It og Digitalisering den 4.september 2019
CAA

Bilag 1: I-sikkerhedsarbejdet i Viborg Kommune – Organisering og Årshjul.

Organisering

I-sikkerhedsarbejdet er i Viborg Kommune organiseret i 2 grupper (se nedenstående punkt 1 og 2). Herudover er sikkerhedsarbejdet forankret i de tekniske teams i It og Digitalisering. Desuden er digitaliseringskonsulenterne i forvaltningerne et vigtigt bindeled i forhold til den praktiske gennemførelse af de beslutninger der bliver taget.

1. I-sikkerhedsgruppen (sekretariatscheferne).

Gruppen består af Direktøren, som har ansvaret for It og Digitalisering (formand), It og digitaliseringschefen, Økonomichefen, Sekretariatscheferne for direktørområderne samt Databeskyttelsesrådgiveren (sekretær). Gruppen mødes 4 – 5 gange om året. Alle møder er med intern dagsorden. Gruppen behandler generelle emner.

2. I-sikkerhedsgruppen i It og Digitalisering.

Medlemmerne er It og digitaliseringschefen, Afdelingslederen samt Databeskyttelsesrådgiveren. Gruppen afholder møder 4-5 gange årligt forud for møderne i I-sikkerhedsgruppen. Alle møder er med lukket dagsorden. Gruppen behandler fortrolige emner samt sårbarheder i sikkerheden. Gruppen indstiller sager til behandling i I-sikkerhedsgruppen.

3. Teknisk sikkerhedsarbejde.

De enkelte tekniske teams i It og Digitalisering har it-sikkerheden som et fokusområde. Disse teams rapporterer direkte til ledelsen i It og Digitalisering. Emner bringes op i den lokale I-sikkerhedsgruppe.

4. Organisatorisk sikkerhedsarbejde.

Databeskyttelsesrådgiveren rådgiver forvaltninger i den organisatoriske del af datasikkerheden. Udsender vejledninger, awareness kampagner, opfølgning på hændelser.
Refererer til It og digitaliseringschefen, men når der arbejdes som DPO/Databeskyttelsesrådgiver refereres der direkte til Direktionen.

5. Forankring i forvaltningerne.

Digitaliseringskonsulenterne er det væsentlige bindeled mellem beslutningerne og den praktiske udførelse. Digitaliseringskonsulenterne er i tæt samarbejde med Databeskyttelsesrådgiveren.
Digitaliseringskonsulenterne arbejder fortrinsvis med at registrere nye systemer indenfor deres fagområde. Derudover er de tovholdere i forhold til risiko-analyser, udarbejdelse af databehandleraftaler samt kontrol af disse.
Børn & Unge har iværksat generelle vejledninger på daginstitutions- og skoleområdet, og udarbejder ud fra det overordnede regelsæt lokale retningslinjer

6. Samarbejde mellem jura og DPO.

KL har iværksat et juridisk netværk, som skal forholde sig til de juridiske aspekter i forbindelse med forordningen og den tilknyttede danske lovgivning. Jura har udpeget juridisk kontaktperson i forhold til KL-netværket. Der afholdes møder mellem DPO og juristen én gang månedligt.

7. Viborg.dk og intranet.

Webkoordinatoren udarbejder i samarbejde med DPO vejledningstekster i forhold til oplysningspligten og Viborg Kommunes persondatapolitik (baseret på GDPR).

Dokumentation

I-sikkerhedsarbejdet dokumenteres i sikkerhedsværktøjet Control Manager, men dagsordener journaliseres i Acadre.

Årshjul

Hvert år på det første møde i I-sikkerhedsgruppen (sekretariatscheferne), gennemgås Viborg Kommunes informationssikkerhedspolitik med henblik på godkendelse af eventuelle ændringer.
Årshjulet for de løbende aktiviteter omkring i-sikkerhed justeres løbende og godkendes på I-sikkerhedsgruppens møder.
Årshjulet omfatter 6 aktiviteter – alle aktiviteter er iterative:

A. System- og dataklassifikation

Systemoversigter udarbejdes fremover kontinuerligt. Opgaven er forankret i den enkelte forvaltning, hvor det er digitaliseringskonsulenterne, der er tovholderne. Disse bistås af det lokale medlem af I-sikkerhedsgruppen samt Databeskyttelsesrådgiveren.

