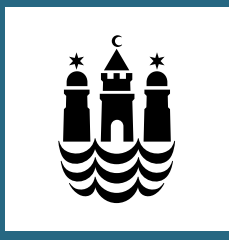
BILAG 4

KØBENHAVNS KOMMUNE

FORRETNINGSCIRKULÆRE FOR PERSONDATABESKYTTELSE DOKUMENTATION OG COMPLIANCE



UDKAST, AUGUST 2018

INDLEDNING

Forretningscirkulæret for **Dokumentation og Compliance** har til formål at sætte rammerne for sikring og dokumentation af Københavns Kommunes behandling af personoplysninger, herunder for implementering, ændringer og vedligeholdelse af alle behandlingsprocesser og datastrømme. Sammen med de underliggende forretningsgange er forretningscirkulæret for Dokumentation og Compliance rammesættende for samarbejdet på tværs af kommunens enheder.

Forretningscirkulæret for Dokumentation og Compliance er udarbejdet i henhold til Informationssikkerhedsregulativet for Københavns Kommune og visionen om: *Lovlig forvaltningsvirksomhed og tryghed for borgerne og virksomhederne i mødet med Københavns Kommune.*

Forretningscirkulæret for Dokumentation og Compliance er bindende og dermed obligatorisk at følge for alle kommunens forvaltninger og underliggende enheder samt kommunens uafhængige enheder. Den enkelte forvaltning/enhed har overfor den administrativt ansvarlige borgmester og Økonomiudvalget ansvaret for, at forretningscirkulæret efterleves i den pågældende enhed.

Forretningscirkulæret for Dokumentation og Compliance indgår i det overordnede regelhierarki i Københavns Kommune som illustreret i figuren nedenfor.

STYRINGSDOKUMENT	STYRINGSMÆSSIGT INDHOLD	OPGAVEANSVARLIG	BESLUTNINGS-KOMPETENCE	KOMMUNIKATION
Love og bekendtgørelser	Fastsætter de overordnede rammer for kommunens drift og tilrettelæggelse af faglige og administrative opgaver.	Eksternt	Folketinget	Implementeres i interne regler og via interne orienteringsskrivelser
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 orienteringsskrivelser
Informationssikkerheds-regulativet inkl. bilag samt politikker og strategier	Fastsætter rammerne for forvaltning af kommunens informationssikkerhed og it med udgangspunkt i kommunens styrelsesvedtægt.	Økonomiforvaltningen	Borgerrepræsentationen	Fælles portal + via interne orienteringsskrivelser
Fællesadministratve forretningscirkulærer	Definerer styringselementerne for kommunens administrative hovedprocesser med udgangspunkt i relevant faglig lovgivning og rammevilkårene i Informationssikkerhedsregulativet.	Økonomiforvaltningen	Økonomiudvalget	Fælles portal + via interne orienteringsskrivelser
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 orienteringsskrivelser
Forvaltningsspecifikke forretningsgange	Indholdet defineres i de enkelte forvaltninger under hensyn til lovgivning og andre interne styringsdokumenter.	Fagforvaltningen	Forvaltningens direktion	Fælles portal + via interne orienteringsskrivelser
Arbejdsgangs-beskrivelser, vejledninger mv.	Indeholder praktisk vejledning til udførelse af handlinger, herunder skærmprint og detailforklaring til de processer i de overliggende forretningsgange. I vejledningen uddybes beskrivelsen af roller og ansvar.	Fagforvaltningen	Ansvarlige kontorchef	Fælles portal + via interne orienteringsskrivelser

Figur 1: Regelhierarki for Københavns Kommune

INDHOLD

PERSONDATABESKYTTELSE – DOKUMENTATION OG COMPLIANCE

Persondatabeskyttelse defineres som kommunens beskyttelse af almindelige, almindelige-fortrolige og følsomme personoplysninger, som kommunen modtager, behandler, opbevarer og videregiver.

Forretningscirkulære for "Persondatabeskyttelse - Dokumentation og Compliance" er et sæt regler for, hvordan kommunen:

1. Håndterer implementering, ændringer eller udfasning af behandlingsprocesser og underliggende datastrømme,
2. Håndterer vedligeholdelse af dokumentationen af behandlingsprocesser og datastrømme, der dokumenterer kommunens behandling af personoplysninger og sikrer den lovpligtige fortegnelse,
3. Sikrer at håndteringen af personoplysninger i driftssituationer lever op til krav i lovgivningen mv.,
4. Sikrer tilstrækkelig tværgående indsigt, overvågning og styring af compliancenivauet hos den dataansvarlige (forvaltningerne),
5. Sikrer et gensidigt værdiskabende samarbejde med Databeskyttelsesrådgiveren og dennes funktion.

Håndtering af registreredes rettigheder dækkes ikke af dette forretningscirkulære, men af Forretningscirkulæret om Persondatabeskyttelse - Registreredes rettigheder.

HOVEDPROCES

Forretningscirkulæret for Dokumentation og Compliance under hovedprocessen "Persondatabeskyttelse" regulerer følgende fællesadministrative delprocesser:

- Tilgang / afgang og ændringer i behandlingsprocesser og datastrømme.
- Vedligeholdelse af dokumentation af behandlingsprocesser og datastrømme
- Personoplysninger, håndtering i drift
- Compliance hos den dataansvarlige (forvaltningerne)
- Databeskyttelsesrådgiveren

AKTØRER

Med dette forretningscirkulære fastsættes en rolle- og ansvarsfordeling for aktiviteter ift. dokumentation og compliance. Aktørernes ansvar og forpligtelser er beskrevet herunder og gælder for aktiviteter i forretningscirkulæret, hvor de er angivet.

Udførende – De(n) aktør(er), som i praksis udfører på aktiviteten.

Ansvarlig - Den aktør, som i sidste ende har ansvaret for, at aktiviteten udføres.

Rådgivende - De(n) aktør(er), som de(n) udførende skal rådføre sig med ift. den konkrete aktivitet. Det fremgår af afsnitsteksten i det konkrete afsnit, hvorvidt udførende har pligt til at rådføre sig med de(n) rådgivende ved en angivelse af, hvorvidt aktiviteten udføres i samarbejde med de(n) rådgivende.

Informeret - De(n) aktør(er), som altid skal informeres om væsentlige afvigelser i udførelsen af aktiviteten.

Det beskrives nærmere i de angivne forretningsgange, hvorledes dette i praksis gøres.

0. GENERELT

0.1. Lov- og regelgrundlag for Persondatabeskyttelse – Dokumentation og Compliance

Det er vigtigt, at gældende lovgivning overholdes, herunder lovgivningen om behandling og dokumentation af personoplysninger samt Københavns Kommunes gældende Informationssikkerhedsregulativ med underliggende forretningscirkulærer overholdes.

Økonomiudvalget/Økonomiforvaltningen varetager den umiddelbare forvaltning af kommunens overordnede og tværgående it-forhold, jf. § 12, stk. 6, pkt. 3 i Styrelsesvedtægten for Københavns Kommune. Overborgmesteren og borgmestrene har over for Økonomiudvalget det overordnede daglige administrative ansvar inden for hver deres udvalgsområde for blandt andet it- og datasikkerhedsopgaven. It-kredsen, der er nedsat på tværs af forvaltningerne, er koordinerende uden formel beslutningskompetence.

Den behandlende forvaltning/enhed har over for den respektive borgmester ansvaret for, at behandlingen og dokumentationen mv. af personoplysninger overholder den til enhver tid gældende lovgivning, herunder særligt:

- EU-Databeskyttelsesforordningen
- Databeskyttelseslovgivningen
- Særlovgivningens regler vedr. håndtering og beskyttelse af personoplysninger
- Kommunens øvrige interne regler for informationssikkerhed herunder blandt andet principperne om konsekvensanalyser, der vurderer persondatabeskyttelse gennem design og standardindstillinger i forbindelse med eksisterende og nye systemer

Databeskyttelsesrådgiveren kan til hver en tid kontaktes med spørgsmål og rådgivning i forhold til fortolkning og praktisk udmøntning af Databeskyttelseslovgivningen samt med anbefalinger til ledelsesmæssige beslutninger.

