelsæt i overensstemmelse med kommunens regelhierarki og skal understøttes af styringsprincipper, dokumenterede processer og det rette kompetenceniveau hos kommunens medarbejdere.

7. Tilsyn

Tilsyn foretages ud fra en risikobaseret tilgang og gennemføres af de relevante aktører i Københavns Kommune:

- Lovpligtig Revision
- Borgerrepræsentationen og Økonomiudvalget
- Databeskyttelsesrådgiveren
- Forvaltningens ledelse

8. Beredskab

Der skal foreligge opdaterede beredskabsplaner for relevante områder og systemer i Københavns Kommune til brug i de situationer, hvor systemer eller områder evt. rammes af forhold, der aktiverer beredskabet. Beredskabsplanerne skal baseres på en vurdering af områdets eller systemets kritikalitet.

9. Udmøntning og drift

Udmøntning af politikken sker gennem Informationssikkerhedsregulativet og dertil hørende underliggende cirkulærer, der regulerer følgende tre hovedområder:

- Informationssikkerhed
- Databeskyttelse
- It-livscyklus.

10. Ikrafttrædelse og ajourføring

Politikken træder i kraft, når den er godkendt af Borgerrepræsentationen og gælder til en ny version er godkendt af Borgerrepræsentationen.

Redaktionelle ændringer, som ikke ændrer grundlæggende ved Informationssikkerhedspolitikken, Informationssikkerhedsregulativet eller forretningscirkulærer, kan dog godkendes af Økonomiforvaltningens direktion. Tilsvarende gælder ændringer affødt af Borgerrepræsentationens beslutninger, der medfører, at der skal foretages konsekvensrettelser ved Informationssikkerhedspolitikken, Informationssikkerhedsregulativet eller underliggende forretningscirkulærer.