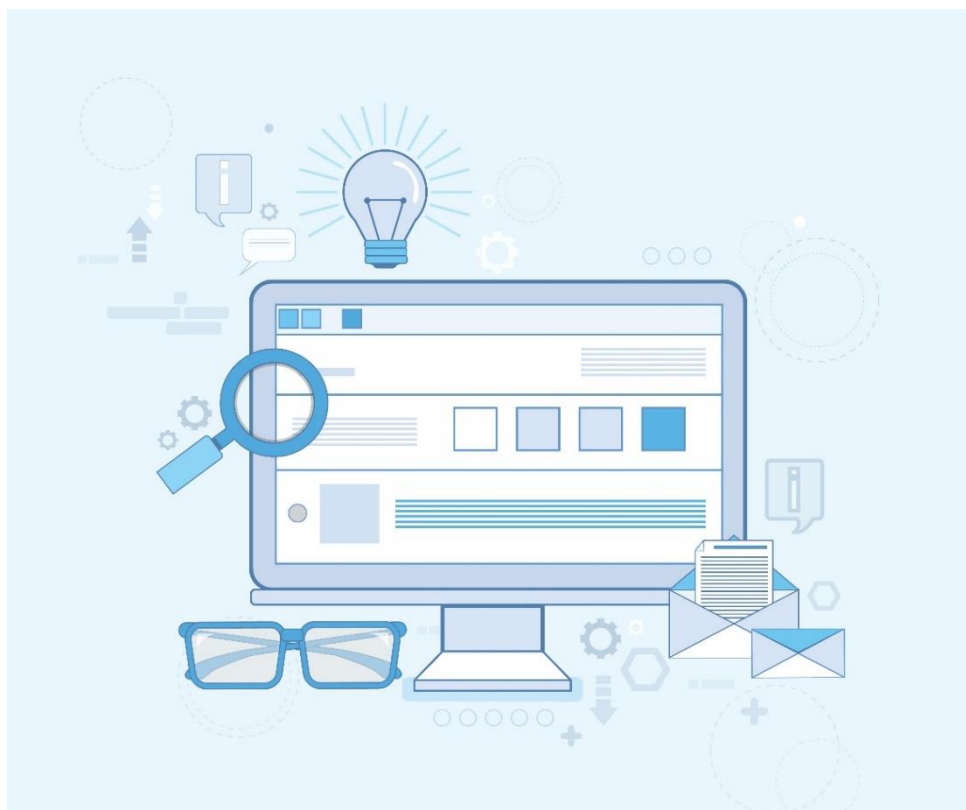




Guide til systemejere i Randers Kommune

Om ansvar og opgaveportefølje ifm. rollen som
systemejer



Indholdsfortegnelse

Introduktion	3
Systemejerens ansvar	3
Systemejerens opgaver	5
Databeskyttelsesforordningen	5
Generel sikkerhed og dokumentation.....	5
Drift og daglig brug.....	6
Afvikling af system (exitstrategi)	6



Introduktion

Formålet med arbejdet med systemejerskab er, at der er en person som grundet dennes funktion, har ansvar for at sikre, at Randers Kommune kan overholde krav til informationssikkerheden - herunder datasikkerhed, systemanvendelse, fejlhåndtering m.m., for det pågældende system.

Det er nødvendigt, at håndtere det ansvar og de opgaver, som er tilknyttet systemejerskabet professionelt. Randers Kommunes systemer er aktiver for kommunen, der skal forvaltes og beskyttes.

Systemejerskab er en ledelsesopgave og ansvaret er i Randers Kommune tillagt direktører, fag- eller stabschefer eller ledere med direkte reference til fag- og stabschefer. Opgaver der følger systemejerskabet kan dog godt uddelegeres, mens ansvaret er pålagt systemejeren.

Definition på et system:

Digitaliseringsstyrelsen definerer et it-system som *"et system der består af digitale informationsteknologier"*.

Et system er altså et it-system, en online tjeneste, en database eller en app som anvendes i Randers Kommunes opgaveløsning og som håndterer data i tekst, tale, billeder, video eller andet digital format.

