FREDERIKSSUND KOMMUNE

Databeskyttelsesrådgivernes årsrapport 2019 til Byrådet i Frederikssund kommune

Indledning

Denne rapport er udarbejdet med henblik på at informere kommunens øverste ledelse om status på Frederikssund Kommunes overholdelse af databeskyttelsesreglerne - som fastlagt i EU-Databeskyttelsesforordningen (GDPR) (EU 2016/679), samt i de danske vedtagne bestemmelser om samme (Databeskyttelsesloven nr. 502 af 23/05/2018).
I årsrapporten for 2019 vil vi forsøge at give et indblik i arbejdet med databeskyttelses-forordningen (GDPR) i Frederikssund Kommune.

Det er passende at se tilbage og gøre status på den fortsatte tilpasning og implementeringen af GDPR i Frederikssund Kommune. Vi vil sætte fokus på nogle af de emner der har været særlig opmærksomhed på, fra enten kommunen selv, os DPO'er og Datatilsynet.

Til sidst i rapporten vil vi komme med nogle anbefalinger til arbejdet med databeskyttelse for 2020.

Samarbejdet med nøgleressourcer i kommunen

Vi har et tæt og god kontakt med kommunens GDPR nøgleressourcer. Det gælder både fra distancen og når vi har tilstedeværelsesdage på rådhuset. Samarbejdet fungerer godt, det er tydeligt at GDPR nøgleressourcerne har taget ejerskab af opgaven og de har været gode til at formidle regler og vejledning bredt i organisationen. Vi oplever at de bruger os til sparring og rådgivning når der opstår et behov.

Borgerhenvendelser

I vores rolle som databeskyttelsesrådgivere skal vi stå til rådighed, både for kommunens ansatte og for kommunens borgere. I takt med at Frederikssund Kommune har opfyldt sin oplysningspligt på diverse skemaer, formularer m.m. er borgerne blevet oplyst om, at de kan kontakte kommunens databeskyttelsesrådgiver, hvis de fx har spørgsmål vedrørende kommunens håndtering af persondata. Det er ikke noget der tager meget af vores tid.

DPO funktionen

Det er et grundlæggende krav, at en databeskyttelsesrådgiver ikke må blive instrueret af andre om, hvordan rådgiveren skal udføre sine opgaver. Databeskyttelsesrådgiverne rapporterer direkte til øverste ledelsesniveau (jf. Datatilsynet). Evaluering og afrapportering af status sker løbende til styregruppen for Nordsjællands Digitaliserings Samarbejde (herefter NDS), samt én gang årligt ved aflæggelse af rapport til byrådet.

Det er fortsat en vigtig opgave for os, at rådgive og vejlede Frederikssund Kommune i håndteringen af GDPR, både når det gælder enkelt sager og når vi kommer med en generel udmelding som kan bruges på af alle NDS kommunerne. De generelle sager, kan fx omhandle håndteringen af et databrud hos en leverandør, der har aftaler med flere NDS kommuner. I de tilfælde vil vores vejledning ofte være enslydende for de berørte kommuner.

Henvendelse fra Datatilsynet, vedrørende DPO

I 2019, har Frederikssund Kommune modtaget 2 henvendelser fra Datatilsynet, hvor de efterspørger oplysninger vedrørende DPO'ernes faglige kvalifikationer, ressourcer og opgaver.

Spørgsmålene til første besvarelse, omhandlede DPO'ernes uddannelse, opdatering af GDPR relevante kompetencer, kendskab til den kommunale forvaltning, inddragelse ang. beskyttelse af personoplysninger m.m. Henvendelse blev rettidigt besvaret ultimo juni 2019.

Spørgsmålene til anden besvarelse, omhandlede DPO'ernes opgavevaretagelse vedr. at føre tilsyn med kommunens overholdelse af databeskyttelsesreglerne, inkl. planlagte/ikke planlagte kontroller. Henvendelse blev rettidigt besvaret primo november 2019.

Svarene til Datatilsynet er foretaget af DPO'erne samt relevante ressourcer i Frederikssund kommune. Samme henvendelse har de øvrige NDS kommuner også modtaget. Det er endnu uvist hvordan Datatilsynet forholder sig til besvarelserne, da vi ikke har modtaget en afgørelse.

Henset til Datatilsynets egen vejledning om databeskyttelsesrådgivere, kan der forventes kritik i forhold til det niveau af ressourcer der er dedikeret til opgaven.

Ressourcer

DPO'erne har bl.a. opgaven med at vejlede om databeskyttelsesreglerne, at overvåge kommunens overholdelse, rådgive om tilpasning af processer, foreslå forbedrende tiltag og meget andet. Det er dog kommunen der har ansvaret for at sikre at behandling af personoplysninger sker i overensstemmelse med Databeskyttelsesforordningen og for at varetage de driftsopgaver dette medfører. I den forbindelse er det en del af kommunens ansvar, at der udpeges tilstrækkelige ressourcer til at kunne håndtere denne opgave.

Uddelegering af ansvar til centerledelsen

Frederikssund Kommune etablerede et informationssikkerhedsudvalg medio 2019. Gruppen har det overordnede ansvar for optimeringen af GDPR i Frederikssund Kommune. Det daglige ansvar for overholdelse af Databeskyttelsesforordningen er, i Frederikssund Kommune, placeret hos centercheferne. Dermed er "ejerskabet" af de enkelte GDPR opgaver blevet fordelt på flere ledere. Det har den fordel at hvert center får en bedre mulighed for at tilpasse ressourcer og tid til at løfte de pålagte GDPR opgaver.

