TILSYNSRAPPORT

Databeskyttelsesrådgiveren

Dato 26. august 2022

Tilsyn med KK-databank

Økonomiforvaltningen

MODTAGER

Søren Hartmann Hede
Mads Grønvall

Indholdsfortegnelse

1. Indledning og formål

Københavns Kommunes Koncern IT har siden 2016 driftet en databank, der beskrives som:

"KK Databank er et fælles data storage kombineret med en række compute tools til analyse, machine learning og traditionel BI."

KK Databank skal betragtes som et dataopbevarings-"system". Databanken kan således trække personoplysninger fra et forvaltningsspecifikt eller tværgående system fx kvantum, hvorefter data kan anvendes til andre formål. Disse formål kan f.eks. være frafaldsovervågning på forskellige enheder i SUF ift. SOSU-elever.

Data kan ligeledes bruges til at udarbejde ledelsesinformation, statistik eller til sammenstilling af personoplysninger, således at det er muligt at benytte oplysningerne på andre elle nye måder. Dette kunne fx være til at foretage en mere effektiv kontrol af bopælsregistreringer eller opdage svindel med sociale ydelser.

Systemer eller databaser (som databanken), der muliggør samkøring og datalagring, har umiddelbart en høj iboende risiko i forhold til overholdelse af de databeskyttelsesretslige regler og dermed en høj risiko for de registrerede (borgerne). Det stiller store krav til velbeskrevne forretningsgange, identifikation af risici og etablering af kontroller der skal sikre overholdelse af de databeskyttelsesretlige regler.

Vi er bekendt med, at databanken indeholder en betydelig mængde personoplysninger og har derfor valgt at foretage et tilsyn rettet mod databanken med det formål at påse, at databanken administreres tilfredsstillende.

1.1 Tilsynets omfang og udførelse

Formålet med tilsynet er at konstatere, hvorvidt Københavns Kommunes databank administreres i overensstemmelse med kommunens interne regler og databeskyttelsesreglerne.

- Første del af undersøgelsen omhandler, hvorvidt der er udpeget en systemansvarlig chef og en teknisk og forretningsmæssig systemejer.

- Anden del af undersøgelse omhandler, hvorvidt den systemansvarlige chef og den tekniske og forretningsmæssige systemejer har indgået dataudvekslingsaftaler, udarbejdet fortegnelser, risikovurderinger og eventuelle konsekvensanalyser som kommunens regelsæt foreskriver.

- Tredje del af undersøgelsen handler om at påse at de udvalgte opgaver rettet mod databeskyttelsesområdet jf. ovenfor, er håndteret effektivt i forhold til at sikre den nødvendige databeskyttelse.

Tilsynet omfatter ØKF som systemejer.

1.2 Rapportering

Observationerne i afsnit 5 er forinden fremsendelse af udkast, fremsendt skriftligt til faktuel høring i forvaltningen.

I henhold til funktionsbeskrivelsen for Databeskyttelsesrådgiveren, rapporteres der 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.

Det anbefales, at forvaltningens behandling af rapporten, herunder fremlæggelse for stående udvalg, følger anvisningen angivet på bilag 1.

2. Konklusion og anbefaling

Konklusionerne bygger på observationer fra forvaltningernes skriftlige tilbagemeldinger og er angivet nedenfor i afsnit 5.

Tilsynet har givet anledning til følgende konklusioner og anbefalinger.

