



INFORMATIONSSIKKERHEDSREGULATIV

Indhold

1.	Generelt.....	2
1.1.	Formål	2
1.2.	Lovgrundlag	2
1.3.	Regelsættets opbygning.....	3
1.4.	Gyldighedsområde	4
1.5.	Ajourføring	4
2.	Habilitet og uafhængighed.....	5
3.	Styringsprincipper	5
3.1.	Ledelses- og beslutningshierarki	5
3.2.	Rolle- og ansvarsfordeling.....	6
3.3.	Ressourcer og kompetencer	7
3.4.	Risikovurderinger	8
3.5.	Dokumentation	8
3.6.	Styring af eksterne parter	9
3.7.	Tilsyn	9
3.8.	Rapportering	10
3.9.	Hændelsesforanstaltninger	11
3.10.	Databeskyttelse og registreredes rettigheder	11
3.11.	Beredskabsplaner	11
4.	Databeskyttelsesrådgiveren.....	12
5.	Udmøntning og drift.....	13
6.	Ikrafttrædelse.....	13



1. Generelt

Det påhviler enhver medarbejder at handle sagligt og forsvarligt i alle anliggender, der kan have betydning for informationssikkerheden i Københavns Kommune.

1.1. Formål

Økonomiudvalget varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it-forhold, jf. Styrelsesvedtægten for Københavns Kommune (KKSTV), § 12, stk. 6, 3. pkt.

Informationssikkerhedsregulativet (herefter Regulativet) har til formål at udmønte ansvars- og rollefordelingen i KKSTV dels i relation til styringen af kommunens overordnede og tværgående it-forhold, dels i relation til varetagelsen af kommunens ansvar som dataansvarlig i henhold til lovgivningen om behandling af personoplysninger, herunder udmøntning af Københavns Kommunes informationssikkerhedspolitik, der gennem vision, strategi og mål fastlægger rammen for kommunens informationssikkerhed. Målet for kommunens informationssikkerhedspolitik er:

- *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.*

Regulativet fastlægger således de overordnede principper for kommunens håndtering af følgende overordnede områder: 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus'.

Vedtagelse og håndhævelse af underliggende bindende tværgående forretningscirkulærer og fællesadministrative forretningsgange inden for de pågældende områder skal ske i overensstemmelse med og indenfor rammerne af den til enhver tid gældende lovgivning og med respekt for forvaltningernes ansvar for varetagelse af deres respektive myndighedsopgaver og hensynet til forsvarlig forvaltning af kommunens opgaver i øvrigt.

1.2. Lovgrundlag

Regulativet respekterer den til enhver tid gældende lovgivning, herunder Lov om kommunernes styrelse (KSL), Styrelsesvedtægten for Københavns Kommune (KKSTV), databeskyttelsesforordningen og -loven samt forvaltningsretlige krav i øvrigt af betydning for informationssikkerheden og sikringen af borgernes rettigheder. På informationssikkerhedsområdet følges tillige principperne i ISO 27001-standardens.

1.3. Regelsættets opbygning

Regulativet indgår i det overordnede regelhierarki i Københavns Kommune som illustreret i figur 1 nedenfor.