Tabel 1: Ansvars- og rollefordeling ift. "Lov- og regelgrundlag for Compliance"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikre fastholdelse og effektivitet i kommunens tværgående beskyttelsesniveau	ØKF og LCF samt It-kredsen og 7 Dir	Økonomiudvalget	DPO BP og efterfølgende Databeskyttelses-rådgiveren	-
Sikre overholdelse af lov- og regelgrundlag pr.	Den enhed hvor personoplysninger	Respektive borgmestre	DPO BP og efterfølgende	-

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
forvaltning	håndteres		Databeskyttelses-rådgiveren	

0.2. Retningslinjer

Formålet med fælles regelsæt, herunder fælles retningslinjer, er, at sikre at Københavns Kommune på tværs af kommunen har et vedvarende, ensartet og passende niveau for lovmedholdelighed, fortrolighed, integritet og tilgængelighed, når kommunen modtager, behandler, opbevarer og transmitterer personoplysninger.

Økonomiforvaltningen har, efter koordinering med It-kredsen, ansvaret for at fastsætte, hvilke retningslinjer, som anvendes i Københavns Kommune under hensyntagen til nationale og sektorspecifikke standarder.

Økonomiforvaltningen har ligeledes, efter koordinering med It-kredsen, ansvaret for at beslutte, i hvilken enhed ejerskabet for den pågældende retningslinje er placeret.

Den enhed under Økonomiforvaltningen som har ansvaret for de pågældende retningslinjer er ansvarlig for, at de besluttede retningslinjer udarbejdes i samarbejde med øvrige relevante enheder i kommunen. Den enhed under Økonomiforvaltningen skal rettidigt inddrage Databeskyttelsesrådgiveren forud for udstedelse af retningslinjer for, hvordan databeskyttelsesretlige regler skal overholdes i organisationen.

Den ansvarlige enhed har ligeledes ansvaret for at sikre, at retningslinjer til enhver tid er opdaterede og tilgængelige. Økonomiforvaltningen beslutter efter koordinering med It-kredsen, hvordan disse tilgængeliggøres med henblik på at sikre kendskabet.

Den ansvarlige enhed er forpligtet til at yde vejledning og rådgivning i de pågældende retningslinjer.

Fastsatte retningslinjer, der er koordineret med Legal Compliance Forum og/eller It-kredsen er obligatoriske at følge. Såfremt en forvaltning / enhed ønsker at fravige en given retningslinje, skal sagen forelægges for Økonomiforvaltningen, som efter koordinering Legal Compliance Forum og/eller It-kredsen, har ansvaret for at beslutte muligheder for evt. dispensation herfra, samt skriftligt at begrunde dette overfor Databeskyttelsesrådgiver jf. bestemmelserne i databeskyttelseslovgivningen.

Tabel 2: Ansvars- og rollefordeling ift. "Retningslinjer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Aftale retningslinjer	ØKF/It-kredsen	Økonomiudvalget	Databeskyttelses-rådgiver	Digitaliserings-kontorer, Legal Compliance Forum og Koncern IT
Udarbejde retningslinjer	Udpegede ansvarlige enhed	Den ansvarlige enheds direktion	Databeskyttelses-rådgiver	Digitaliserings-kontorer, Legal Compliance Forum

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
				og Koncern IT
Yde rådgivning og vejledning i retningslinje	Udpegede ansvarlige enhed	Den ansvarlige enheds direktion	Databeskyttelses-rådgiver	-
Tilgængeliggørelse og sikring af kendskab	ØKF/It-kredsen	Økonomiudvalget	Databeskyttelses-rådgiver	Digitaliserings-kontorer, Legal Compliance Forum og Koncern IT

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

0.3. Organisering af databeskyttelsesarbejdet

I Københavns Kommune er samarbejdet, opgave- og ansvarsfordeling i forbindelse med databeskyttelsesarbejdet organiseret i forhold til de niveauer, der dokumenterer kommunens behandlingsprocesser og datastrømme. Dette skal sikre et fuldstændigt og entydigt ejerskab og dermed medvirke til at sikre håndteringen af personoplysninger og dokumentationen heraf.

Databeskyttelsesrådgiveren er en uafhængig funktion i kommunen, der fungerer som kommunens rådgiver og tilsynsfunktion på området og skal inddrages og rådføres om overholdelse af de databeskyttelsesretlige regler. Databeskyttelsesrådgiverens ansvar fremgår af Informationssikkerhedsregulativet og den praktiske opgaveudførelse af efterfølgende afsnit i nærværende cirkulære.

DPO Business Partner og dennes stedfortræder er kontaktpunkt til Databeskyttelsesrådgiveren og er forvaltningernes (dataansvarlig) vidensperson indenfor databeskyttelsesområdet. DPO Business Partneren skal til stadighed vurdere complianceniveauet i forvaltningen og skal gennem en direkte adgang til forvaltningens ledelse underrette om dette. Endvidere skal DPO Business Partneren proaktivt arbejde for, at forvaltningens complianceniveau lever op til lovgivning og regler gennem rådgivning af og samarbejde med forvaltningens medarbejdere. Desuden skal DPO Business Partneren proaktivt samarbejde og vidensdele med kommunens andre forvaltninger blandt andet gennem Business Partner Forum for at sikre et optimalt complianceniveau for kommunen som helhed.

Behandlingsprocesansvarlige er kontaktpunkt til DPO Business Partner i de enkelte forvaltninger. I forhold til forvaltningens ansvar som dataansvarlig og ansvarlig for databehandlere, er den behandlingsprocesansvarlige nøglemedarbejder og vidensperson på den behandlingsproces, vedkommende har ansvaret for inklusiv fuldstændigheden af de underliggende datastrømme. Behandlingsprocesansvarlig ved, hvad der indgår i processen, og hvilken betydning, dette har i relation til databeskyttelse og lovgivning herfor. Behandlingsprocesansvarlige er ansvarlig for, at dokumentationen til stadighed er korrekt/opdateret i Pactius, herunder er i overensstemmelse med lovgivning mv. (altså hvad kommunen skal og må med personoplysninger) og faktiske forhold. Det påhviler den enkelte medarbejder og linjeleder at sikre, at behandlingsprocessen udføres, som den er dokumenteret.

Datastrømsansvarlige er kontaktpunkt til Behandlingsprocesansvarlig og nøglemedarbejder og vidensperson på de givne datastrømme, som vedkommende har ansvaret for. Dette inkluderer sikring af, at der forefindes en databehandleraftale, samt at denne er uploadet ved datastrømmen. Datastrømsansvarlig ved, hvad der indgår i datastrømmen, og hvilken betydning, dette har i relation til databeskyttelse og lovgivning herfor. Datastrømansvarlig er ansvarlig for at dokumentationen til stadighed er korrekt/opdateret, herunder er i overensstemmelse med lovgivning mv. og faktiske forhold. Det påhviler den enkelte medarbejder og linjeleder at sikre, at datastrømmen udføres, som den er dokumenteret.

Tabel 3: Ansvars- og rollefordeling ift. "Organisering af databeskyttelsesarbejdet"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udpegning af DPO Business Partner & stedfortræder	Respektive direktioner	Respektive borgmestre	Databeskyttelses-rådgiver	Legal Compliance Forum og It-kredsen

0.4. Uenigheder

Uenigheder vedrørende tolkning og/eller udmøntning af lovgivning eller regler om persondatabeskyttelse i en forvaltning mellem forvaltninger eller i Københavns Kommunes tilstræbes løst i det tværgående compliancearbejde. Kan enighed ikke opnås kan uenigheden eskaleres til Legal Compliance Forum, herefter Legal Compliance Forum og dernæst It-kredsen – for Økonomiforvaltningen, der efter inddragelse af de involverede forvaltningers administrerende direktører og borgmestre i givet fald forelægger sagen for Økonomiudvalget til beslutning. Eskalering kan foretages, medmindre det ikke er lykkedes at opnå enighed blandt de involverede parter, evt. ved inddragelse af kredse eller kommunens Databeskyttelsesrådgiveren.