2.1 Økonomiforvaltningen

Forvaltning	ØKF	Revisionsområde	Databeskyttelse	Væsentlighedsniveau
Reference		Revisionsemne	KK Databank	
Observationer	Systemansvarlig chef for Databanken FISKK-id #2136 henhører under ØKF Den systemansvarlige chef har ansvaret for at: • udpege og placere en forretningsmæssig systemejer for det it-system, vedkommende er ansvarlig for • sikre, at den forretningsmæssige systemejer løfter alle opgaver beskrevet i § 22 og § 23 og i øvrige relevante forretningscirkulærer, for de it-systemer vedkommende har ansvar for." Den systemansvarlige chef har oplyst, at man har overladt ansvaret for opgaverne der påhviler rollen som forretningsmæssig systemejer til flere personer i forvaltningerne. Jævnfør kommunens regler, skal der udpeges en forretningsmæssig systemejer, for hver forvaltning. For at varetage rollen som forretningsmæssig systemejer skal den systemansvarlige chef sikre, at de udpegede forretningsmæssige systemejer har modtaget den nødvendige uddannelse til at udfylde rollen. Den systemansvarlige chef har ikke sikret, at de udpegede datamanagere har modtaget den nødvendige uddannelse ligesom det ikke er sikret, at de har løftet de opgaver der kræves i rollen. Endelig har vi konstateret, at Databanken anvendes til test. Der er særlige regler for anvendelse af personoplysninger i test, som skal efterleves.			
Konklusioner og anbefalinger	Det henstilles, at den systemansvarlige chef sikrer, at kommunens regler efterleves vedrørende databanken. Der skal udpeges en forretningsmæssig systemejer i hver forvaltning der har den nødvendige uddannelse, som kræves i rollen som forretningsmæssig systemejer. Det anbefales, at det vurderes hvordan den systemansvarlige chef skal sikre at den forretningsmæssige systemejer udfører de opgaver der kræves i rollen når systemet anvendes i flere forvaltninger.			
Forvaltningens iværksatte tiltag	ØKF har udarbejdet en handleplan for implementering af tiltag, som sikrer, at kommunens regler efterleves samt en tidslinje for gennemførsel. Tiltagene skal sikre den nødvendige databeskyttelse i forbindelse med anvendelse af KK Databank.			

	Følgende tiltag implementeres: 1. Der udpeges forretningsmæssige systemejere i de forvaltninger som anvender databank 2. Forretningsmæssige systemejere pålægges at gennemføre krævet uddannelse 3. Forretningsmæssige systemejere pålægges at sikre overholdelse af gældende regler 4. Systemansvarlig chef indskærper kontrolproces 5. Systemansvarlig chef overvejer, hvorvidt systemansvarlig rolle også skal uddelegeres til forvaltningerne. 6. ØKF udarbejder "Fælles administrativ forretningsgang for tværgående behandlingsprocesser". Den samlede handleplan herunder tidslinje er fremgår af bilag 2.	

3. Forvaltningens tiltag

Rapportens konklusion er drøftet med ledelsen, der er enig i indholdet af rapporten, og har tilsluttet sig Databeskyttelsesrådgiverens vurderinger i tilknytning hertil. På dette grundlag har forvaltningen formuleret en række tiltag, som det fremgår ovenfor i afsnit 3.

Databeskyttelsesrådgiveren vurderer, at de anførte vil reducere de identificerede risici. Databeskyttelsesrådgiveren foretager en opfølgning på forvaltningens iværksatte, som led i næste års aktivitetsplan.

4. Krav jf. Databeskyttelsesforordningen

4.1 Databeskyttelsesforordningen

Det følger af databeskyttelsesforordningen, at der skal udarbejdes risikovurderinger og fortegnelser på alle behandlingsprocesser. Det følger endvidere, at i de tilfælde, hvor en behandling indebærer høj risiko for den registrerede, skal der udarbejdes en konsekvensanalyse.

Art. 30 - Fortegnelse
Stk. 1. Hver dataansvarlig og hvis det er relevant, den dataansvarliges repræsentant fører fortegnelser over behandlingsaktiviteter under deres ansvar. Disse fortegnelser skal omfatte alle af følgende oplysninger […]

Art. 32 - Risikovurdering
Stk. 1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant […]

Art. 35 - Konsekvensanalyse
Stk. 1.Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici […]

5. Databeskyttelsesrådgiverens observationer

I de følgende afsnit redegøres der for de gældende regler i databeskyttelsesforordningen og Københavns Kommunes interne regler.

5.1 Systemansvarlig chef (ØKF)

I forretningscirkulære for organisering af informationssikkerhed er følgende anført:

"§ 21. Den systemansvarlige chef har ansvar for at udpege og placere en forretningsmæssig og teknisk systemejer for det it-system, vedkommende er ansvarlig for.