STYRINGSDOKUMENT	STYRINGSMÆSSIGT INDHOLD	OPGAVEANSVARLIG	BESLUTNINGSKOMPETENCE	KOMMUNIKATION
Love og bekendtgørelser	Fastsætter de overordnede rammer for kommunens drift og tilrettelæggelse af faglige og administrative opgaver.	Ekstern	Folketinget	Implementeres i interne regler og via interne orientingsskrivelser
Styrelsesvedtægten for Københavns Kommune	Fastsætter de overordnede rammer for kommunens delegation af roller og ansvar til de stående udvalg, herunder formaliseres kommunens faglige organisering.	Borgerrepræsentationen	Borgerrepræsentationen med orientering til ekstern revision	Fælles portal + via interne orientingsskrivelser
Informationsikkerhedsregulativet inkl. bilag samt politikker og strategier	Fastsætter rammerne for forvaltning af kommunens informationsikkerhed og it med udgangspunkt i kommunens styrelsesvedtægt.	Økonomiforvaltningen	Borgerrepræsentationen	Fælles portal + via interne orientingsskrivelser
Fællesadministrative forretningscirkulærer	Definerer styringselementerne for kommunens administrative hovedprocesser med udgangspunkt i relevant faglig lovgivning og rammevilkårene i Informationsikkerhedsregulativet.	Økonomiforvaltningen	Økonomiudvalget	Fælles portal + via interne orientingsskrivelser
Fællesadministrative forretningsgange	Indeholder beskrivelse og kortlægning af de processer der defineres i cirkulæret, herunder en beskrivelse af aktiviteter samt dokumentation af risikovurdering. I forretningsgangen tages også stilling til fordeling af roller og ansvar.	Økonomiforvaltningen	Økonomiforvaltningen efter koordinering med It-kredsen	Fælles portal + via interne orientingsskrivelser
Forvaltningspecifikke forretningsgange	Indholdet defineres i de enkelte forvaltninger under hensyn til lovgivning og andre interne styringsdokumenter.	Fagforvaltningen	Forvaltningens direktion	Fælles portal + via interne orientingsskrivelser
Arbejdsgangsbeskrivelser, vejledninger mv.	Indeholder praktisk vejledning til udførelse af handlinger, herunder skærmpoint og detaljforklaring til de processer i de overliggende forretningsgange. I vejledningen uddybes beskrivelsen af roller og ansvar.	Fagforvaltningen	Ansvarlige kontorchef	Fælles portal + via interne orientingsskrivelser

Figur 1: Det overordnede regelhierarki i Københavns Kommune



Udmøntningen af informationssikkerhedspolitikken i kommunen sker inden for rammerne af Regulativet, tilhørende forretningscirkulærer samt fællesadministrative og forvaltningsspecifikke forretningsgange.

Forretningscirkulæernerne, fastsat i medfør af Regulativet, uddyber de overordnede regler og retningslinjer i forhold til et afgrænset område inden for informationssikkerhed-, persondatabeskyttelse- eller it-livscyklusområdet. Forretningscirkulæernerne uddyber rolle- og ansvarsfordelingen inden for forretningscirkulæerernes respektive områder.

Forretningsgange, herunder de fællesadministrative forretningsgange og de forvaltningsspecifikke forretningsgange fastlægger udførelsen af den praktiske opgaveløsning og kravene hertil. Udarbejdelsen og implementeringen af forretningsgangene skal følge den til enhver tid gældende kvalitetsstandard for dokumentation af forretningsgange i kommunen. Forretningsgange skal så vidt muligt understøttes af beskrevne processer, der fastlægger sammenhængen mellem aktiviteter, beslutninger og ansvarsplaceringen på organisationsneutrale roller. Hver rolle tilknyttes konkrete aktører, der svarer til den organisering, der er valgt i kommunen.

Arbejdsgangsbeskrivelser, vejledninger mv. supplerer eller udfolder forretningsgange, hvor det måtte være nødvendigt. For mindre opgaveområder kan der fastlægges retningslinjer for opgaveløsningen som erstatning for en forretningsgang.

1.4. Gyldighedsområde

Regulativet gælder for alle juridiske enheder under Københavns Kommune. Regulativets bestemmelser og underliggende regelsæt er minimumskrav til den data- og informationssikkerhed, der skal være etableret i alle kommunens enheder.

Styringsprincipperne, herunder rolle- og ansvarsfordelingen, omfatter også det pædagogiske it-område (PIT) i Børne- og Ungdomsforvaltningen.

1.5. Ajourføring

Økonomiforvaltningen har overfor Økonomiudvalget og Borgerrepræsentationen ansvar for vedligeholdelse og ajourføring af Regulativet gennem inddragelse af kommunens relevante tværgående fora, hvori alle forvaltninger er repræsenteret på direktionniveau. Regulativet skal som minimum gennemgås én gang årligt med henblik på en vurdering af eventuelle nødvendige tilpasninger. Resultatet af den årlige gennemgang forelægges for kredsen af Københavns Kommunes administrative direktører.

Forslag til ændringer af Regulativet forelægges af Økonomiforvaltningen for Økonomiudvalget og Borgerrepræsentationen til godkendelse. Forslag til ændringer af de underliggende tværgående forretningscirkulærer forelægges af Økonomiforvaltningen for Økonomiudvalget til endelig godkendelse.