Den overordnede ansvars- og rollefordeling for varetagelsen af Københavns Kommunes opgaver er fastlagt i Lov om kommunernes styrelse og i Styrelsesvedtægten for Københavns Kommune, 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 inden for informationssikkerheds-, databeskyttelses- og it-livscyklusområdet.

De anførte kredse i Tabel 4 nedenfor er koordinerende uden formel beslutningskompetence i medfør af Styrelsesvedtægten for Københavns Kommune.

De "Øvrige aktører" i Tabel 4 nedenfor afleder deres kompetence i henhold til Databeskyttelseslovgivningen, Lov om kommunernes styrelse og Styrelsesvedtægten for Københavns Kommune.

Tabel 4: Aktører i ledelses- og beslutningshierarkiet for varetagelse af kommunens informationssikkerhedsmæssige opgaver

Aktører (hierarkisk)	Kredse	Øvrige aktører
Borgerrepræsentationen	Kredsen af adm. Direktører	Datatilsynet
Økonomiudvalget	Økonomikredsen	Datebeskyttelsesrådgiver

Aktører (hierarkisk)	Kredse	Øvrige aktører
OB og Borgmestrene	It-kredsen	Lovpligtig revision
Økonomiforvaltningen	Legal Compliance Forum	DPO Business Partner
Forvaltningsledelse		Intern revision

Den beskrevne beslutningsvej gælder endvidere for alle uenigheder, som måtte opstå ifm. enhver aktivitet beskrevet i dette forretningscirkulære.

Herom gælder følgende forretningsgange:

- *Herom gælder arbejdsgange for indstilling af sager til pågældende kreds eller aktør*

1. TILGANG, AFGANG, ÆNDRINGER I BEHANDLINGSPROCESSER ELLER DATASTRØMME

1.1. Initiering, juridisk vurdering og implementering af forandringer

Informationerne i kommunens behandlingsprocesser og datastrømme er grundlaget for compliancestatus og en længere række aktiviteter, som GAP analyser, vurdering af tilsyns- og rådgivningsindsatser, grundlag for risikoprofiler og konsekvensanalyser mv. Desuden danner informationerne grundlag for den lovpligtige fortegnelse, den overordnede oplysningspligt, besvarelse af indsigtsanmodninger og meget mere. Derfor skal indholdet i registreringer af behandlingsprocesser og datastrømme til stadighed vedligeholdes.

Hver forvaltning skal tilrettelægge processer og forretningsgange, der sikrer, at forvaltningens behandlingsprocesser og underliggende datastrømme til stadighed overvåges, vurderes og er implementeret, så de efterlever formål og gældende lovgivning.

Forvaltningerne gør dette ved at identificere, hvilke forhold i den daglige drift, der initierer at en behandlingsproces og/eller en datastrøm ændrer sig, eksempelvis ved ændring af lovgrundlag, nye forvaltningsaktiviteter, organisationsændringer, ændringer i eller nye systemer etc. Identifikationen kan tillige ske gennem GAP analyser i dokumentationssystemet (Pactius).

Det kan være proaktive overvågningsaktiviteter for at følge den løbende vurdering og vedligeholdelse, eller reaktive aktiviteter som følge af henvendelser fra organisationen.

I tilknytning til identifikationen af en tilgang, afgang eller ændringer i behandlingsprocesser og/eller datastrømme skal der foretages en juridisk vurdering til sikring af, at behandlingsprocessen og de underliggende datastrømme er lovlige, samt at alle registreringerne i Pactius Privacy stemmer overens med den faktiske behandling af personoplysningerne. Eksempelvis hvis formålet med en behandling ændrer sig, skal der fortages en juridisk vurdering af hvilket regelgrundlag, der herefter skal lægges til grund for behandlingen.

Hvis lovgrundlaget ændrer sig, er det så fortsat de samme regler for behandling, typer af personoplysninger mv., der kan anvendes.

De medarbejdere/brugere, der har adgang til og/eller behandler de berørte personoplysninger i praksis skal informeres og instrueres, såfremt ændringerne har betydning for den måde, personoplysningerne må behandles på.

Information om og betydningen af tilgang, afgang eller ændringer i behandlingsprocesser og/eller datastrømme skal desuden formidles til relevante parter hos forvaltningen, til andre forvaltninger, til koncernfællesskaber og eksterne parter i det omfang, det har en betydning for dem i deres muligheder for at være compliant og tilstrækkeligt databeskyttet.

Tabel 5: Ansvars- og rollefordeling ift. "Tilgang, afgang og ændringer i behandlingsprocesser eller datastrømme"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Tilrettelæggelse af processer og forretningsgange	DPOBP	Forvaltnings-ledelse	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver LCF
Initiering, juridisk vurdering og implementering af forandringer	Behandlingsproces-ansvarlig	Forvaltnings-ledelse	DPOBP Databeskyttelses-rådgiver funktion	DPOBP

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

1.2. Risikovurdering og konsekvensanalyse

Af databeskyttelseslovgivningen fremgår, at den dataansvarlige (Københavns Kommune), er forpligtiget til at foretage en konsekvensanalyse af databeskyttelsen, når en behandling af personoplysninger sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder [1].

Konsekvensanalyser har til formål at afdække, i hvilket omfang en behandlingsproces udsætter personoplysningerne for fare, og hvilke krav der skal stilles til de systemer, der håndterer oplysningerne, og den organisation, der får adgang til dem.

Risikovurdering af behandlingsprocesser

Behandlingsprocessers risikoprofil anvendes blandt andet som grundlag for at beslutte, om der skal foretages en konsekvensanalyse (jf. pkt. 1 herunder). Risikovurdering beregnes ud fra de

[1] Fysisk, materiel eller immateriel skade – forskelsbehandling, identitetstyveri, identitetssvig, økonomiske konsekvenser/tab, skade på omdømme, sociale konsekvenser indflydelse på privatliv, skade på menneskelig værdighed eller legitime interesser, begrænsning / krænkelse af fundamentale rettigheder og frihedsrettigheder, forhindring af udøvelse af kontrol med egne oplysninger.

registreringer, der er fortaget i Pactius Privacy, og som udgør dokumentationen for kommunens behandlingsprocesser og datastrømme.

Konsekvensanalysen skal gennemføres i følgende tilfælde:

1. Hvis eksisterende eller nye behandlingsprocesser har en risikoprofil (jf.) hvor sandsynlighed og/eller konsekvens score er over 2,0.

2. Hvis der skal implementeres et nyt system, eller der foretages ændringer i et eksisterende system eller infrastruktur i tilknytning til givne behandlingsprocesser.

   Ad 1

   Indgår der flere systemer i behandlingsprocessen, anvendes de primære systemers informationer i vurderingen af omfanget af foranstaltninger.

   Er der forskel på sikkerhedsniveauet af foranstaltninger i de primære systemer, anvendes den foranstaltning, der giver mindst sikkerhed i konsekvensanalysen.

   Ad 2

   Indgår der flere behandlingsprocesser i en ny systemanskaffelse, skal der udarbejdes en konsekvensanalyse for hver behandlingsproces.

   Konsekvensanalysen udarbejdes frem til og med vurderingen af de iboende risici (procestrin 2.B herunder) og opstiller dermed krav til foranstaltninger.

   Senest inden systemet kan modtage ibrugtagningstilladelse anføres de faktiske foranstaltninger og en fornyet risikovurdering, der dermed påviser om krav fra konsekvensanalysen er indfriet og risici er reduceret i tilstrækkelig grad.

   Viser en konsekvensanalyse en fortsat høj risiko på trods af foranstaltninger fremsendes resultatet af konsekvensanalysen til ansvarlig ledelse og Koncern IT, sammen med anbefalinger til foranstaltninger og information til ledelsen om, at der ikke kan gives en ibrugtagningstilladelse, før foranstaltninger er tilstrækkelige.

   Er der på trods af foranstaltninger fortsat en høj risiko for registreredes rettigheder og frihedsrettigheder, skal forvaltningen sikre, at konsekvensanalysen sendes i høring hos Datatilsynet.

