

Databeskyttelsesrådgivernes årsrapport 2018

til kommunalbestyrelsen i

Hørsholm Kommune

Introduktion til databeskyttelsesrådgiverne.....	2
Samarbejdet	2
Netværk	2
DPO leverancer	2
Databrud	3
Typen af sikkerhedsbrud	3
Niveauet for sikkerhedsbrud	3
Databehandleraftaler.....	4
Borgerhenvendelser	4
Ressourcer og modenhed.....	5
Forventninger til 2019	5
Afslutnings kommentar.....	6

Introduktion til databeskyttelsesrådgiverne

Vi startede i vores rolle som databeskyttelsesrådgivere (DPO) i maj 2018. Vores opgave består i at rådgive og vejlede kommunen og dens borgere, i håndteringen af persondataforordningen (GDPR), hjælpe med at kommunen overholder de databeskyttelsesretlige regler og være et kontaktpunkt for Datatilsynet.

Vi har vores faste kontor i Fredensborg, hvilket vi er meget tilfredse med, det fungerer godt i forhold til transport mellem de forskellige arbejdssteder.

Samarbejdet

Vi udfylder vores DPO-rolle i Nordsjællands Digitaliserings Samarbejde (NDS), der er et udviklingssamarbejde mellem 7 kommuner¹.

Det har fra starten været vigtigt for os, at have et tæt samarbejde med alle 7 kommuner, og vi oplever at vores samarbejde med alle kommunerne er rigtig godt. Der er en god dialog og vi inddrages ofte i sager der vedrører persondata.

Vi tilstræber at fordele vores tid ligeligt og efter behov, til alle NDS kommunerne, og vælger ofte at være "på besøg" en hel arbejdsdag. Det giver kollegaerne mulighed for at komme til at kende os og henvende sig, hvis de har spørgsmål. Det er vigtigt for os, at viden om GDPR metoder, procedurer og vejledninger deles på tværs af kommunerne.

Netværk

Tidligt i vores ansættelse, opsøgte vi muligheden for at netværke med andre, som varetager DPO rollen. Det er en god mulighed for at høre om andres erfaringer og udfordringer. Vi vil gerne være med i et netværk, for at fortælle om vores håndtering af GDPR og forhåbentlig få noget retur, som kan bruges i det videre arbejde med implementeringen af GDPR.

Sammen med 2 DPO'er fra "Den Storkøbenhavnske Digitaliseringsforening", har vi taget initiativ til at etablere en netværksgruppe for kommunale DPO'er. Netværksgruppen har nu afholdt 3 møder og den er blevet udvidet, så vi nu består af 10 personer, som varetager DPO rollen, tilsammen dækker vi 25 kommuner.

DPO leverancer

I forbindelse med implementeringen af GDPR per 25. maj 2018, er der kommet en række krav til hvordan kommunen skal behandle persondata. For at imødekomme disse krav, har vi skrevet nogle vejledninger, fx til brug af foto og video, anvendelse af sociale medier, samt et bilag til kravspecifikation ifm. ny-indkøb af IT systemer.

Derudover har vi lavet et GDPR årshjul, månedlige nyhedsbreve og tilpasning af databehandleraftaler, så de er mere målrettet mod de enkelte leverandører.

¹ Fredensborg, Hørsholm, Hillerød, Helsingør, Gribskov, Halsnæs, Frederiksund

Vi bliver jævnligt kontaktet vedrørende spørgsmål til GDPR. Henvendelserne omhandler mange forskellige områder, så som skoler, institutioner, bosteder m.m.

Databrud

Som følge af de nye regler i databeskyttelsesforordningen, blev det efter den 25. maj et krav, at sikkerhedsbrud, som udgangspunkt skal anmeldes til Datatilsynet, og besked gives til de berørte borgere. Med til reglerne hører, at underretning til Datatilsynet skal ske indenfor en forholdsvis kort tidsfrist, 72 timer fra bruddet er konstateret. Der er blevet ført statistik over antallet og karakteren af hændelser, der har fundet sted i Hørsholm Kommune, siden forordningen trådte i kraft. Nedenfor er opført antallet af hændelser, og hvor mange der er blevet anmeldt til Datatilsynet.

- 25 registrerede hændelser
- 7 hændelser er anmeldt til Datatilsynet

Når en hændelse ikke anmeldes til Datatilsynet, skyldes dette at dens alvorlighed, er blevet vurderet til at ligge under en bagatelgrænse.