Ansvar for forelæggelse til beslutning af ændringer og ajourføringer af Regulativet og de underliggende tværgående forretningscirkulærer sker således indenfor rammerne om ansvars – og rollefordelingen i KKSTV.

Redaktionelle ændringer, som ikke indebærer egentlige ændringer i Regulativet eller forretningscirkulærer, kan dog godkendes af Økonomiforvaltningens direktion. Tilsvarende gælder ændringer, der som følge af Borgerrepræsentationens beslutninger måtte indebære konsekvensrettelser i Regulativet eller i de underliggende forretningscirkulærer.

2. Habilitet og uafhængighed

De almindelige habilitetsregler for offentlig forvaltningsvirksomhed gælder for alle medlemmer af Borgerrepræsentationen og ansatte i Københavns Kommune. Det er et grundlæggende princip, at alle forvaltningsafgørelser og -beslutninger skal træffes alene ud fra saglige hensyn.

Modstridende funktioner og ansvarsområder skal, medmindre det ikke er muligt, adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af kommunens informationsaktiver. I tilfælde, hvor det er særligt vanskeligt eller uladsiggørligt at gennemføre egentlig funktionsadskillelse, skal andre sikkerhedsforanstaltninger iværksættes gennem overvågning af aktiviteter, tilsyn mv. Det er enhver leders ansvar at sikre funktionsadskillelse og tilsyn hermed.

Det er et grundlæggende krav, at kommunens Databeskyttelsesrådgiver er uafhængig og ikke må blive instrueret af andre om, hvordan denne skal udføre sine opgaver. Databeskyttelsesrådgiveren må således ikke modtage instruks, afskediges eller sanktioneres for at udføre sine lovpligtige opgaver og skal rapportere direkte til kommunens øverste politiske ledelsesniveau.

3. Styringsprincipper

I det følgende redegøres nærmere for rammerne for styringen og ledelsen af kommunens informationssikkerhed:

3.1. Ledelses- og beslutningshierarki

Den overordnede ansvars- og rollefordeling for varetagelsen af Københavns Kommunes opgaver er fastlagt i KSL og i KKSTV, der dermed tillige fastlægger den overordnede ansvars – og rollefordeling for varetagelsen af kommunens informationssikkerhed. Aktørerne i Københavns Kommunes ledelses- og beslutningshierarki har således alle et ansvar indenfor de overordnede områder 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus'.

De anførte 'Kredse' i Tabel 1 nedenfor er koordinerende uden formel beslutningskompetence i medfør af KKSTV.



De "Øvrige aktører" afleder deres kompetence i henhold til databeskyttelseslovgivningen, KSL og KKSTV.

Aktører - i hierarkisk orden	Kredse	Øvrige aktører
Borgerrepræsentationen Økonomiudvalget OB og Borgmestrene Økonomiforvaltningen Forvaltningsledelse	Kredsen af adm. direktører Økonomikredsen It-kredsen Digitaliseringschefkredsen Legal Compliance Forum	Datatilsynet Databeskyttelsesrådgiver Lovpligtige revision DPO Business Partner Intern revision

Tabel 1: Aktører i ledelses- og beslutningshierarkiet for varetagelse af kommunens informationssikkerhedsmæssige opgaver

Beslutninger og varetagelse af kommunens informationssikkerhedsopgaver- og forhold samt opgavevaretagelse i forhold til databeskyttelse og it-livscyklus følger kommunens normale ansvars- og beslutningsprocesser inden for rammerne af kommunens styreform som fastlagt i KKSTV.

Styringsprincip

Ved udarbejdelse af forretningscirkulærer og forretningsgange inden for områderne 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus' samt ved efterlevelsen heraf skal kommunens overordnede ledelses- og beslutningshierarki, jf. KKSTV, iagttages.

3.2. Rolle- og ansvarsfordeling

Borgerrepræsentationen vedtager kommunens informationssikkerhedspolitik og -regulativ efter anbefaling fra Økonomiudvalget på grundlag af indstilling fra Økonomiforvaltningen.

Økonomiudvalget varetager den umiddelbare forvaltning af Københavns Kommunes overordnede og tværgående it-forhold, jf. Københavns Kommunes styrelsesvedtægt § 12, stk. 6, 3. pkt.