Konsekvensanalysen skal udarbejdes og dokumenteres i overensstemmelse med de til enhver tid gældende retningslinjer herfor.

Koncern IT skal påse, at der er udarbejdet en konsekvensanalyse, og den indholdsmæssigt er tilstrækkeligt udarbejdet. Konsekvensanalysen skal endvidere, fremsendes til ansvarlig forvaltningsledelse til orientering og den skal journaliseres/arkiveres i Pactius Privacy under den vurderede proces.

Forvaltningerne kan anmode Databeskyttelsesrådgiveren om rådgivning i forbindelse med konsekvensanalysen. I tilfælde af uenighed mellem den dataansvarlige forvaltning og

Databeskyttelsesrådgiveren vedrørende konsekvensanalysens vurderinger eller foranstaltninger, skal det specifikt fremgår af selve konsekvensanalysen, hvorfor databeskyttelsesrådgiverens indstilling ikke er fulgt.

Vedligeholdelse af konsekvensanalyser skal ske i følgende tilfælde:

- Ved ændringer i en behandlingsproces revideres konsekvensanalysen tilsvarende.
- Hvis iboende risici er reduceret orienteres Koncern IT herom.
- Hvis iboende risici er øget, gennemføres konsekvensanalysen på ny.
- Ved sikkerhedsbrud - såfremt bruddet omfatter forhold behandlet i en konsekvensanalyse eksempelvis brugeradgange – foretages en ny vurdering af foranstaltninger for at sikre databeskyttelsen.

Tabel 6: Ansvars- og rollefordeling ift. "Risikovurdering og konsekvensanalyser"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Risikovurdering af behandlingsprocesser	DPO Business Partner	Forvaltningens ledelse	Databeskyttelses-rådgiver	Forvaltningens direktion
Konsekvensanalyse udarbejdelse, godkendelse og dokumentation	Behandlingsproces-ansvarlig	DPO Business Partner	Databeskyttelses-rådgiver	Forvaltningens direktion, Koncern IT
Konsekvensanalyse vedligeholdelse	Behandlingsproces-ansvarlig	DPO Business Partner	Databeskyttelses-rådgiver	Forvaltningens direktion, Koncern IT

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

2. VEDLIGEHOLDELSE AF DOKUMENTATION

2.1. Initiering, kvalitetssikring, opdatering og kontrol af informationer

For at sikre det bedst mulige udgangspunkt for at kunne dokumentere kommunens ret til at håndtere og evne til at beskytte personoplysninger, udvise ansvarlighed, føre tilsyn samt opfylde registreredes rettigheder, registreres en række oplysninger i et fælles dokumentationssystem Pactius.

Som en del af processen for initiering, juridisk vurdering og implementering af forandringer i behandlingsprocesser og datastrømme, skal dokumentationen af disse opdateres, ændres, sammenlægges, adskilles, tilføjes og slettes, så dokumentationen til stadighed er i overensstemmelse med faktiske forhold.

Dokumentationens fuldstændighed, rigtighed, afstemning og relationer til andre processer og datastrømme samt systemer og eksterne parter mv. påhviler den dataansvarlige (DPOBP, behandlingsprocesansvarlig og datastrømsansvarlig), herunder at informationer er kvalitetssikret, inden de registreres og i den periode de er registeret i fælles dokumentationssystem Pactius.

Opdatering af dokumentationen skal ske umiddelbart efter, at de juridiske vurderinger under pkt. 1.1. er foretaget, og indholdet af proces / datastrøm er kvalitetssikret.

Opdatering af en behandlingsproces og afledte forhold skal afsluttes i en arbejdsgang, således at informationssystemet ikke indeholder "halvt opdaterede" processer og datastrømme.

Indtastningen i følger gældende forretningsgange / vejledninger herfor.

Det skal altid være muligt for Databeskyttelsesrådgiveren at tilgå eller modtage information om hvilke ændringer, der er foretaget, hvem der har foretaget disse, og hvornår de er foretaget.

Tabel 7: Ansvars- og rollefordeling ift. "Initiering og kvalitetssikring af informationer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Vedligeholdelse af dokumentation	DPOBP	DPOBP	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver Forvaltnings-direktion

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

3. PERSONOPLYSNINGER, HÅNDTERING I DRIFT

3.1. Awareness og uddannelse

For at kunne sikre tilstrækkelig beskyttelse af personoplysninger, er det vigtigt, at alle medarbejdere med ansvar eller opgaver, hvormed personoplysninger behandles eller kan komme til medarbejderens kendskab, har viden om og er trænet i efterlevelsen af gældende lovgivning og regler, for aktivt at kunne medvirke til en korrekt og sikker håndtering af oplysningerne.

Forvaltningerne har pligt til løbende at sikre, at deres medarbejdere er opdaterede på gældende regler for håndteringen af personoplysninger. Den generelle introduktion til behandling og beskyttelse af personoplysninger kan ske igennem Københavns Kommunes e-learnings moduler eller ved tiltag, som forvaltningerne selv tager initiativ til.

Indhold og omfang af uddannelsen skal om nødvendigt suppleres og skal svare til medarbejderens ansvar og opgaver.

Regelmæssig gennemførelse af uddannelsesprogrammer er nødvendigt, og forvaltningerne skal have en konkret uddannelsesplan for, hvordan det sikres.

Uddannelsesplaner og de konkrete gennemførte uddannelser pr. medarbejder skal kunne dokumenteres.

Medarbejdere skal ved ansættelsesstart samt ved ændring af stilling, ansvar eller opgaver gennemføre relevant uddannelse om behandling og beskyttelse af personoplysninger.

Opstår der ændringer i krav til behandling og beskyttelse af personoplysninger på medarbejderens område skal medarbejderen uddannes tilsvarende.

Medarbejderne skal gennemføre relevant uddannelse minimum hvert 2. år.

Tabel 8: Ansvars- og rollefordeling ift. "Awareness og uddannelse"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af medarbejders uddannelse	Nærmeste leder	Forvaltnings-ledelse	DPOBP	Databeskyttelses-rådgiveren

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

3.2. Databeskyttelse i daglige sagsgange og ledelsestilsyn

For at sikre den bedst mulige databeskyttelse i alle grene af organisationen skal håndteringen af personoplysninger understøttes af nødvendige skriftlige og mundtlige anvisninger og regler samt kontrol.

Medarbejdernes grundlag for en optimal databeskyttelse og håndtering af personoplysninger i daglig drift, eksempelvis i form af arbejdsgangsbeskrivelser, vejledninger, mv., skal i tilstrækkeligt omfang være designet, implementeret, tilgængelige og effektive.

Konstateres der relevante problemstillinger, eller opstår der konkrete situationer, skal medarbejderen omgående gøre opmærksom på dette til nærmeste leder, der har ansvar for at håndtere forholdet, så risikoen for lignede forhold/sager minimeres.

Løbende ledelsestilsyn skal sikre og kontrollere forsvarlig adfærd, at instrukser og regler overholdes og er effektive (dvs. fungerer i praksis).

Forvaltningens compliance enhed vedr. databeskyttelse (DPOBP), skal inddrages i / orienteres om relevante problemstillinger, samt rådgive på anfordring og skal om nødvendigt understøtte en løsning.

Tabel 9: Ansvars- og rollefordeling ift. "Databeskyttelse daglige sagsgange"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikring af grundlag for databeskyttelse / håndtering af personoplysninger	Nærmeste leder	Forvaltningsdirektion	DPOBP	Databeskyttelses-rådgiver
Ledelsestilsyn	Nærmeste leder	Forvaltningsdirektion	DPOBP	Databeskyttelses-rådgiver
Rådgivning / support til nærmeste leder	DPOBP	DPOBP	Databeskyttelses-rådgiver	//

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

3.3. Persondatabrud

Københavns Kommunes har en række lovbestemte forpligtigelser og et selvstændigt ansvar for og interesse i, at tilliden til kommunens håndtering af personoplysninger er optimal, hvorfor en hurtig og effektiv håndtering af brud på persondata er meget vigtig.

