

Kontrol af databehandlere og underdatabehandlere

Detaljeret og konkret plan – Viborg Kommune

Baggrund

Datatilsynet har udtalt alvorlig kritik af Viborg Kommunes kontrol af databehandlere og underdatabehandlere. Som en del af udtalelsen har Datatilsynet bedt om at få tilsendt en detaljeret og konkret plan for, hvordan Viborg Kommune vil leve op til kravene fremefter.

Årsplan

I vedlagte bilag "Bilag 1: I-sikkerhedsarbejdet i Viborg Kommune – Organisering og Årshjul" er organisering, roller og ansvar samt gennemgang af årligt tilbagevendende opgaver oplistet. Afsnittet "F. Indgåelse af og opfølgning på databehandleraftaler" er tilrettet iht. Datatilsynets udtalelser.

I løbet af 2019-2020 kommer der desuden en række skabeloner og dokumenter fra KL's projekt omkring implementering af EU-persondataforordningen – herunder en meget detaljeret årsplan, som dækker i-sikkerhedsaktiviteterne bredt. Viborg Kommune følger dette arbejde tæt.

Herunder uddybes konkrete forhold, som relaterer sig til Datatilsynets kritikpunkter, med angivelse af de handlinger, som Viborg Kommune har eller planlægger igangsat.

Databehandleraftaler – udarbejdelse og kontrol

Ny databehandleraftale

Ved etablering af ny kontrakt med en leverandør af et system, som forudsætter indgåelse af databehandleraftaler, kan der ikke underskrives kontrakt, inden databehandler og eventuelle underdatabehandlere er godkendt.

En godkendelse forudsætter kontrol af seneste revisionserklæring, alternativt fysisk besøg eller telefoninterview. Viborg Kommune forlanger som udgangspunkt revisionserklæring udleveret, men en risikovurdering af systemets kritikalitet kan medføre, at revisionserklæring erstattes af fysisk besøg/telefoninterview. Som støtte for besøg eller interview er der udarbejdet skabelon, som sikrer kontrollen vil give et retvisende sikkerhedsbillede af databehandler og underdatabehandlere.

Der er særlig fokus på databehandlers anvendelse af underdatabehandlere og databehandlers dokumentation for kontrol af disse.

Resultat af gennemgang af revisionserklæring eller kontrolbesøg/interview journaliseres i kommunens ESDH-system sammen med selve databehandleraftalen.

Ovennævnte procedure bliver indarbejdet i kommunens it-projektmodel, og desuden har direktionen allerede på et tidligere tidspunkt besluttet, at enhver it-kontrakt skal underskrives af både systemansvarlig, It- og digitaliseringschefen og Udbuds- og indkøbschefen. Herved opnås en tilstrækkelig sikkerhed for, at kontrakter ikke indgås inden databehandleraftale er underskrevet.

Afslutningsvis skal det nævnes, at indarbejdelse af ovenstående proces ikke er uden udfordringer, når det skal kobles med udbudsreglerne ved f.eks. EU-udbud eller tilbudsindhentning.

Kontrol af eksisterende databehandlersaftale

Alle databehandlersaftaler er registreret i kommunes system til administration af i-sikkerhedsopgaver – Control Manager. Hver databehandlersaftale er registreret med tidspunkt for indgåelse, tidspunkt for næste kontrol iht. 12 måneders kontrolregel og systemansvarlig, som har ansvaret for kontrol af databehandler og underdatabehandlere. Desuden er det registreret, hvor vidt der er indgået aftale om fremsendelse af seneste revisionserklæring, eller om kontrol sker ved fysisk besøg eller telefoninterview.

Den årlige kontrol af databehandler og underdatabehandlere foregår herefter fuldstændig identisk med proceduren beskrevet under etablering af ny databehandlersaftale.

Også her er der særlig fokus på databehandlers anvendelse af underdatabehandlere og databehandlers dokumentation for kontrol af disse.

Resultat af gennemgang af revisionserklæring eller kontrolbesøg/interview journaliseres i kommunens ESDH-system sammen med selve databehandlersaftalen.

Microsoft

Datatilsynet havde under tilsynet i november 2018 udtaget Microsofts databehandlersaftale til særlig gennemgang. Komplexiteten i Microsofts dokumenter vedr. databehandler og underdatabehandlere har medført, at Viborg Kommune på kvartalsmøder med Microsoft har det med som fast punkt hver gang.

Desuden er der aftalt særlig instruktion fra Microsoft, med det formål at instruere repræsentanter fra It og Digitalisering i den portal, hvor Microsoft løbende opdaterer dokumenter relateret til databehandler og underdatabehandlere. Den særlige instruktion kombineret med det faste punkt på statusmøderne skal sikre Viborg Kommune den nødvendige viden om databehandlersaftale og underdatabehandlere, som Datatilsynet kritiserede i referatet fra tilsynsbesøget.

Systemejere – opkvalificering

Fra Viborg Kommunes sikkerhedspolitik:

For alle væsentlige anvendte, definerbare datamængder identificeres en Data- og Systemejer, som tildeles ansvaret for, at håndtering af kommunens data varetages med en hensigtsmæssig sikkerhed. Data- og Systemejere er som udgangspunkt forvaltningsdirektører og stabsdirektører. Data- og Systemejere kan delegere opgaven, men ikke ansvaret internt - eller overdrage opgaven, men ikke ansvaret for håndteringen af informationssikkerheden til eksterne samarbejdspartnere.

Alle systemejere er registreret i administrationssystemet Control Manager. Viborg Kommunes DPO gennemfører i 2. halvår 2019 sammen med It og Digitalisering en instruktion af alle registrerede systemejere med databehandlersaftaler i forhold til deres opgaver med årlig kontrol af databehandlere og underdatabehandlere.

Ved ansættelse af nye ledere, der overtager systemansvar, vil denne instruktion være obligatorisk.

Digitaliseringskonsulenter – opkvalificering

Iht. årsplanen i bilag 1 har digitaliseringskonsulenterne en særdeles aktiv rolle i at gennemføre kontrol af databehandlere og underdatabehandlere under ansvar over for systemejere.

DPO gennemfører en detaljeret instruktion af alle digitaliseringskonsulenter i denne kontrolopgave, og DPO'en deltager så vidt mulig i kontrollerne, indtil digitaliseringskonsulenten er tilstrækkelig tryk ved opgaven.

Samtidig opfordrer I-sikkerhedsgruppen alle digitaliseringskonsulenter til at deltage i KL's kursus for DPO'er, for at tilegne sig yderligere sikkerhedsmæssige kompetencer til øvrige sikkerhedsopgaver ud over kontrol af databehandlere og underdatabehandlere.