Stk. 2 Den systemansvarlige chef har ansvar for at sikre, at den forretningsmæssige systemejer og tekniske systemejer løfter alle opgaver beskrevet i § 22 og § 23 og i øvrige relevante forretningscirkulærer, for de it-systemer vedkommende har ansvar for."

Kravene til den tekniske og forretningsmæssige systemejer kan ses i bilag 2.

Vi har påset at der er udpeget en systemansvarlig chef for Databanken FISKK-id #2136.

Der er ligeledes udpeget en teknisk systemejer for Databanken.

Den systemansvarlige chef har oplyst, at man har overladt ansvaret for opgaverne der påhviler rollen som forretningsmæssig systemejer til flere personer i forvaltningerne i henhold til Forretningscirkulære for organisering af informationssikkerhed § 22, stk. 2.

Det er ifølge det oplyste, sket via den AD-rolle, som kaldes "datamanager". Ved gennemførelsen af tilsynet har ØKF 32 datamanagere. TMF har fem, SOF har fem og KFF har seks.

Jævnfør kommunens regler skal der udpeges en forretningsmæssig systemejer for hver forvaltning. Denne person kan herefter overlade ansvaret for udførelsen af opgaverne til flere personer og enheder inden for egen forvaltning. Det er dog forsat den udpegede forretningsmæssige systemejer der har ansvaret for, at de opgaver der er beskrevet i kommunens cirkulære overholdes.

For at varetage rollen som forretningsmæssig systemejer skal den systemansvarlige chef sikre, at de udpegede forretningsmæssige systemejere har modtaget den nødvendige uddannelse til at udfylde rollen. Den systemansvarlige chef har ikke sikret, at de udpegerede datamanagere har modtaget den nødvendige uddannelse.

6.1 Forretningsmæssig systemejer

Som anført ovenfor har den systemansvarlige chef oplyst, at det er AD-rollen, kaldet "datamanager", der har det overordnede ansvar for at efterleve de krav der stilles til den forretningsmæssig systemejer, jf. Forretningscirkulære for organisering af informationssikkerhed.

Vi har derfor kontaktet forvaltningernes GDPR-koordinatorer for at undersøge om forvaltningernes datamanagere har udført de opgaver, som er pålagt den forretningsmæssige systemejer, eller om der i hver forvaltning er en person der varetager rollen som hovedansvarlig forretningsmæssig systemejer.

6.1.1 Økonomiforvaltningen (KIT, KS og KEID)

I ØKF er der ikke udpeget en hovedansvarlig forretningsmæssig systemejer. Håndteringen er derfor overladt til forvaltningens 32 datamanagere.

ØKF har ikke udarbejdet fortegnelser over deres aktuelle behandlinger i databanken. Det er derfor ikke muligt at se oplysninger som fx lovhjemmel, formål, hvem der behandles oplysninger om, hvilket typer af oplysninger der behandles om den enkelte mv.

Der er ligeledes ikke udarbejdet risikovurderinger på behandlingsprocessen eller udarbejdet en tilstrækkeligt dækkende konsekvensanalyse. Der er endvidere ikke udarbejdet en forvaltningsspecifik forretningsgang for brugen af databanken.

6.1.2 Forhold hos de anvendende forvaltninger

Ingen af de forvaltninger, der iht. FISKK anvender databanken, har udpeget en hovedansvarlig forretningsmæssig systemejer. Håndteringen er derfor overladt til forvaltningens fem datamanagere.

I to af de tre forvaltninger var der ikke udarbejdet fortegnelser. En enkelt forvaltning havde udarbejdet en fortegnelse, der var dog uoverensstemmelser mellem i fortegnelsen og den beskrivelse af databehandlingen, som forvaltningen har fremsendt til Databeskyttelsesrådgiveren.

Ingen af forvaltningerne har udarbejdet risikovurderinger på behandlingsprocessen. I to tilfælde havde forvaltningerne ikke taget stilling til, hvorvidt der skal laves en eller flere konsekvensanalyser, samt udarbejdet eventuelle konsekvensanalyser. I et tilfælde var der udarbejdet en konsekvensanalyse, som ikke indholdsmæssigt lever op til kravene til en konsekvensanalyse

Der er endvidere ikke udarbejdet en forvaltningsspecifik forretningsgang for brugen af databanken.