Et persondatabrud defineres som en episode, der fører til en hændelig eller en ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Alle medarbejdere i kommunen har pligt til at anmelde potentielle persondatabrud via en fast systemindgang (pt. ServiceNow) eller direkte til DPOBP i den pågældende forvaltning.

Københavns Kommunes fælles proces og fælles administrative forretningsgang og deri fastsatte tidsfrister for håndteringen af persondatabrud skal følges.

Det er den enkelte leders ansvar, at forretningsgangen over for medarbejderne er implementeret, tilgængelig og effektiv, samt at medarbejderen har den fornødne viden om, hvordan den enkelte medarbejder skal opfylde sin forpligtigelse.

Tabel 10: Ansvars- og rollefordeling ift. "Sikkerhedsbrud"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Anmeldelse og håndtering af persondatabrud	Medarbejder	Nærmeste leder	DPOBP	Forvaltnings-direktion Databeskyttelses-rådgiver

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

4. COMPLIANCE HOS DATAANSVARLIG

4.1. Kontaktpunkt og formidling til/fra Databeskyttelsesrådgiveren

Den dataansvarlige (forvaltningerne) har ansvaret for at sikre, at Databeskyttelsesrådgiveren i alle henseender modtager information og bliver inddraget, så Databeskyttelsesrådgiven kan udføre sine opgaver, der består i at understøtte, at organisationen efterlever de databeskyttelsesretlige regler og kommunens regler, og derigennem skaber værdi for compliancearbejdet.

Alle forvaltninger har ansvaret for at informere, dokumentere og inddrage Databeskyttelsesrådgiveren, så denne kan underrette og rådgive organisationen og de ansatte om databeskyttelse.

Databeskyttelsesrådgiveren skal blandt andet, men ikke udelukkende, informeres og kan vælge at lade sig yderligere inddrage i følgende tilfælde:

- Ved overvejelser og tilrettelæggelse af eksisterende eller nye regler, retningslinjer, processer, forretningsgange etc. der skal sikre compliance.
- Ved overvejelser og tilrettelæggelse af eksisterende eller ny organisering af databeskyttelsesarbejdet hos den dataansvarlige
- Ved overvejelser og beslutninger om hvordan organisationens compliance med databeskyttelses sikres såvel i eksisterende som nye behandlingsprocesser
- Ved konsekvensanalyser, herunder beslutninger om nødvendige foranstaltninger i it-systemer for at efterleve krav til databeskyttelse gennem tekniske og organisatoriske foranstaltninger
- Før offentliggørelse af udbudsmateriale på it-systemer etc., hvor der er en høj risiko for registreredes rettigheder eller frihedsrettigheder er i fare.

Inddragelsen skal være rettidig, det vil sige inden beslutninger er truffet, retningslinjer er udstedt, it-system er anskaffet mv. Databeskyttelsesrådgiveren kan ikke inddrages i eller udføre den operationelle drift, og kan ikke tage stilling til eller godkende ledelsesmæssige beslutninger.

Forvaltningerne skal også viderebringe Databeskyttelsesrådgiverens henvendelser og/eller information til de rette enheder i forvaltningen. Forvaltningen skal følge op på henvendelserne, sikre nødvendige besvarelser til Datatilsynet samt underretning til Databeskyttelsesrådgiver om forvaltningens svar.

Databeskyttelsesrådgiverens anbefalinger og rådgivning bør tages til efterretning af den dataansvarlige og dennes organisation. Såfremt Databeskyttelsesrådgiverens rådgivning eller anbefalinger ikke følges, skal organisationen dokumentere dette i overensstemmelse med Databeskyttelseslovgivningens krav om accountability.

Tabel 11: Ansvars- og rollefordeling ift. "Kontaktpunkt og formidling til/fra Databeskyttelsesrådgiveren"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Information,	DPO	Forvaltnings	Databeskyttelses-	//

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
dokumentation og inddragelse til og fra Databeskyttelses-rådgiver	DPO BP	direktion	rådgiveren	

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

4.2. Rådgivning og overvågning (tilsyn) hos dataansvarlig

Forvaltningernes centrale/tværgående compliancearbejde har til formål at understøtte det daglige databeskyttelsesarbejde, ledelsestilsyn og forvaltningsdirektionens tilsyn med complianceniveauet i forvaltningerne. Derfor skal det være tilstrækkeligt, effektivt og værdiskabende for forvaltningernes enheder, ledere og medarbejdere og skal tilrettelægges ud fra en risikobaseret tilgang.

Forvaltningerne skal etablere et entydigt placeret og forankret complianceansvar i forvaltningen og sikre at forvaltningens enheder, ledere og medarbejdere er bekendt med, hvad compliancearbejdet består af. Desuden skal forvaltningen sikre, at enheder, ledere og medarbejdere er bekendt med, hvordan rådgivning i øvrigt kan modtages. Rådgivning skal ydes på anfordring, og skal endvidere proaktivt gives, hvor observationer i forbindelse med compliancearbejdet viser forhold, der kan forbedres.

Compliancearbejdet skal som minimum omfatte:

- At regler, retningslinjer, værktøjer og vejledninger og rådgivere er formidlet, kendt og implementeret i forvaltningen.
- At sikre et aktuelt overblik over forvaltningens databeskyttelsesorganisation herunder behandlingsprocesansvarlige og datastrømsansvarlige, og at denne fungerer efter hensigten.
- At sikre et aktuelt overblik forvaltningsaktiviteter og afledt dokumentation af forvaltningens behandlingsprocesser og datastrømme mv. til stadighed er korrekt, vedligeholdt og opdateret.
- At sikre et aktuelt overblik over forvaltningens complianceniveau, og at risikoprofilen for forvaltnings behandlingsprocesser til stadighed udgør den lavest mulige risiko, alternativt at risikoprofiler er kendt og accepteret af ledelsen.
- Overvåge særligt risikofyldte behandlingsprocesser.
- At yde rådgivning og sparring til forvaltningernes enheder og til forvaltningens ledelse i alle spørgsmål vedr. håndtering af personoplysninger, persondatabeskyttelse og registreredes rettigheder, herunder når særlovgivning, databeskyttelseslovgivning, teknik og kommunens egne regler mødes og skal omsættes til praksis.
- At modtage, koordinere og håndtere mulige konkrete brud på persondatasikkerheden, samt sikre anmeldelser til datatilsynet inden for tidsfristen på 72 timer.
- At overvåge at der er udarbejdet og forligger dokumentation for konsekvensanalyser, slettefrister, databehandleraftaler mv.
- At understøtte forvaltningens proces for anskaffelse af nye it-systemer med henblik på at sikre privacy i systemer.
- At deltage i tværgående complianceaktiviteter med henblik på at sikre, at kommunens samlede complianceniveau er tilstrækkeligt
- At sikre Databeskyttelsesrådgiverens tilstrækkelige og rettidige inddragelse med henblik på dennes mulighed for vurdering af, at databeskyttelsesretlige regler mv. overholdes.

Compliancearbejdet skal delvist tage udgangspunkt i en årsplan og delvist omfattes aktiviteter, der opstår ved at følge forvaltningens daglige drift, eventuelle sikkerhedshændelser mv. Den årlige complianceplan skal tilrettelægges og gennemføres ud fra en risikobaseret tilgang og i sammenhæng med kommunens aktuelle risikoniveau. Endvidere skal planens tilsynsemner og tilsynsmål være

afstemt med forvaltningsledelse og Databeskyttelsesrådgiveren, således at det samlede tilsyn for kommunen er dækkende, tilstrækkeligt og effektivt.

Ved tilrettelæggelse og gennemførelse af tilsyn skal det sikres:

- At der føres tilsyn med at fastlagte regler, processer, forretningsgange mv. er etableret.
- At de udførende medarbejdere har det nødvendige kendskab til at overholde regler og gennemføre proces, forretningsgange mv.
- At regler overholdes samt, at proces og forretningsgange reelt fungerer.

