Vejledning om pligt til at inddrage databeskyttelsesrådgiveren (DPO)

Organisation	**Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)**
Dokument navn	Vejledning om pligt til at inddrage databeskyttelsesrådgiveren v1.0.docx
Dokument ejer	Daniel Bach, Michael Drews Olsen
Senest ændret	27. august 2018
ISO 27002 reference	18.1.4 - Privatlivets fred og beskyttelse af personoplysninger
GDPR reference	Artikel 38.1 – inddragelse af DPO

Version	Dato	Revisions forfatter	Beskrivelse
1.0	27. august 2018	Daniel Bach	Første version

Formål: Formålet med denne vejledning er at sikre, at DPO'en inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.

Omfang: Alle kommuner og selvejende institutioner tilsluttet den fælles databeskyttelsesrådgiverfunktion i DSD.

Lovkrav
Kommunen har pligt til at sikre rettidig og tilstrækkelig inddragelse af DPO'en i alle spørgsmål vedrørende beskyttelse af personoplysninger, jf. persondataforordningens artikel 38, stk.1.

Pligten til at sikre inddragelse af DPO'en gælder i forhold til alle kommunens spørgsmål vedrørende beskyttelse af personoplysninger. Det skal for god ordens skyld bemærkes, at DPO'en ikke skal inddrages, blot fordi kommunens ansatte har spørgsmål til behandling af personoplysninger.

Rettidig og tilstrækkelig inddragelse
Pligten til rettidig og tilstrækkelig inddragelse betyder, at kommunen i god tid skal inddrage DPO'en, således at kommunen kan tage højde for DPO'ens rådgivning eller anbefalinger i forbindelse med kommunens beslutninger. Det betyder, at DPO'en skal inddrages i så god tid, at DPO'en kan foretage en egentlig vurdering af det forhold, som DPO'en inddrages i.

Kommunen skal forsyne DPO'en med fornødne oplysninger, hvis det er nødvendigt for DPO'ens rådgivning, således at DPO'en kan foretage en vurdering på et kvalificeret grundlag.

Inddragelse i alle spørgsmål vedrørende beskyttelse af personoplysninger
Pligten til at inddrage DPO'en omfatter som udgangspunkt alle spørgsmål om kommunens og databehandlerens overholdelse af de regler i forordningen, herunder nationale regler om databeskyttelse, som kommunen og databehandleren skal overholde[1].

Pligten til at inddrage DPO'en i alle spørgsmål vedrørende beskyttelse af personoplysninger betyder for det første, at DPO'en skal inddrages i kommunens overvejelser og vurderinger om, hvorvidt behandlinger, som der foretages eller skal iværksættes, efterlever hjemmelskrav. Det samme gælder i forhold til kommunens overvejelser om, hvorvidt behandlinger overholder grundlæggende behandlingsprincipper.

Pligten betyder for det andet, at DPO'en skal inddrages i kommunens vurderinger og overvejelser om, hvorvidt og hvorledes de registreredes rettigheder skal efterleves, herunder i kommunens overvejelser om passende foranstaltninger for efterlevelse af reglerne.

For det tredje betyder pligten, at DPO'en skal inddrages i kommunens vurderinger og overvejelser om overholdelse af pligterne med hensyn til gennemførelse af fornødne sikkerhedsforanstaltninger, indgåelse af databehandleraftaler, udarbejdelse af behandlingsfortegnelser samt anmeldelser til Datatilsynet og/eller underretning af registrerede i tilfælde af brud på persondatasikkerheden.

Kommunen har herudover pligt til at rådføre sig med DPO'en, hvis kommunen skal foretage en konsekvensanalyse i henhold til forordningens artikel 35. Pligten til at rådføre sig med DPO'en i forbindelse med konsekvensanalyse er særskilt reguleret i artikel 35.

Anbefalinger
Kommunen bør sikre formaliseret, struktureret og ensartet inddragelse af DPO'en. Det kan kommunen sikre ved udarbejdelse af retningslinjer eller procedurer, herunder ved forankring af ansvaret for

[1] Betænkning nr. 1565, bind 1, kapitel 5.20., side 576

inddragelse af DPO'en i kommunens organisation f.eks. i teams, udvalg eller råd, som varetager complianceopgaver efter persondataforordningen.

I det omfang der i kommunen allerede foreligger retningslinjer eller procedurer vedrørende complianceopgaver efter forordningen, bør DPO'en indtænkes i disse, hvor det er relevant (se straks nedenfor).