Økonomiudvalget varetager således - herunder ved delegation til Økonomiforvaltningen med underliggende enheder - bl.a. ansvaret for:

- It-systemer, som understøtter opgavevaretagelsen på tværs af kommunens forvaltninger (fællessystemer og infrastruktur).
- Kommunens overordnede og tværgående informationssikkerhed
- It-sikkerhedsfunktionen i kommunen.
- Udarbejdelse og vedligeholdelse af kommunens informationssikkerhedsbestemmelser.
- Tilsyn med overholdelse af kommunens informationssikkerhedsbestemmelser.
- It-sikkerhedsvurderinger af fællessystemer, fagsystemer og it-infrastruktur.
- At medarbejdere, som varetager it-opgaver inden for Økonomiudvalgets ansvarsområder, har de nødvendige kompetencer.



Overborgmesteren og borgmestrene varetager inden for hver deres udvalgsområde ansvaret for den øverste daglige administrative ledelse, jf. KKSTV § 11. Den øverste daglige administrative ledelse varetages af borgmestrene med ansvar overfor Økonomiudvalget. Med ansvaret følger, at overborgmesteren og borgmestrene, herunder de enkelte forvaltninger, inden for hver deres udvalgsområde bl.a. har ansvaret for:

- It-systemer (fagsystemer), som specifikt understøtter forvaltningens opgavevaretagelse.
- At fastlæggelsen af informationssikkerhedsniveauet i egen forvaltning sker inden for rammerne af kommunens overordnede og tværgående bestemmelser vedr. kommunens informationssikkerhedsniveau samt med ansvar for, at forvaltningens informationssikkerhedsniveau ikke indebærer risiko for negativ påvirkning af kommunens samlede risiko på tværs af forvaltningerne.
- At forvaltningens behandling af personoplysninger efterlever den til enhver tid gældende lovgivning, herunder databeskyttelseslovgivningen og kommunens fastsatte rammer og retningslinjer herfor, herunder bl.a. kravene til dokumentation, jf. afsnit 3.5.
- At der i forbindelse med samarbejde med eksterne parter i nødvendigt omfang er indgået databehandleraftaler i overensstemmelse med kommunens fælles standardskabelon herfor, jf. afsnit 3.6.
- At der i hver forvaltning er udpeget en DPO Business Partner som kontaktperson til kommunens Databeskyttelsesrådgiver, jf. afsnit 4.
- At der gennemføres risikovurderinger, jf. afsnit 3.4, inden for forvaltningens egne ansvarsområder under iagttagelse af, at forvaltningens eget risikoniveau ikke må indebære risiko for negativ påvirkning af kommunens samlede risiko på tværs af forvaltningerne.
- At forvaltningens medarbejdere, som behandler personoplysninger og arbejder med it-systemer inden for forvaltningens egne ansvarsområder, har de nødvendige kompetencer og viden om persondata og informationssikkerhed, jf. afsnit 3.3.

Om Databeskyttelsesrådgiverens ansvarsområder henvises til afsnit 4.

Den nærmere beskrivelse af roller og ansvar inden for områderne 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus' fastsættes i forretningscirkulæreform.

Styringsprincip

Ved udmøntning og præcisering af roller og ansvar i forretningscirkulærer og forretningsgange samt ved efterlevelsen heraf skal den konkrete rolle- og ansvarsfordeling være entydigt fastsat inden for rammerne af KKSTV.

3.3. Ressourcer og kompetencer

Overborgmesteren og borgmestrene har indenfor hver deres udvalgsområde ansvar for at sikre tilstrækkelige og uddannede ressourcer til opfyldelse af vision, strategi og mål i kommunens informationssikkerhedspolitik. De har endvidere ansvar for, at sammensætningen af allokerede ressourcer og deres



kompetencer sikrer udmøntningen af alle elementer i Regulativet samt underliggende forretningscirkulærer og forretningsgange.

Ansvaret indebærer, at der i forvaltningerne løbende sikres en bevidsthed om databeskyttelse, it-sikkerhed og øvrige forhold i relation til informationsikkerhed, således at kendskabet og forståelsen for områderne er en naturlig del af medarbejdernes adfærd.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at sikre tilstrækkelige og uddannede ressourcer. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang fastsættes bestemmelser om nødvendige kompetencer.