Der kan dog observeres en tendens til, at hændelserne primært foregår i centre, hvor der i højere grad er tæt kontakt med borgere. Eksempler på sådanne centre er Center for Arbejdsmarked og Center og Borgerservice, IT og Digitalisering.

Typen af sikkerhedsbrud

Langt størstedelen af de hændelser der er blevet registreret og anmeldt til Datatilsynet, har været forårsaget af menneskelige fejl, hvor medarbejderen ved et uheld har videregivet personoplysninger til den forkerte modtager.

I de centre hvor hændelserne har fundet sted, har der efterfølgende været sat fokus på at forhindre denne type af fejl i at gentage sig. Til dette formål har vi generelt opfordret til, at hændelserne anvendes som læringsværktøjer, således at man i fællesskab tager ved lære af sådanne fejl og dermed forhindrer at de samme typer af sikkerhedsbrud sker i fremtiden.

Parallelt hermed afsøges der ligeledes mulighed for at minimere risikoen for fejl, ved hjælp af tekniske løsninger.

Niveauet for sikkerhedsbrud

I forhold til det store antal behandlingsaktiviteter, der til daglig foretages i kommunen, giver dette antal af hændelser ikke umiddelbart anledning til bekymring.

Tværtimod illustrerer registreringerne at man i forvaltningen, er bevidst omkring og reagere på den omstændighed, at sådanne hændelser skal indberettes. En bevidsthed som vores erfaringer har vist os, ikke er en selvfølge, men derimod et resultat af målrettede oplysningskampagner. Som fx den informationssikkerhedskampagne, der i Hørsholm Kommune blev gennemført i 2018.

Denne formodning underbygges desuden af de tendenser vi ser på tværs af de kommuner, som vi varetager DPO-rollen for.

Databehandleraftaler

Som offentlig myndighed er det vigtigt, at kommunen efterlever gældende lovgivning på området, eksempelvis at der er indført passende behandlingssikkerhed som fastsat i Databeskyttelsesforordningen. Det betyder, at der skal laves databehandleraftaler med leverandører, angående behandling og udveksling af personoplysninger. Det skal gøres for at sikre, at leverandøren beskytter data ligeså forsvarligt, som kommunen selv gør. Hvis kommunen har et højt beskyttelsesniveau, til de data som leverandøren behandler, så skal leverandøren have implementeret det samme niveau.

Status for Hørsholm Kommunes databehandleraftaler er følgende:

Der er registreret 183 aftaler i Acadre (journal-system).

- ca. 143 er underskrevet og afsluttet
- ca. 40 i proces fra "modtaget" til "godkendt- afventer underskrift".
10 af disse mangler blot underskrift og journalisering.

Det betyder, at mere end 80 % af aftalerne er på plads. Da hver aftale kan være ret kompleks og ofte kræver flere iterationer, samt at der er en behandlingstid hos leverandøren, er det et forventeligt niveau der er nået, det gælder også når vi sammenligner med de øvrige 6 kommuner i NDS. Det forventes at de resterende aftaler er underskrevet og journaliseret senest i 2. kvartal 2019.

Det er ikke alle aftaler, som er blevet behandlet og registeret af sikkerhedsteamet. Derfor *kan* der være flere aftaler på ikke-it områder, fx social-, og børn- og ungeområdet. Det er endnu ikke fuldt afdækket.

Borgerhenvendelser

Det hører med til DPO-rollen, at rådgive borgerne om deres rettigheder i forhold til persondataforordningen, samt besvare spørgsmål omkring kommunens behandling af deres personoplysninger.

Vi har i tiden efter den 25. maj, kun oplevet et meget begrænset antal henvendelser fra borgere, angående spørgsmål af den ovenstående karakter, alt i alt er der tale om en håndfuld. Henvendelserne vi har fået i Hørsholm Kommune, har primært drejet sig om sletning af oplysninger, indsigt i egne oplysninger eller spørgsmål af mere generel karakter.

På tværs af de syv kommuner, oplever vi generelt en lille stigning af henvendelser fra borgere, og vi forventer at denne tendens vil øges, i takt med at kendskab til DPO-rollen stiger, hvilket naturligvis må kunne forventes, da en beskrivelse af vores funktion og kontaktoplysninger, nu fremgår af de oplysninger, kommunen er forpligtiget til at give borgere, når der indsamles oplysninger om disse.

Vi forventer således at henvendelser fra borgere, langsomt vil begynde at fylde mere i løbet af 2019.