Systemejersens ansvar

Systemejeren har ansvaret for det enkelte it-system i hele dets livscyklus – og har dermed ansvaret for systemets drift, anvendelse, vedligeholdelse og kontraktlige forhold samt sikkerheden i systemet.

Systemejeren sikrer fortløbende, at systemets funktionalitet fungerer effektivt og understøtter arbejdsprocesserne, herunder behandlingen og sikring af informationer og lovkrav.

Det er systemejers ansvar, at udarbejde retningslinjer og procedurer samt at føre løbende kontrol med overholdelsen.

I Randers Kommune, er systemejere som udgangspunkt også dataejere, derfor har systemejere også ansvaret for behandling af data i det pågældende system.

Systemejere skal orientere sig i interne politikker og procedurer for informationssikkerhed, og skal kende kravene i databeskyttelsesforordningen.

Systemejere skal sikre, at der tages backup af systemet, samt sikre, at backuppen testes regelmæssigt.

Systemejeren skal sikre, at data er tilstrækkelig beskyttet i systemet. Dette sker ved, at der er gennemført passende organisatoriske og tekniske foranstaltninger både for at sikre de registreres



rettigheder i forhold til systemets behandling af persondata og for at beskytte organisationens følsomme data.

Ved indkøb, nyudvikling eller videreudvikling, stilles krav om overholdelse af organisatoriske og tekniske krav til informationssikkerhed jf. databeskyttelsesforordningen ("Privacy by design"). Derfor har systemejeren en aktiv rolle ved anskaffelse af systemer, da systemejeren skal sikre at kravene til informationssikkerhed aktivt tænkes ind fx ved standardprofiler i systemet ("Privacy by default").

Systemejer er ansvarlig for, at der er udarbejdes risikovurderinger inden systemet tages i brug. Systemejer er også ansvarlig for at disse bruges aktivt, for at sikre at de rette foranstaltninger er implementeret. Systemejer skal derudover sikre at risikovurderingerne ajourføres.

Systemejer skal, i dialog med kommunens databeskyttelsesrådgiver, sikre om der skal udarbejdes en konsekvensanalyse, hvis der ud fra de databeskyttelsesretslige regler er krav til dette. Ved nyudvikling/ændringer i systemet skal systemejer sikre, om ændringen medfører et behov for en revideret konsekvensanalyse.

Som systemejer har du ansvaret for, at sikre de registreredes rettigheder jf. databeskyttelsesforordningen i det givne system.

Systemejer har overordnet ansvaret for:

- ✓ informationssikkerheden for systemet, herunder ansvar for at der bliver udarbejdet procedurer og retningslinjer for anvendelse og behandling af data i systemet.
- ✓ at der føres løbende kontrol med, at procedurer og retningslinjer overholdes og sikre vedligeholdelse af overblik over systemet.
- ✓ at der tages backup af systemet, samt at backuppen testes regelmæssigt
- ✓ for kontraktlige forhold herunder indgåelse af databehandleraftale.
- ✓ at godkende risikovurderinger og eventuel konsekvensvurdering samt at sikre at disse udarbejdes.
- ✓ at godkende anskaffelser og installation af disse.
- ✓ at give adgang til system og data.
- ✓ at sikre korrekt journalisering, arkivering og sletning.
- ✓ at godkende beredskabsplaner.
- ✓ at følge op på sikkerhedshændelser og brud på persondatasikkerheden.



Systemejerens opgaver

Det kræver ikke særlig teknisk indsigt at være systemejer, men det kræver et godt overblik over de forretningsprocesser, systemet understøtter.

Systemejeropgaven varierer i indhold og omfang alt efter systemets størrelse og omfang.

Databeskyttelsesforordningen

Hvis du er systemejer for et system, der behandler personoplysninger, skal dit system overholde reglerne i EUs databeskyttelsesforordning (GDPR) og den danske databeskyttelseslov. Det omhandler bl.a. følgende opgaver:



Databehandleraftale: Hvis du er systemejer for et system, der udveksler personoplysninger med eksterne databehandlere, kræver det en skriftlig aftale mellem Randers Kommune og den eksterne databehandler. Det kan fx være i forbindelse med drift-, hosting- eller cloud-løsninger eller indkøbte konsulentopgaver.