Det anbefales navnlig at sikre formaliseret, struktureret og ensartet inddragelse af DPO'en i forhold til følgende:

- Risikovurderinger og gennemførelse af passende sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til risici forbundet med behandlingen af de pågældende personoplysninger.

- Nye projekter i kommunen eller ved anskaffelse og ibrugtagning af nye systemer i kommunen, som involverer behandling af personoplysninger, herunder ved ændringer af igangværende behandlingsaktiviteter ved brug af nye teknologier.

- Kravspecifikationer ved indkøb af nye it-systemer hvor der behandles personoplysninger (bl.a. krav om privacy by design og embedded privacy).

- Pligt til konsekvensanalyse (DPIA)

Officielle kilder:

Persondataforordningen artikel 38, stk. 1.
Datatilsynets Vejledning om databeskyttelsesrådgivere (December 2017) sektion 5.4 https://www.datatilsynet.dk/media/6561/databeskyttelsesraadgivere.pdf
ISO 27002 reference: 18.1.4 - Privatlivets fred og beskyttelse af personoplysninger
Betænkning nr. 1565, bind 1, kapitel 5.20.

Bilag (standardinformation i vejledninger fra databeskyttelsesrådgiverfunktionen i Den Storkøbenhavnske Digitaliseringsforening)

Ansvarsfordeling:
[Kommunalbestyrelsen] fastlægger og godkender den overordnede sikkerhedspolitik og strategi for overholdelse af persondataforordningen.

Den [Centeransvarlige] / [fagansvarlige] er bekendt med sikkerhedspolitikker, retningslinjer og procedurer for overholdelse af persondataforordningen og sikre at disse er indarbejdet i projekter eller ved anskaffelse og ibrugtagning af fag-systemer hvori der behandles personoplysninger, dette kan blandt andet ske igennem inddragelse af databeskyttelsesrådgiveren.

[Sikkerhedsansvarlige]/[IT-ansvarlige] sikre at sikkerhedspolitikker, retningslinjer og procedure beskriver i hvilke situationer databeskyttelsesrådgiveren skal inddrages i projekter og/eller ved anskaffelse og ibrugtagning af fag-systemer hvori der behandles personoplysninger.

Kommunens [Indkøbsafdeling] er bekendt med sikkerhedspolitikker, retningslinjer og procedurer for overholdelse af persondataforordningen og sikre at databeskyttelsesrådgiveren inddrages ved udbud eller anskaffelse af fag-systemer hvori der behandles personoplysninger.

Definitioner:

»Sikkerhedskoordinator«: En sikkerhedskoordinator er databeskyttelsesrådgiverens primære kontaktperson i kommunen. Sikkerhedskoordinatorer deltager i regelmæssige møder med andre DSD kommuner for at harmonisere tilgangen til sikkerhed og compliance. Sikkerhedskoordinatoren har også et privilegeret samarbejde med kommunens sikkerhedsansvarlige og fagcentre.

»Fagansvarlig«: En fagansvarlig bærer typisk rollen som dataansvarlige. Efter forordningen er Dataansvarlig en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

»Fagcenter«: Kommunen er opdelt i forskellige enheder med fokus på et specifikt pligtområde (forvaltninger, afdelinger, centre). Disse enheder kalder vi fagcentre. Et fagcenter har en eller flere [fagansvarlig], der bærer rollen som dataansvarlige.

»Dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

»Behandling«: enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

»Register«: enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier, hvad enten denne samling er placeret centralt eller decentralt eller er fordelt på funktionsbestemt eller geografisk grundlag

»Personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.
Forordningen opdeler personoplysninger i 3 kategorier: Følsomme Personoplysninger, Oplysninger om Strafbare forhold og Almindelige Personoplysninger.

Følsomme Personoplysninger jf. GDPR artikel 9
• Racemæssig eller etnisk oprindelse • Politisk, religiøs eller filosofisk overbevisning • Fagforeningsmæssige tilhørsforhold • Behandling af genetiske eller biometriske data med henblik på unik identifikation • Helbredsoplysninger • Oplysninger om en persons seksuelle forhold eller seksuelle orientering • CPR-nummer behandles som en Følsom Personoplysning
Oplysninger om Strafbare jf. GDPR artikel 10
• Straffedomme • Lovovertrædelser
Eksempler på Almindelig Personoplysninger
• Navn, adresse, telefonnummer, e-mail • Køn • Fødselsdato • Familieforhold • Ansøgning og CV • Løn • Arbejdstider • Sygedage (men ikke årsagen, som er en følsom personoplysning) • Skat og gæld • Nummerplade • Oplysninger om strafbare forhold • Sociale problemer • Andre rent private forhold end følsomme oplysninger