Tabel 12: Ansvars- og rollefordeling ift. "Rådgivning og overvågning hos dataansvarlig"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Udmøntning af rådgivning og overvågning	DPO Business Partner	Forvaltningens direktion	Databeskyttelses-rådgiver	//

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

4.3. Overvågning (tilsyn) af eksterne relationer, databehandlere, dataansvarlige og registrerede

Københavns Kommunes håndtering af personoplysninger involverer eksterne parter. Kommunen har eksterne databehandlere, der på vegne af kommunen varetager myndighedsopgaver og derfor modtager og behandler personoplysninger, som Kommunen har overladt til disse. Kommunen udveksler oplysninger med andre dataansvarlige som en naturlig del af kommunens myndighedsopgaver. I disse tilfælde har kommunen som dataansvarlig et ansvar for, at databeskyttelsen lever op til lovgivningen, og at registreredes rettigheder opfyldes.

<u>Databehandlere</u>

Overvågning / tilsyn med databehandlere tager afsæt i den databehandleraftale, der er indgået med den eksterne part, og som skal opfylde kravene i Københavns Kommunes fælles standardskabeloner for databehandleraftaler med bilag. Det forudsættes at Databehandleraftalen i nødvendigt omfang er kvalitetssikret af medarbejdere med henholdsvis juridisk, faglig og teknisk kompetence inden for det givne aftalefelt.

Det forudsættes endvidere, at databehandleraftalen er afstemt med leveranceaftalen med den pågældende leverandør, således at der af leveranceaftalen ikke fremgår modstridende betingelser i forhold til håndtering og beskyttelse af personoplysninger samt kommunens krav til informationssikkerhed generelt.

Er der i aftalen omfattet særlige forhold, hvor der sker fravigelser til databehandleraftalens standardbetingelser, skal fravigelserne beskrives og begrundes, og journaliseres, efter at disse er ledelsesgodkendt på et niveau svarende til risikoniveauet. Ændringer til standardbetingelser må ikke ud fra en risikovurdering forringe regeloverholdelsen og/eller beskyttelsen af

personoplysninger og/eller opfyldelsen af registreredes rettigheder eller stille kommunen ringere i tilfælde af sikkerhedsbrud, ved compliancetjek mv.

Der skal i nødvendigt omfang ske en løbende opfølgning og tilsyn med det aftalte samarbejde, regeloverholdelse, behandlingen af personoplysninger og tilhørende informationssikkerhed. 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.

Frekvens for tilsyn eller periodisk indhentelse af revisorerklæring skal fremgå af databehandleraftalen og skal ske minimum en gang pr. år efter, at den faktiske behandling af personoplysninger er påbegyndt. Tilsynsvurdering, omfang og indhold følger den til enhver tid gældende fælles administrative forretningsgang.

Såfremt en opfølgning, et tilsyn eller en revisorerklæring viser, at databehandleren ikke lever op til databehandleraftalens bestemmelser og instrukser, skal påpegede forhold omgående udbedres og efterfølgende forbedres med henblik på fremtiden. Alternativt skal aftalen med leverandøren opsiges.

Dataansvarlige

Der skal ske en løbende overvågning af / tilsyn med, at kommunen som dataansvarlig har hjemmel til at videregive personoplysninger til den modtagne dataansvarlige, ligesom denne om nødvendigt skal kunne dokumentere over for kommunen, hvilket hjemmelsgrundlag de modtager personoplysningerne på.

Der skal endvidere ske en løbende overvågning af / tilsyn med, at kommunen har hjemmel til at modtage personoplysninger fra andre dataansvarlige.

Kommunen og de dataansvarlige, der udveksles personoplysninger med, har et fælles ansvar for at kommunikationsform / -linjer er sikre, hvilket der ligeledes skal føres tilsyn med.

Registrerede og deres rettigheder

Der skal ske en løbende overvågning af / tilsyn med forvaltningernes overholdelse af regler og forretningsgange for håndtering af registreredes rettigheder.

Overvågning/tilsyn skal påpege og analysere indhold og omfang af svagheder i måden registreredes rettigheder (oplysningspligt, indsigtshåndtering mv.) håndteres på, herunder hvorvidt registrerede oplever, at kommunen i tilstrækkelig grad efterlever loven.

Resultatet af overvågning/tilsyn skal kunne danne grundlag for beslutninger, forbedringstiltag mv., eller kan medvirke til at betrykke ledelse i, at complianceniveauet og databeskyttelsen er tilstrækkelig.

Tilsynet kan tilrettelægges med afsæt i et udvalgt område, der er omfattet af registreredes rettigheder (oplysningspligt, indsigtshåndtering mv.) eller organisatoriske områders evne til samlet at overholde registreredes rettigheder.

Generelt vedrørende overvågning / tilsyn af eksterne relationer

Frekvens for overvågning og tilsyn, samt tilrettelæggelse og gennemførelse af tilsyn følger anvisningerne under pkt. 4.2.

Tabel 13: Ansvars- og rollefordeling ift. "Overvågning af eksterne relationer"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overvågning af eksterne relationer	DPO Business Partner	Forvaltningens direktion	Databeskyttelses-rådgiver	//

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

4.4. Ledelsesrapportering

En kontinuerlig ledelsesrapportering i forlængelse af blandt andet tilsyn skal sikre det bedst mulige udgangspunkt for generel ledelsesinformation, ledelsesbeslutninger, intern og ekstern information om kommunens complianceniveau samt dokumentation af, at kommunen til stadighed udviser ansvarlighed i forhold til at opfylde databeskyttelseslovgivningen.

Forvaltningerne skal tilrettelægge nødvendig og tilstrækkelig ledelsesrapportering for så vidt angår enheders, områders og forvaltningens compliance- og risikoniveau.

Status, begrundelse og eventuelle tiltag som følge af status på forvaltningens samlede complianceniveau og risikoniveau skal forelægges forvaltningsdirektionen og Databeskyttelsesrådgiveren minimum en gang pr. år pr. 1. juni.

I forlængelse af overvågning/tilsyn og i umiddelbar tilknytning til hver tilsynsaktivitet, skal der udarbejdes en rapportering. Rapportering skal have særlig fokus på uhensigtsmæssige/ utilstrækkelige forhold i relation til behandling og beskyttelse af personoplysninger og/eller manglende efterlevelse af databeskyttelseslovgivningen. Af rapporteringen (i form af notat eller rapport) skal observationer, vurdering af risikoniveau og anbefalinger til forbedringer fremgå. Rapportering skal forelægges forvaltningsdirektionen og Databeskyttelsesrådgiveren umiddelbart efter, at rapportering er afsluttet.

Tabel 14: Ansvars- og rollefordeling ift. "Ledelsesrapportering"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Ledelsesrapportering tilrettelæggelse og udførelse	DPO Business Partner	Forvaltningens direktion	Databeskyttelses-rådgiver	Databeskyttelses-rådgiver

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

5. DATABESKYTTELSESRÅDGIVEREN

5.1. Underretning og rådgivning

Databeskyttelsesrådgiveren skal gennem underretning og rådgivning understøtte forvaltningers DPO Business Partnere (DPOBP), forvaltningernes direktioner og det politiske niveau i at fastholde og udvikle et optimalt complianceniveau i kommunen.

Databeskyttelsesrådgiveren underretter uden ugrundet ophold forvaltningerne gennem DPOBP, når ekstern praksis, principper, afgørelser eller tilsvarende interne forhold mv. kommer til Databeskyttelsesrådgiverens kendskab.

På anfordring fra DPOBP eller forvaltningsledelser kan Databeskyttelsesrådgiveren besvare spørgsmål eller rådgive til fortolkning og/eller praktisk udmøntning af databeskyttelseslovgivningens bestemmelser, og herunder opstille anbefalinger til ledelsesmæssige beslutninger.

Databeskyttelsesrådgiveren skal informeres og inddrages inden beslutninger er truffet, retningslinjer er udstedt, it-system er anskaffet mv. Databeskyttelsesrådgiveren kan ikke inddrages i eller udføre den operationelle drift, og kan ikke tage stilling til eller godkende ledelsesmæssige beslutninger

Modtages henvendelser fra andre end DPOBP eller DPOBP teamet i forvaltningerne, vurderes forholdet og besvares enten direkte med cc til DPOBP, eller der henvises til DPOBP.