Før ibrugtagning af nye systemer, skal data klassificeres, alt afhængigt af om de indeholder almindelige- eller følsomme/fortrolige personoplysninger. Dette danner grundlag for risikovurderingen.

Eksisterende systemer bør mindst 1 gang årligt revurderes i forhold til om der er sket ændringer i klassifikationen af data i systemet f.eks. om der i et system, der hidtil er registreret til blot at behandle almindelige personoplysninger nu tillige behandles følsomme eller fortrolige oplysninger.

B. Risikovurderinger

Risikovurderinger udføres ved ibrugtagning af systemer eller ved væsentlige ændringer.
Sårbarhedsanalysen foretages af It og Digitalisering og eller digitaliseringskonsulenterne.
Konsekvensanalysen foretages af den ansvarlige leder bistået af enten den lokale digitaliseringskonsulent og/eller af Databeskyttelsesrådgiveren. Dette for at give så ensartet et niveau for analyserne.

C. Beredskabsplanlægning og test

It og Digitalisering planlægger årligt en test af It og Digitaliserings beredskabsplan på et udvalgt segment af infrastrukturen. Derudover skal der årligt gennemføres mindst én penetrationstest udført af en ekstern samarbejdspartner på sikkerhedsområdet. Viborg Kommune har i 2. halvår 2017 arbejdet med beredskabsplaner i samarbejde med Midtjysk Brand og Redning i samarbejde med Silkeborg Kommune, og planerne er publiceret pr. 1. januar 2018.

D. Opfølgning, revision m.v.

I-sikkerhedsgrupperne er grundlaget for opfølgningen og ledelsesrapporteringen.

E. Awareness

Awareness, som er opmærksomhedsskabende adfærd hos medarbejderne, er en central del af arbejdet, og skal køre hele året. Awareness kan både være Nanolearning men også undervisning i sikkerhedsrelaterede emner som f.eks. behandling af personoplysninger, sikker post mm. Denne del varetages af Databeskyttelsesrådgiveren i samarbejde med I-sikkerhedsgrupperne.

F. Indgåelse af og opfølgning på databehandleraftaler

Der må ikke tages systemer i brug, hvor personoplysninger behandles eksternt, førend der er indgået en databehandleraftale med leverandøren. Herunder skal der foretages en godkendelse af databehandler og underdatabehandlere. En godkendelse forud for indgåelse af databehandleraftaler sker ved indhentning og gennemgang af seneste revisionserklæring. Alternativt via fysisk tilsyn eller telefoninterview. Notat med beskrivelse af den sikkerhedsmæssige kontrol journaliseres sammen med revisionserklæring og/eller notater. Ingen databehandleraftale må indgås uden databeskyttelsesrådgiverens medvirken.

Det er den enkelte systemejers ansvar, at der årligt udføres en kontrol af, om databehandleren lever op til de krav der er anført i databehandleraftalen med leverandøren. I det omfang databehandleren benytter sig af underdatabehandlere, skal det også sikres, at disse lever op til databehandleraftalen.

Tidspunktet for disse kontroller lægges ind i Control Manager, hvorefter systemet udsender påmindelser til systemejer om, at der skal udføres kontrol inden en bestemt dato.

Der er to former for kontrol:

1. Hvis det af databehandleraftalen fremgår, at der stilles en revisionsrapport til rådighed, gennemgås denne, og hvis der er punkter i denne, som afviger i forhold til kontrolmålene, skal man forholde sig til disse. Er der tale om en revisionserklæring uden anmærkninger, anses kontrolforpligtelsen for udført. Revisionserklæring journaliseres sammen med eventuelle bemærkninger, spørgsmål til og svar fra leverandøren mv.
2. Hvis der ikke er indgået aftale om revisionsrapport påhviler det systemejer, at der udføres en kontrol. Denne kontrol vil være risikobaseret, idet en behandling af fortrolige/følsomme personoplysninger normalt vil indebære et fysisk besøg eller en skriftlig redegørelse (instruks er udarbejdet), hvorimod behandling af almindelige personoplysninger normalt vil kunne udføres ved telefoniske kontroller eller evt. en skriftlig redegørelse. Besøgsrapport eller notat fra telefoninterview journaliseres sammen med eventuelle bemærkninger, spørgsmål til og svar fra leverandøren mv.