3.4. Risikovurderinger

Københavns Kommune foretager risikovurderinger for at sikre opfyldelsen af vision, strategi og mål i kommunens informationsikkerhedspolitik.

Risikovurderinger skal f.eks. foretages ved iværksættelse af enhver ny behandling af personoplysninger og ved ændringer i behandlingen samt ved indførelse og væsentlige ændringer af it-systemer og infrastruktur. Vurderingerne skal være relevante og kvalificerede i forhold til det vurderede område. Heri ligger blandt andet:

- At vurderingerne i nødvendigt omfang skal tage afsæt i anerkendte, standardiserede og vedtagne principper for risikovurderinger, tilpasset det pågældende område og under hensyntagen til, at det i nødvendigt omfang skal være muligt at sammenholde og sammenligne risikoniveauet på tværs af forvaltninger.
- At vurderingerne skal udføres af kvalificerede medarbejdere.
- At omfanget af risikovurderinger skal være proportionalt med det vurderede områdes betydning.
- At den foretagne risikovurdering dokumenteres.
- At risikovurderinger foretages med den fornødne frekvens, og at det i relevant omfang er muligt at følge risikoudviklingen over tid.

Styringsprincip

Ved udarbejdelse af forretningscirkulærer og forretningsgange i medfør af Regulativet, skal der i nødvendigt omfang fastsættes nærmere bestemmelser om risikovurderinger.

3.5. Dokumentation

Alt dokumentation skal opfylde indholdsmæssige og formmæssige krav til registrering, dokumentudformning mv., som nærmere fastsat i Regulativets underliggende forretningscirkulærer og bestemmelser, herunder i forretningscirkulæret for persondatabeskyttelse - dokumentation og compliance.



I forhold til databeskyttelse og informationsaktiver skal navnlig væsentlige dispositioner, hændelser, aktiver og beslutninger dokumenteres. Det er eksempelvis i form af instrukser, processer, kontraktuelle forhold, beslutningsnotater, business cases, infrastrukturtegninger og systemdokumentation, risikovurderinger, beskrivelse af brugeradministration og adgangsstyring mv.

I forhold til databeskyttelsen skal der endvidere foreligge særlig dokumentation i form af kommunens fortegnelse over behandlinger af personoplysninger, datastrømme mv., som fastsat i Regulativets underliggende regelsæt.

I forhold til dokumentation af samarbejdet med eksterne parter skal evt. særlige behov for dokumentation opfyldes, jf. afsnit 3.6.

Styringsprincip

Inden for Regulativets områder har alle forvaltninger ansvar for at sikre den fornødne dokumentation. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang fastsættes nærmere bestemmelser om dokumentation.

3.6. Styring af eksterne parter

Aftaler med eksterne parter skal, medmindre særlige forhold gør sig gældende, opfylde kravene i Københavns Kommunes fælles standardskabeloner for databehandleraftaler og skal i nødvendigt omfang være kvalitetssikret af medarbejdere med henholdsvis juridisk, faglig og teknisk kompetence inden for det givne aftalefelt.

Der skal i nødvendigt omfang ske en løbende opfølgning og tilsyn med det aftalte samarbejde. Såfremt der ikke kan træffes aftale om kommunens eget tilsyn af eksterne parter, kan det efter en risikobaseret vurdering være nødvendigt at indgå aftale om periodisk indhentelse af revisorerklæring.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at sikre den fornødne styring af eksterne parter. Aftaler med eksterne parter skal, medmindre særlige forhold gør sig gældende, opfylde kravene i Københavns Kommunes fælles standardskabeloner for databehandleraftaler.

3.7. Tilsyn

Tilsyn foretages ud fra en risikobaseret tilgang. Tilsynet varetages og gennemføres af følgende relevante aktører i Københavns Kommune:

- Forvaltningerne: forvaltningernes respektive direktioner og ledere har ansvaret for gennemførelse af ledelsestilsyn i forvaltningernes enheder med henblik på sikring af forvaltningernes egenkontrol i relation til medarbejderadfærd, funktionsadskillelse, informationsikkerhed og databeskyttelse.