6.1.3 Øvrige observationer

I Københavns Kommune er der generelt forbud mod at anvende personoplysninger i test, med undtagelser. I henhold til cirkulæret for informationssikkerhed pkt. 8.6 følger det,

> *"Person- eller værdioplysninger må ikke anvendes i tests, medmindre der foretages anonymisering af oplysningerne, eller det på forhånd begrundes, dokumenteres og godkendes af den ansvarlige enheds direktion, at der er taget passende sikkerhedsmæssige foranstaltninger, for at sikre, at der tages hensyn til den registreredes rettigheder, og at kommunens data ikke mistes, ændres, at uvedkommende ikke får adgang til data, eller at it-systemet eller andre it-systemer ikke lider skade. I et sådan tilfælde skal reglerne for tests og afprøvninger iagttages, som de står anført i forretningscirkulære for it-anskaffelser. Ved en eventuel anonymisering af oplysninger skal det sikres, at det ikke på nogen måde er muligt at identificere de personer, som oplysningerne oprindeligt vedrørte"*

Databeskyttelsesrådgiveren har erfaret, at der ligeledes bliver foretaget POC'er (Proof of concept), i databanken, hvilket sidestilles med test.

Enhedens direktion skal derfor godkende forvaltningernes brug af personoplysninger i test, inden igangsættelsen. Dette bør, være sikret via. Kontrol og kunne dokumenteres af Koncern IT, hvilket ikke har været tilfældet.

BILAG 1 Definition af prioriteter for væsentlighedsniveau

I tilsynsrapporter fra Databeskyttelsesrådgiveren vil formidlingen af risiko og væsentlighed på de enkelte observationer blive påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 

- Prioritet 1 markeringer anvendes for forhold, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en rapportering til BR.
- Et forhold anses for kritisk, hvis der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt for borgeren.
- Prioritet 1 markeringer rapporteres til ledelsen med anbefaling om, at disse forelægges for det stående udvalg eller Økonomiudvalget.

Prioritet 2 – markeres med 

- Prioritet 2 markeringer anvendes for forhold, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre rapportering til BR.
- Et forhold anses for væsentlig, hvis der en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse for borgeren.
- Prioritet 2 markeringer rapporteres til ledelsen i den reviderede forvaltning.

Prioritet 3 – markeres med 

- Anvendes for forhold, der ikke har givet anledning til omtale eller kun anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter.
- En risiko anses for mindre væsentlig, hvis der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.

BILAG 2 Forvaltningens handleplan

Handleplan for KK Databank

Databeskyttelsesrådgiveren har foretaget et tilsyn med kommunens administration af Københavns Kommunes (KK) Databank. Tilsynet har identificeret nogle forhold, som Databeskyttelsesrådgiveren har vurderet som kritiske, hvilket har medført henstillinger og anbefalinger. Nærværende dokument udgør handleplan for implementering af tiltag, som sikrer, at kommunens regler efterleves samt en tidslinje for gennemførsel. Tiltagene skal sikre den nødvendige databeskyttelse i forbindelse med anvendelse af KK Databank.

Anbefalinger i tilsynsrapporten
Tilsynet med KK Databank har medført følgende henstillinger og anbefalinger jf. bilag 2.

1. Det henstilles, at den systemansvarlige chef sikrer, at kommunens regler efterleves vedrørende databanken.

2. Der skal udpeges en forretningsmæssig systemejer i hver forvaltning, der har den nødvendige uddannelse, som kræves i rollen som forretningsmæssig systemejer.

3. Det anbefales, at det vurderes, hvordan den systemansvarlige chef skal sikre, at den forretningsmæssige systemejer udfører de opgaver, der kræves i rollen, når systemet anvendes i flere forvaltninger.

Håndtering af tilsynsrapportens henstillinger og anbefalinger
Følgende tiltag implementeres.