Fortegnelse over behandlinger af personoplysninger: Randers Kommune skal have et overblik over alle de behandlinger af personoplysninger som kommunen foretager.



Hvis du som systemejer er ansvarlig for et nyt system og derfor en ny behandling af personoplysninger, skal du sikre at Randers Kommunes fortegnelser er korrekt ajourførte ift. den nye behandling.

Konsekvensanalyse: Det kan være nødvendigt at udarbejde en konsekvensanalyse.



Ved at udarbejde en konsekvensanalyse kan du på et oplyst grundlag tage stilling til, om behandlingen af personoplysninger – på trods af de risici, der er identificeret herved – skal påbegyndes.

De registreredes rettigheder: Som systemejer er det relevant på forhånd af få afklaret, hvilke rettigheder det pågældende system skal kunne leve op til.



Sikkerhedsbrud: Som systemejer er det dit ansvar at håndtere, hvis der skulle forekomme et sikkerhedsbrud i systemet.

Generel sikkerhed og dokumentation

Systemejer har ansvaret for at der udarbejdes og følges op på dokumentation i ift. sikkerhed. Dette giver bl.a. følgende opgaver:

- ☐ At der er udfyldt en fyldestgørende systembeskrivelse for systemet
- ☐ Der er dokumenteret procedurebeskrivelse af brugerstyring (oprettelse, ændring og sletning af bruger)



- ☐ Der er dokumenteret procedurebeskrivelse af kontrol af brugeradgange jf. reglerne for informationssikkerhed og at proceduren følges
- ☐ Der er dokumenteret slettefrister af personoplysninger og at sletning varetages
- ☐ Der er en dokumenteret risikovurdering i forhold til eventuelle personoplysninger i systemet (den registreredes synspunkt)
- ☐ Der er en dokumenteret risikovurdering i forhold til integritet, tilgængelighed og fortrolighed og sikring af tilstrækkelig tekniske og organisatoriske foranstaltninger herfor.
- ☐ Der ved behov er en dokumenteret konsekvensanalyse
- ☐ Der ved behov er dokumenteret it-beredskab med manuelle procedurer, så kommunen kan håndtere fortsat nødvendig drift, hvis systemet helt eller delvist er utilgængeligt på grund af fx nedbrud, opdatering eller lignende

Drift og daglig brug

Systemejer har ansvaret for drift af systemet og derved også det daglige brug. Dette ansvar medfører en række opgaver:

- ☐ Systemet bedst muligt opfylder fagområdets og brugernes behov og dermed understøtter udviklingen af fagområdet og kommunens opgaveløsning
- ☐ Sikre at systemet anvendes optimalt og korrekt
 - Sager og dokumenter er korrekt mærket op i systemet, fx jævnfør KLE, hvis systemet benytter denne klassifikationsmetode
 - Relevant materiale journaliseres og arkiveres i henhold til henholdsvis slettefrister, GDPR, offentlighedsloven og arkivloven
 - Aktive sager og dokumenter overdrages til en anden medarbejder, når en medarbejder fratræder sin funktion
- ☐ Have det overordnede overblik i, hvordan systemet fungerer (fejlhåndtering m.m.)
- ☐ Have det overordnede overblik over videreudvikling og ændringer af systemet
- ☐ Sikre at der løbende sker opdatering af anvendt software
- ☐ Håndtere systemet i forhold til sikkerhedsbrud

Afvikling af system (exitstrategi)

Når et system ikke længere skal anvendes, har systemejer ansvar for at systemet afvikles korrekt, herunder at:

- ☐ Kontrakt med leverandør opsiges, når systemet ikke længere skal anvendes
- ☐ Data som fortsat skal anvendes migreres til andet system



- ☐ Ansvar for at data slettes hos evt. leverandør
- ☐ Arkivpligtigt materiale arkiveres

Når et system afvikles, skal IT og Digitalisering have besked. Skal systemet afløses af nyt system, skal indkøbet følge Randers Kommunes indkøbsguide for it-indkøb.

OBS: Husk at eventuelle links til selvbetjening skal fjernes fra kommunens hjemmeside, borger.dk, virk.dk og andre steder, hvor det måtte forekomme.