Databeskyttelsesrådgiveren skal løbende vurdere, om underretning eller rådgivning kan berøre eller have betydning for flere forvaltninger eller kommunen som helhed og i så fald sikre, at underretning eller rådgivning omfatter de berørte parter.

Databeskyttelsesrådgiveren kan i forbindelse med sit virke vælge, at udarbejde en skriftlig eller afgive en mundtlig udtalelse. Udtalelser, hvor Databeskyttelsesrådgiveren kommer med anbefalinger, bør tages til efterretning og efterleves af forvaltningerne. Vælger forvaltningerne at fravige Databeskyttelsesrådgiverens anbefalinger, bør dette begrundes og dokumenteres i overensstemmelse med Databeskyttelsesforordningens krav om accountability.

I forbindelse med Databeskyttelsesrådgiverens rådgivning mv. påhviler dataansvaret alene den dataansvarlige Københavns Kommune. Databeskyttelsesrådgiveren har ikke del i dette ansvar.

Tabel 15: Ansvars- og rollefordeling ift. "Underretning og rådgivning"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Underretning og rådgivning	Databeskyttelses-rådgiver funktionen	Databeskyttelses-rådgiveren	//	DPOBP Forvaltnings-direktion

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

5.2. Risikovurdering

Databeskyttelseslovgivningen forudsætter i vidt omfang, at den dataansvarliges arbejde, med at styre, håndtere og beskytte personoplysninger og sikre registreredes rettigheder, foretages på grundlag af en vurdering af, hvor risici er størst, og dermed hvor en compliance indsats er nødvendig og giver størst mulig effekt. Derfor vil etablering og anvendelse af risikovurderinger være grundlaget for Databeskyttelses-rådgiverens arbejde.

Københavns Kommunes risikovurderinger på databeskyttelsesområdet skal foretages ved anvendelse af kommunens dokumentationssystem for behandlingsprocesser og datastrømme (Pactius Privacy / PP), hvor de grundlæggende risikovurderinger for behandlingsprocesser er beregnet.

Databeskyttelsesrådgiveren skal løbende sikre, at beregningsgrundlag og faktorer i PP's risikomodul løbende evalueres og/eller kalibreres, for så vidt at det kan forbedre risikoberegningerne.

Databeskyttelsesrådgiveren skal, hvor det kan kvalificere eller kvantificere compliancearbejde, inkludere risikovurderinger som grundlag eksempelvis ved tilsyn, GAP analyser, ledelsesrapportering og konsekvensanalyser.

Databeskyttelsesrådgiveren skal så vidt det er muligt overvåge risikovurdering af it-systemer, der behandler personoplysninger. Databeskyttelsesrådgiveren skal på grundlag af systemernes risikovurdering og eventuelt systemernes øvrige karakteristika om muligt gøre opmærksom på enkeltforhold eller samlede risici på systemområdet, som kræver den dataansvarliges opmærksomhed.

Databeskyttelsesrådgiveren skal overvåge, at de dataansvarlige forvaltninger anvender Pactius risikovurderinger på deres ansvarsområder og i deres compliancearbejde.

Databeskyttelsesrådgiveren skal endvidere føre tilsyn med, at informationer i PP, der danner grundlag for, at risikovurderinger er korrekt registreret, er i overensstemmelse med faktiske forhold og at faktisk forhold løbende evalueres og forbedres med henblik på at nedsætte risici.

Databeskyttelsesrådgiveren skal i tæt samarbejde med relevante DPO Business Partnere udarbejde simulerede risikoprofiler som grundlag for at opnå den bedst mulige databeskyttelse og compliance i efterfølgende driftssituation. Simulering skal udføres i følgende tilfælde:

- inden der iværksættes ny behandling af personoplysninger,
- ved ændringer i behandlingen
- ved indførelse af væsentlige ændringer af it-systemer og infrastruktur

Risikovurdering fra PP skal om nødvendigt suppleres med individuelle risikovurderinger for at sikre, at vurderingen er tilstrækkelig for at træffe beslutninger. Alle risikovurderinger, der anvendes som grundlag for beslutninger mv. jf. ovenfor skal være dokumenteret.

Alle risikovurderinger skal være udført af kvalificerede medarbejdere og foretages på et ensartet grundlag (for nærværende PP).

Tabel 16: Ansvars- og rollefordeling ift. "Risikovurdering"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Sikre og udvikle risikoberegningsværktøj,	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver	Ekstern Konsulent	DPOBP
Tilsyn	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver	//	DPOBP
Simulering ved nyt og ved ændringer	Databeskyttelses-rådgiver funktion og DPOBP	Databeskyttelses-rådgiver	//	DPOBP
Individuelle supplerende risikovurderinger	DPOBP	Forvaltnings-ledelse	Databeskyttelses-rådgiver funktion	//

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

5.3. Overvågning og tilsyn

Overvågning af overholdelsen af de databeskyttelsesretlige regler i organisationen foretages i sammenhæng med ledelsestilsyn, forvaltningernes tværgående compliancearbejde samt af Databeskyttelsesrådgiveren. Databeskyttelsesrådgiverens overvågning og tilsynsansvar fremgår af Databeskyttelseslovgivningen og omfatter overholdelsen af de databeskyttelsesretlige regler i organisationen.

Databeskyttelsesrådgiveren skal etablere og løbende opdatere det koncept, der skal være grundlaget for at opnå en tilstrækkelig overvågning på/tilsyn med samtlige områder, der hidrører under Databeskyttelsesrådgiverens ansvarsområde.

Databeskyttelsesrådgiverens tilsyn skal tage udgangspunkt i en årsplan. Tilsyn / overvågning kan desuden omfatte aktiviteter, der opstår som at følge af løbende observationer hos forvaltningernes daglige drift, ændringer i risikoniveau, sikkerhedshændelser mv.

Planen kan omfatte tilsyn med udgangspunkt i emner i relation til lovgivningens kravområder fx anvendelse af samtykke, udvalgte tværgående områder fx anvendelse af SoMe eller tilsyn med specifikke organisatoriske områder. Sidstnævnte understøttes af en rotation mellem forvaltningernes enheder, med henblik på at sikre en tilstrækkelig tværgående indsigt i complianceniveauet og om mulig en jævnlig direkte overvågning af / tilsyn med enheder eller områder.

Scoping og udvælgelse af tilsynsemner skal ske med afsæt i risikovurderinger i PP, GAP analyser, observationer i daglig drift og andre forhold, der kan indikere nødvendigheden af et tilsyn.

Tilsyn skal ske på områder, hvor der er behov for en dybere undersøgelse af specifikke forhold og med henblik på mitigerende handlinger eller for at betrykke direktioner og den politiske ledelse i, at complianceniveau er tilstrækkeligt.

Databeskyttelsesrådgiveren har ansvaret for at indsamle information fra forvaltningernes direktioner og DPO Business Partnere med henblik på at scope og udvælge emner. Oplæg til

årsplan skal fremsendes til forvaltninger til kommentering, og med henblik på at sikre at tilsyn og overvågning er dækkende, tilstrækkeligt og effektivt i forhold til forvaltningernes eget compliancearbejde. Databeskyttelsesrådgiveren er beslutningstager på indhold og omfang af den endelige tilsynsplan og øvrige overvågnings- og tilsynsaktiviteter, der vælges gennemført.

Databeskyttelsesrådgiveren underretter DPO Business Partner forud for gennemførelse af større tilsynsopgaver samt præsenterer scopet og planen for tilsynet, der indeholder:

- Formål
- Tilsynsgrundlag
- Tilsynshandlinger
- Tilsynsproces / tidsplan
- Resultat / produkt

Den tidsmæssige plan for tilsynet skal afstemmes mellem parterne, hvorefter forvaltningen skal afsætte nødvendige ressourcer og tid til tilsynet.