1. Der udpeges forretningsmæssige systemejere i de forvaltninger som anvender databank
2. Forretningsmæssige systemejere pålægges at gennemføre krævet uddannelse
3. Forretningsmæssige systemejere pålægges at sikre overholdelse af gældende regler
4. Systemansvarlig chef indskærper kontrolproces
5. Systemansvarlig chef overvejer, hvorvidt systemansvarlig rolle også skal uddelegeres til forvaltningerne.
6. ØKF udarbejder "Fælles administrativ forretningsgang for tværgående behandlingsprocesser".

I nedenstående uddybes de seks tiltag nærmere.

<u>1, Der udpeges forretningsmæssige systemejere i de forvaltninger som anvender databank.</u>
Forvaltningerne pålægges at udpege forretningsmæssige systemejere for deres delområde af databank. Forvaltningerne skal foretage denne udpegning senest Q3 2022. systemejerskabet dokumenteres og ajourføres under FISKK #2136. Systemansvarlig chef og teknisk systemejer varetages af KIT. Forvaltningen skal i forvejen leve op til gældende bestemmelser, hvorfor der ikke bør være et ekstraordinært ressourcetræk i forbindelse med, at ansvarsfordelingen tydeliggøres.

2. Forretningsmæssige systemejere pålægges at gennemføre påkrævet uddannelse.
Forretningsmæssige systemejere skal gennemføre e-learning for systemejerskab senest Q3 2022 jf. bilag 3 forretningscirkulære for informationssikkerhed §14 stk. 9. *Systemejerskab 1. del – e-læring | Københavns Kommune (plan2learn.dk)*

3. Forretningsmæssige systemejere pålægges at sikre overholdelse af gældende regler
Det påhviler forvaltningen at overholde gældende regler. Forvaltningens forretningsmæssige systemejer skal senest Q4 2022 dokumentere overfor systemansvarlig chef, at der sker overholdelse heraf. It-sikkerhedshåndbogen er retningsvisende for gældende krav *Vejledninger - Service Portal (service-now.com)*
I forretningcirkulære for organisering af informationssikkerhed er krav til forretningsmæssig systemejer fastsat jf. bilag 3 forretnings-cirkulære for informationssikkerhed § 22. Pga. databanks arkitektur fastsættes en deling af ansvar mellem det centrale systemejerskab i KIT og anvendende forvaltninger. Ansvarsfordelingen opdeles i tre. KIT ansvar, forvaltningens ansvar og fælles ansvar.

KIT ansvar
Overholdelse af stk. 1, pkt. 2,6,10,11,12,13,15 i bilag 3 forretningscirkulære for informationssikkerhed. Varetagelsen af ansvaret for platformen placeres alene hos KIT.

Forvaltningens ansvar
Overholdelse af pkt. 4, 5, 8, 9, 16 bilag 3 forretningscirkulære for in-formationssikkerhed. Varetagelsen af ansvaret for anvendelse af forvaltningens del af platformen placeres alene hos forvaltningen jf. bilag 3 forretningscirkulære for informationssikkerhed §7 stk. 4.
Forvaltningen sikrer herunder, at der er dokumentation for overholdelse af gældende regler for behandlingsprocesser.
Dokumentationen herfor vedrører udfærdigelse af fortegnelser, risikovurderinger, konsekvensanalyser og dataudvekslingsaftaler.
Dokumentationen udformes jf. vejledningerne på it-sikkerhedsportalen *Vejledning - Service Portal (service-now.com)* og journaliseres ét samlet sted, som er tilgængelig for den systemansvarlige chef.
Den forretningsmæssige systemejer kan uddelegere udførelsen af opgaver til øvrige personer og enheder i forvaltningen jf. §22 stk. 2 bilag 3 forretningscirkulære for informationssikkerhed. Ansvaret for overholdelsen af gældende krav påhviler dog fortsat den forretningsmæssige systemejer.