- Databeskyttelsesrådgiveren: fører med reference direkte til Borgerrepræsentationen et uafhængigt tilsyn med kommunens håndtering af persondata, herunder varetagelsen af ansvaret for og styringen af området, lovmedholdelighed og egenkontrol med henblik på at understøtte, at kommunen overholder de gældende databeskyttelsesretlige regler.
- Borgerrepræsentationen og Økonomiudvalget: har det overordnede ansvar for informationssikkerhed og datasikkerhed i Københavns Kommune og skal således overordnet sikre, at det nødvendige tilsyn på området gennemføres.
- Lovpligtig revision: Fører som led i den lovpligtige revision uafhængigt af Borgerrepræsentationen kontrol med kommunens informationssikkerhed, jf. KSL § 42.

Inden for områderne 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus' skal tilsynsemner og tilsynsmål afstemmes således, at det samlede tilsyn for kommunen er dækkende, tilstrækkeligt og effektivt. Tilsynet skal tilrettelægges ud fra en risikobaseret tilgang og i sammenhæng med kommunens aktuelle risikoniveau.

Ved tilrettelæggelse og gennemførelse af tilsyn skal det sikres:

- At tilsynet følger etablerede og fastlagte processer, forretningsgange mv.
- At de udførende medarbejdere har det nødvendige kendskab til gennemførelse af tilsyn.
- At tilsynet reelt fungerer.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at gennemføre fornødne ledelsestilsyn. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang været taget stilling til behovet og gennemførelse af tilsyn.

3.8. Rapportering

Brud på persondatasikkerheden skal, i overensstemmelse med databeskyttelsesforordningens bestemmelser herom, rapporteres til Datatilsynet inden for 72 timer efter, at forvaltningen er blevet bekendt med bruddet.

Relevante afvigelser på områderne 'informationssikkerhed', 'persondatabeskyttelse' og 'it-livscyklus' skal afrapporteres i overensstemmelse med kommunens ledeshierarki samt i overensstemmelse med Regulativets underliggende regelsæt.

Rapportering er navnlig relevant i forhold til ændringer af væsentlig økonomisk betydning, et øget risikoniveau, sikkerhedshændelser og persondata-brud.



Nærmere regler for afrapportering kan fastlægges i medfør af Regulativet med henblik på, at beslutningstager eller andre aktører bedst muligt kan varetage sine ansvarsområder på et rettidigt og oplyst grundlag.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at sikre den fornødne rapportering. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang fastsættes bestemmelser om rapportering.

3.9. Hændelsesforanstaltninger

Som følge af tilsyn, risikovurderinger, sikkerhedshændelser eller andre identificerede u hensigtsmæssige forhold, der truer informationssikkerheden, skal der iværksættes og dokumenteres foranstaltninger, der nedsætter eller eliminerer konsekvenserne af de u hensigtsmæssige forhold. Såfremt der træffes beslutning om kun delvist at eliminere u hensigtsmæssige forhold, skal dette følges af en ledelsesbeslutning på direktionniveau, med begrundelse for beslutningen. I de tilfælde Regulativets underliggende regelsæt tilsiger det, vil Økonomiforvaltningen være forpligtet til at forelægge beslutninger herom for Økonomiudvalget. Forelæggelsen følger den normale praksis i Københavns Kommune.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at iværksætte fornødne hændelsesforanstaltninger. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang fastsættes bestemmelser om hændelsesforanstaltninger.

3.10. Databeskyttelse og registreredes rettigheder

Københavns Kommune skal opretholde et teknisk og organisatorisk forsvarligt sikkerhedsniveau, hvor kommunen bl.a. skal følge principperne for databeskyttelse gennem design og standardindstillinger af hensyn til informationsikkerheden samt sikre registreredes rettigheder og data.

I tilknytning hertil vil sikringen af den registreredes rettigheder i medfør af bestemmelserne på det persondatarelige område være udmøntet i forretningscirkulærer og i nødvendigt omfang fællesobligatoriske forretningsgangsbeskrivelser.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at varetage den fornødne databeskyttelse mv. Ved udarbejdelse af forretningscirkulærer og forretningsgangsbeskrivelser skal der i relevant omfang fastsættes bestemmelser om databeskyttelse mv.