Ressourcer og modenhed

I vores arbejde med GDPR, på tværs af de syv kommuner, kan vi umiddelbart konstatere en tydelig sammenhæng mellem omfanget af de ressourcer, der har været dedikeret til GDPR-projektet, og den modenhed man på nuværende tidspunkt har opnået i sin organisation.

En sådan sammenhæng må man selvfølgelig også kunne forvente. Vores erfaringer understreger således blot den umiddelbart naturlige antagelse, at det er en forudsætning for en forsat fremgang og forbedring af compliance-niveauet, at der er afsat tilstrækkelige ressourcer til at drive projektet frem.

Vi oplever at Hørsholm Kommune, overordnet set har haft succes med at informere medarbejdere og ledelse, om deres ansvar for at efterleve kravene i databeskyttelsesforordningen, hvilket man har gjort via flere fællesmøder, informationskampagner mv.

Til dette formål er der blevet etableret en programorganisation, hvis formål det har været at forankre GDPR-compliance-arbejdet i kommunen. I denne gruppe, er der blevet arbejdet intensivt med implementering af kravene i GDPR. Dette har medført en bred vifte af aktiviteter, bl.a. indgåelse af databehandleraftaler, gennemgang af processer, udfyldelse af fortegnelser over behandlingsaktiviteter, styrkelse af den digitale sikkerhed, opdatering af sikkerhedspolitikker, svar på organisations spørgsmål om behandling af personoplysninger, samt en lang række andre GDPR relaterede opgaver.

Fremover er det planen, at der for hvert center bliver udnævnt en GDPR-ambassadør eller tovholder, disse vil herefter understøtte den lokale ledelse og kollegerne, i arbejdet med efterlevelse af GDPR-kravene.

Samlet set, er vores indtryk at Hørsholm Kommune tager efterlevelsen af reglerne i forordningen særdeles alvorligt, og vi ser frem til et 2019, hvor der i kommunen forsat vil være skarp fokus på efterlevelsen af de persondataretlige regler.

Forventninger til 2019

Hørsholm kommune er kommet langt med implementeringen af GDPR, men er endnu ikke i mål. Det betyder at i 2019, skal kommunen, sammen med DPO'erne, forsat arbejde med at få processer/procedurer, arbejdsgange, systemer m.m. tilpasset, så de efterlever persondataforordningen. Det vil også være i løbet af 2019, at der skal føres en intern audit (selvkontrol) med overholdelsen af GDPR reglerne. Hørsholm Kommune har modtaget et oplæg til et GDPR årshjul fra os. Vi opfordrer til at det skal integreres med andre årshjul (hvis haves), så det bliver en samlet oversigt med aktiviteter omhandlende IT sikkerhed.

For at Hørsholm Kommune skal opnå et tilstrækkeligt niveau af compliance med GDPR-reglerne, forventer vi at der særligt vil være fokus på disse emner:

- Varetagelse af borgernes rettigheder
- Indgåelse af databehandlaftaler og kontrol af disse
- Fortsættelse af awareness programmer
- Løbende fokus på de tekniske og organisatoriske foranstaltninger
 - o Slette-procedure
 - o Opbevarings-procedure
 - o Kontrol af brugerautorisationer/adgangskontrol
 - o Uddelegering af ansvar
- Dokumentation af reglernes overholdelse
- Fortegnelse over behandlingsaktiviteter

Afslutnings kommentar

Vi er overbeviste om at det gode samarbejde vil fortsætte ind i 2019. Det er realistisk, at Hørsholm Kommune vil opnå det ønskede compliance niveau inden udgangen af 2019. Hvorved den øgede sikkerhed, vil være medvirkende til at fremme borgernes tillid til kommunens håndtering af deres data.

Beskyttelse af borgernes interesser, i forbindelse med behandlingen af personoplysninger, er en grundlæggende rettighed. Den dataansvarlige (kommunen), har således en forpligtigelse til at behandle disse oplysninger med stor respekt og påpasselighed. Som følge af de udfordringer, den hastige teknologiske udvikling skaber, vil der i stigende grad være behov for at den retlige og praktiske sikkerhed styrkes, i forhold til borgernes og medarbejdernes personoplysninger.

Det er vores vurdering og konklusion, at Hørsholm Kommunes arbejde med implementeringen af GDPR, varetages af en kvalificeret og kompetent gruppe af medarbejdere. En forsat fremdrift af implementeringsarbejdet forudsætter dog, at der i organisationen fortsat afsættes tilstrækkelige ressourcer, til at kommunen, også fremadrettet, vil kunne håndtere de forpligtigelser og udfordringer der følger af forordningens regler.