Fælles ansvar
Overholdelse af stk. 1, pkt. 1, 3, 7, 14 bilag 3 forretningscirkulære for informationssikkerhed. En række områder afføder et delt ansvar mellem forvaltningens forretningsmæssige systemejer og den forretningsmæssige systemejer for platformen, som varetages af KIT.
Jf. stk. 1, pkt. 3 bilag 3 forretningscirkulære for informationssikker-hed. Forvaltningen har sammen med systemejerskabet ansvaret for at have indsigt i fælles lovkrav. Forvaltningen har alene ansvaret for at have indsigt i særlige lovkrav, der vedrører forvaltningen.
Jf. stk. 1, pkt. 7 bilag 3 forretningscirkulære for informationssikker-hed. Koncern IT har ansvaret for, at der forefindes databehandleraftale og tavshedspligterklæringer for systemet. Forvaltningen har ansvaret for, at der forefindes databehandleraftaler og tavshedspligt-erklæringer for de databehandlere, som forvaltningen anvender.

4. Systemansvarlig chef indskærper kontrolproces
Systemansvarlig chef gennemfører nedenstående tilsynsaktiviteter årligt Q1, Næste kontrol foretages Q1 2023.

1. Forretningsmæssig systemejer og systemansvarlig chef gennemgår fortegnelsen for behandlingsprocesser for dokumenteret hjemmel.
2. Systemansvarlig chef fører tilsyn med, at de registrerede behandlingsprocesser har den nødvendige dokumentation, herunder risikovurdering, konsekvensanalyse, dataudvekslingsaftaler, databehandleraftaler & evt. samtykkeerklæringer.
3. Forretningsmæssig systemejer og systemansvarlig chef gennemgår databank for kontrol af, at der er overensstemmelse med det dokumenterede og den faktiske anvendelse af systemet.
4. Systemansvarlig chef dokumenterer kontrollen i edoc under FISKK ID #2136.

5. Systemansvarlig chef overvejer hvorvidt systemansvarlig rolle også skal uddelegeres til forvaltningerne.
På baggrund af de implementerede tiltag, foretages en vurdering af, om den fastsatte ansvarsfordeling i tilstrækkelig grad er dækkende for udførelse og ansvar i medfør af bilag 3 forretningscirkulære for informationssikkerhed §7 stk. 4, §10 stk. 2.På baggrund af vurderingen indstilles evt. ændringsforslag til ansvarsfordelingen.

6. ØKF udarbejder "Fælles administrativ forretningsgang for tværgående behandlingsprocesser"
Der er identificeret behov for at tydeliggøre ansvarsfordelinger og forretningsgang i de tilfælde, hvor KIT stiller platforme til rådighed for forvaltningerne. Forretningsgangen har til hensigt at håndtere ansvarsfordelingen i forbindelse med administrationen af systemet og behandlingsprocesser, hvor data fra eksterne systemer opsamles, behandles og evt. videregives.

Koncern IT udarbejder udkast til "fælles administrativ forretningsgang for tværgående behandlingsprocesser". Forretningsgangen sendes til godkendelse i ØKF direktion efter inddragelse af IT-kredsen Q4 2022.

BILAG 3 KK's Interne regler

FORRETNINGSMÆSSIG SYSTEMEJER

§ 22. Forvaltningen har ansvaret for at udpege en person til at varetage følgende opgaver:

1) at holde sig orienteret i kommunens og forvaltningsspecifikke regelsæt
2) at indgå i relevante faglige fællesskaber omkring systemejerrollen
3) at have indsigt i eventuelle særlige lovkrav for det pågældende forvaltningsområde, som kan have indflydelse på de krav, der stilles til it-systemet
4) at have indsigt i hjemmelsgrundlaget for de oplysninger, som behandles i it-systemet
5) at it-systemet ikke indeholder oplysninger, som der ikke er hjemmel til at behandle, eller som skulle have været slettet
6) at roller og rettigheder er beskrevet i forhold til brugeradministrationen i it-systemet
7) at der indgås nødvendige databehandleraftaler og tavshedspligtserklæringer
8) at der foretages nødvendige konsekvensanalyser i overensstemmelse med forretningscirkulære for persondatabeskyttelse – dokumentation og compliance, hvis registreringen og anvendelsen af data ændrer sig
9) at der i samarbejde med den behandlingsprocesansvarlige og datastrømsansvarlige, jf. forretningscirkulære for persondatabeskyttelse – dokumentation og compliance, foretages registreringer i det it-system, som Databeskyttelsesrådgiveren stiller til rådighed for registrering af dataprocesser mv.
10) at have indsigt i forvaltningens udviklingsønsker til det pågældende it-system og bistå den tekniske systemejer, så it-systemets funktionalitet løbende tilpasses og understøtter kommunens behov
11) at styre økonomi for it-systemet i henhold til forretningsbehov
12) at sikre, at der sker kontrol af dataoverførsler fra fagsystemer til økonomisystemer for at sikre et korrekt regnskab
13) at sikre, at den indgåede kontrakt indsendes til Koncern IT, og at der følges op på leverandørers opfyldelse af krav
14) at samarbejde med den tekniske systemejer om en sikker og effektiv udfasning af et it-system ved at varetage den forretningsmæssige side af udfasningen, herunder ansvar for at overholde regler vedr. databeskyttelse samt opbevaring af it-systemets logs efter udfasning
15) at godkende overtagelsesprøve fra leverandøren i forbindelse med udvikling og ændring af it-systemer
16) at fungere som kontaktperson mellem Koncern IT og kommunens brugere af it-systemet