3.11. Beredskabsplaner



Der skal foreligge opdaterede beredskabsplaner for alle forvaltninger, herunder for alle relevante systemer i Københavns Kommunes enheder, der behandler person- og værdioplysninger, der kan blive ramt af forhold, der aktiverer beredskabet. Planerne skal baseres på en vurdering af kritikalitet og skal løbende opdateres samt testes med en relevant frekvens.

Styringsprincip

Alle forvaltninger har inden for egne ansvarsområder i medfør af Regulativet ansvar for at udarbejde og opdatere beredskabsplaner. Ved udarbejdelse af forretningscirkulærer og forretningsgange skal der i relevant omfang fastsættes bestemmelser om beredskabsplaner.

4. Databeskyttelsesrådgiveren

Databeskyttelsesrådgiverens rolle og opgaver er fastsat i databeskyttelseslovgivningen med Justitsministeriets og Datatilsynets tilhørende vejledninger. Databeskyttelsesrådgiveren er en i kommunen uafhængig funktion, der fungerer som kommunens rådgiver og tilsynsfunktion på området og skal inddrages og rådføres om overholdelse af de databeskyttelsesretlige regler.

Databeskyttelsesrådgiverens opgaver er i hovedtræk følgende:

- Underrette og rådgive om databeskyttelse. Det indebærer konkret rådgivning om beskyttelse af personoplysninger i Københavns Kommune, herunder hvordan lovmedholdelighed mv. sikres i forbindelse med indkøb af nye it-systemer, kravspecifikationer til leverandører, udarbejdelse af datapolitikker mv. samt stå til rådighed for ledelsen vedrørende spørgsmål om datasikkerhed.
- Modtage underretninger og yde rådgivning i forbindelse med sikkerhedshændelser med indflydelse på personoplysninger og derefter rådgive i forbindelse med potentielle eller konkrete sikkerhedsbrud.
- Overvåge overholdelsen af de databeskyttelsesretlige regler i kommunen. Det indebærer bl.a. at overvåge kommunens politikker om databeskyttelse, uddannelsen af personale i databeskyttelse, oplysningskampanjer, fordeling af ansvar og revisioner etc.
- Databeskyttelsesrådgiveren skal rådgive ved udarbejdelse af konsekvensanalyser vedrørende databeskyttelse, når der anmodes herom, samt overvåge deres opfyldelse.
- Inddragelse forud for udstedelse af retningslinjer og procedurer for, hvordan de databeskyttelsesretlige regler skal overholdes i kommunen herunder informationssikkerhedspolitik, -regulativ, forretningscirkulærer, processer og forretningsgange mv.
- Samarbejde med Datatilsynet på kommunens vegne.
- Agere som kontaktpunkt for Datatilsynet angående alle spørgsmål om behandling af personoplysninger i kommunen, herunder:
 - hvis en behandling af personoplysninger vil medføre en høj risiko, der kræver, at Datatilsynet høres forinden iværksættelsen af behandlingen.
 - hvor sager om kommunens behandling af personoplysninger indbringes for Datatilsynet.
- Vejlede den registrerede:



- angående den registreredes rettigheder ved behandling af personoplysninger.
- ved at besvare spørgsmål om behandling af personoplysninger. Kommunen skal bistå samt stille ressourcer og informationer til rådighed ved bl.a. at besvare henvendelser om, hvordan den registreredes oplysninger behandles.
- Aflægge årlig statusrapport i oktober til Borgerrepræsentationen.
- Ved særlige hændelser og/eller brud på datasikkerheden afrapporterer Databeskyttelsesrådgiveren til Borgerrepræsentationen.

5. Udmøntning og drift

Udmøntning af Regulativet sker gennem en række underliggende forretningscirkulærer, der fastlægger de bindende retningslinjer på Regulativets tre hovedområder:

- Informationssikkerhed.
- Persondatabeskyttelse.
- It-livscyklus.

Det finder sted i form af følgende 6 forretningscirkulærer:

- Forretningscirkulæret for persondatabeskyttelse - registreredes rettigheder.
- Forretningscirkulæret for persondatabeskyttelse - dokumentation og compliance.
- Forretningscirkulæret for informationssikkerhed.
- Forretningscirkulæret for organisering af informationssikkerhed.
- Forretningscirkulæret for it-anskaffelser.
- Forretningscirkulæret for it-drift, -vedligehold og -udfasning.

6. Ikrafttrædelse

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