Databeskyttelsesrådgiveren skal til enhver tid have adgang til organisationens personoplysninger, den behandling, der pågår af disse samt øvrige nødvendige oplysninger for at udføre overvågnings- / tilsynsopgaver. Der er tale om en vid adgang, der skal kunne tilvejebringes efter behov.

Ved tilrettelæggelse og gennemførelse af tilsyn skal det sikres:

- At der føres tilsyn med, at fastlagte regler, processer, forretningsgange mv. er etableret
- At de udførende medarbejdere har det nødvendige kendskab til at overholde regler og gennemføre proces, forretningsgange mv.
- At regler overholdes, samt at proces og forretningsgange reelt fungerer.

Tabel 17: Ansvars- og rollefordeling ift. "Overvågning og tilsyn"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Overvågning og tilsyn med dataansvarlige	Databeskyttelses-rådgiverfunktion	Databeskyttelses-rådgiver	//	Revisionsudvalg Forvaltningsledelse DPOBP

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

5.4. Rapportering

Rapportering skal sikre at forhold af betydning for databeskyttelsen kommer til direktioner og det politiske niveaus kendskab, samt at direktioner og det politiske niveau som kommunens øverste dataansvarlig har en tilstrækkelig viden om kommunens compliance- og databeskyttelsesniveau.

Databeskyttelsesrådgiveren refererer og rapporterer i alle forhold vedrørende Databeskyttelsesrådgiver ansvar, opgaver og observationer til Borgerrepræsentationen via Revisionsudvalget.

Databeskyttelsesrådgiveren rapporterer løbende til Revisionsudvalget og direktionerne, for så vidt at tilsynsaktiviteter har identificeret særlig kritiske forhold eller risiko for, at kommunen, forvaltninger eller givne områder ikke er compliant med Databeskyttelsesforordningen og/eller databeskyttelsesloven.

Databeskyttelsesrådgiveren rapporterer til direktionerne på sikkerhedsbrud, for så vidt at bruddet er væsentligt, og Databeskyttelsesrådgiveren samtidig vurderer, at bruddet ikke håndteres i tilstrækkelig grad. Er sikkerhedsbrud af en særlig væsentlig karakter rapporteres disse tillige til Revisionsudvalget. Databeskyttelsesrådgiveren kan indstille til, at særlige kritiske forhold kan forelægges Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget..

Databeskyttelsesrådgiveren udarbejder årligt pr. 1. oktober en risikovurdering pr. forvaltning og for kommunen som helhed suppleret med en kort vurdering af complianceniveauet, omfanget af sikkerhedsbrud samt øvrige forhold i relation til databeskyttelse i København Kommune.

Rapporterne pr. forvaltning fremsendes til forvaltningernes direktioner og til Revisionsudvalget.

Rapporten for Københavns Kommune fremsendes til Revisionsudvalget samt til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

Tabel 18: Ansvars- og rollefordeling ift. "Rapportering"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Rapportering	Databeskyttelses-rådgiveren	Revisionsudvalg	//	Revisionsudvalg Direktioner DPOBP

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

5.5. Samarbejde med Datatilsynet

For at sikre det bedst mulige samarbejde med Datatilsynet er Københavns Kommunens Databeskyttelsesrådgiveren Datatilsynets kontaktpunkt.

Databeskyttelsesrådgiveren er Datatilsynets kontaktpunkt til Københavns Kommune.

Alle henvendelser **fra** Datatilsynet til Københavns Kommune skal, uanset hvem der modtager disse, sendes til Databeskyttelsesrådgiveren til orientering eller videreformidling.

Alle henvendelser **til** Datatilsynet fremsendes til Databeskyttelsesrådgiveren, inden disse fremsendes til Datatilsynet. Databeskyttelsesrådgiveren orienterer sig i sagen og skal give sin tilkendegivelse, hvorefter forvaltningen fremsender til Datatilsynet. Dette udelukker ikke, at en forvaltning telefonisk kan kontakte Datatilsynet med henblik på at modtage generel rådgivning.

Forvaltningerne har ansvaret for håndtering og besvarelse af alle henvendelser, der måtte komme fra Datatilsynet samt overholdelse af fastsatte tidsfrister. Databeskyttelsesrådgiveren kan yde rådgivning på anfordring.

Tabel 19: Ansvars- og rollefordeling ift. "Samarbejde med Datatilsynet"

Aktivitet	Udførende	Ansvarlig	Rådgivende	Informeret
Henvendelser fra Datatilsynet	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver	//	Revisionsudvalg DPOBP LCF
Henvendelser til Datatilsynet på vegne af kommunen som helhed	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiveren	//	DPOBP LCF
Henvendelser til Datatilsynet på vegne af én forvaltning	Forvaltningen	DPOBP	Databeskyttelses-rådgiver funktion	Databeskyttelses-rådgiver funktion

Herom gælder følgende forretningsgange:

- *Forvaltningsspecifikke forretningsgange kan understøtte dette*

6. FORRETNINGSGANGE

Jf. regelhierarkiet for Københavns Kommune udmøntes regelsættes i dette cirkulære af et antal fællesadministrative forretningsgange, som beskriver den aftalte proces.

Kvalitetsstandard for dokumentation af forretningsgange i Københavns Kommune gælder for udarbejdelse af forretningsgange. Kvalitetsstandarden indeholder retningslinjer for udarbejdelse af forretningsgange, herunder anvendelse af notationer og procesniveauer samt forhold omkring identifikation af risici (identifikation og klassifikation af risici og kontrolaktiviteter).

Formålet med denne kvalitetsstandard er at sikre en entydig metodetilgang for dokumentation af forretningsgange i Københavns Kommune. Ved anvendelse af kvalitetsstandarden sikres, at dokumentationen for kommunens forretningsgange har en tilstrækkelig faglig kvalitet.

FÆLLES ADMINISTRATIVE FORRETNINGSGANGE

Fællesadministrative forretningsgange godkendes jf. kommunens regelhierarki af Økonomiforvaltningen efter koordinering med It-kredsen.

Følgende fællesadministrative forretningsgange er gældende i medhør af forretningscirkulæret:

- *Fællesadministrativ forretningsgang for it-leverancer ("leverancemodellen")*
  OBS: Denne forretningsgang er fortsat under udarbejdelse, hvorfor forretningscirkulæret konsekvensrettes, når forretningsgangen er endelig godkendt.

FORVALTNINGSSPECIFIKKE FORRETNINGSGANGE

Forvaltningsspecifikke forretningsgange godkendes af den pågældende forvaltnings direktion.

Den enkelte forvaltning har selv ansvaret for at udarbejde nødvendige forretningsgange til at understøtte de fællesadministrative forretningsgange samt regelsættet på it- og informationssikkerhedsområdet, i det omfang forvaltningen vurderer det nødvendigt.

7. ÆNDRING OG AJOURFØRING

Økonomiforvaltningen har overfor Økonomiudvalget ansvar for vedligeholdelse og ajourføring af dette forretningscirkulære gennem inddragelse af kommunens relevante tværgående fora, hvori alle forvaltninger er repræsenteret.

INDHOLDSMÆSSIGE ÆNDRINGER

Forslag til ændringer af forretningscirkulæret forelægges af Økonomiforvaltningen for Økonomiudvalget til godkendelse.

Underliggende fællesadministrative forretningsgange udarbejdes og besluttes af Økonomiforvaltningen efter forelæggelse for It-kredsen.

Underliggende forvaltningsspecifikke forretningsgange udarbejdes af den enkelte forvaltning og forelægges den enkelte forvaltnings direktion til godkendelse.

REDAKTIONELLE ÆNDRINGER

Redaktionelle ændringer, som ikke indebærer egentlige ændringer i forretningscirkulæret, kan dog godkendes af Økonomiforvaltningens direktion. Tilsvarende gælder ændringer, der som følge af Borgerrepræsentationens, Økonomiudvalget og It-kredsens beslutninger måtte indebære konsekvensrettelser i forretningscirkulæret.

KØBENHAVNS KOMMUNE

FORRETNINGSCIRKULÆRE FOR IT-ANSKAFFELSER