Stk. 2. Ansvaret for udførelsen af de i stk. 1, nr. 1-16, nævnte opgaver kan overlades til flere personer og enheder inden for egen forvaltning. I så fald skal den ansvarlige person som supplement til sin rolle som kontaktperson, jf. stk.1, nr. 16, også fungere som kontaktperson til disse personer og enheder.

Stk. 3. For at varetage opgaven som forretningsmæssig systemejer på henholdsvis generiske administrative it-systemer, infrastruktur, tværgående fagsystemer og fagsystemer skal det i § 14, stk. 9, omtalte kursus være gennemført. Se forretningscirkulære for it-anskaffelser for definitioner på ovenstående.

TEKNISK SYSTEMEJER

§ 23. Den tekniske systemejer har ansvaret for at varetage følgende opgaver:

1) at holde sig orienteret i kommunens og forvaltningsspecifikke regelsæt
2) at indgå i relevante faglige fællesskaber omkring systemejerrollen
3) at sikre, at systemfunktionalitet og -anvendelse løbende tilpasses og bedst muligt understøtter informationssikkerhedskravene samt forretnings- og brugerbehov
4) at enhver ændring, der har snitflader til og/eller deling af ressourcer med Koncern IT eller kommunens øvrige netværk, skal ske efter Koncern IT's procedurer for ændring af it-systemer (change)
5) at der er etableret procedurer, der sikrer it-systemet en stabil, effektiv og sikker drift, og at disse er løbende dokumenteret
6) at der er indgået aftale om it-beredskabet efter de kriterier og retningslinjer, der er fastlagt i kommunens informationssikkerhedsregler
7) at der i relevant omfang kan foretages maskinel logning, når det kræves af lovgivning og/eller kommunens egne regler
8) at der sker test inden migrering fra udvikling til produktion for at sikre det ønskede drifts- og it-sikkerhedsniveau
9) at dokumentationen af it-systemer og processer er ajourført og tilgængelig for relevante medarbejdere
10) at kunne forelægge retvisende og opdateret dokumentation for tildelte autorisationer i det givne it-system
11) at bistå med systemteknisk viden i forhold til udførelsen af det forretningsmæssige systemejerskab jf. § 22
12) at understøtte den forretningsmæssige budgetstyring af it-systemet ved at identificere kommende og nødvendige tekniske investeringsbehov for it-systemet
13) at registreringen af it-systemet i kommunens liste over it-systemaktiver, jf. § 10, stk. 1, til stadighed er retvisende

14) at samarbejde med den forretningsmæssige systemejer om en sikker og effektiv udfasning af et it-system ved at varetage den tekniske side af udfasningen, herunder opsigelse af infrastrukturkomponenter.

Stk. 2. For at varetage opgaven som teknisk systemejer på henholdsvis generiske administrative it-systemer, infrastruktur, tværgående fagsystemer og fagsystemer skal det i § 14, stk. 9, omtalte kursus være gennemført. Se forretningscirkulære for it-anskaffelser for definitioner på ovenstående.