Nøgleressourcer

Den daglige håndtering af kommunens GDPR aktiviteter, varetages af meget få ressourcer. De har ydet et stort arbejde med at udbrede awareness af GDPR, og af den grund er det vores indtryk, at kommunens ansatte har et fornuftigt kendskab til GDPR reglerne.

Når vi ser på forholdet mellem en kommunes GDPR-modenhed og de udpegede GDPR ressourcer, vil der ofte være en direkte sammenhæng. Jo flere ressourcer, der bruger dele af deres tid på GDPR opgaver, des hurtigere opnås kommunens ønskede GDPR-modenheds niveau. Vi har vurderet at Frederikssund Kommune har opnået et forholdsvis højt modenheds niveau, og det på trods af et lavt antal GDPR nøgleressourcer. For at opretholde og fortsat skærpe modenheden, er det nødvendigt at den aktuelle GDPR bemanding, som minimum bibeholdes, og gerne udvides til at omfatte flere lokale center-ressourcer, der bliver dedikerede til opgaven med at varetage dele af GDPR aktiviteterne i eget center.

Databehandleraftaler

I medhør af Databeskyttelsesforordningen er det en forpligtigelse for kommunen, at der indgås skriftlige aftaler med samtlige af de leverandører, som behandler personoplysninger på kommunens vegne. Det følger i forlængelse heraf, at kommunen har en forpligtigelse til løbende, at føre tilsyn med at personoplysninger behandles på en måde, der er i overensstemmelse med de persondataretlige regler.

Håndteringen af databehandleraftaler består bl.a. af forhandling om indgåelse, vedligehold af indhold og tilsyn med aftalen, hvilket tilsammen indebærer en væsentlig administrativ byrde for en organisation, som en kommune, der i sin natur til daglig behandler personoplysninger i stort omfang.

Kommunen har i samarbejde med databeskyttelsesrådgiverne og arbejdsgrupper i Nordsjællands Digitaliseringssamarbejde, udarbejdet værktøjer til hjælp ved indgåelsen, og den efterfølgende kontrol med kommunens databehandleraftaler. I tilknytning hertil, har kommunens informationssikkerhedskoordinator udarbejdet proces for Tilsyn og kontrol og afholdt workshops for at ruste udvalgte medarbejdere i centrene til denne arbejdsopgave.

Det er blevet besluttet at ansvaret for tilsynet med kommunens databehandlere varetages af de enkelte centre, der til daglig benytter systemet. IT-afdelingen har ansvaret for tilsynet med en række større tværgående systemer. Kommunens informationssikkerhedskoordinator vil i forbindelse med centrenes tilsyn bidrage med råd og vejledning om udførelse af opgaverne.

Ved udgangen af 2019, havde Frederikssund Kommune ført tilsyn med sine primære leverandører af IT-systemer. Der udestår således et antal leverandører som kommunen ikke har ført tilsyn med, vi bemærker i den forbindelse, at dette er et forhold, der vil kunne medføre kritik og evt. andre sanktioner fra Datatilsynet.

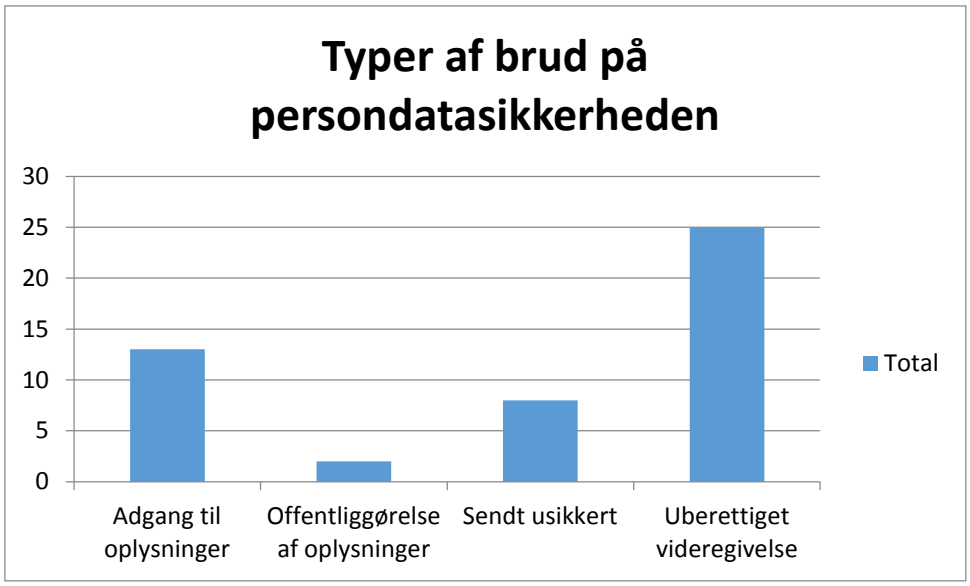
Databrud

Det har siden 25. maj 2018, været en forpligtigelse for kommunen at føre en intern liste over samtlige brud på persondatasikkerheden, og herunder indberette hændelser af en vis alvorlighed til Datatilsynet. Brud på persondatasikkerheden dækker primært over hændelser hvor personoplysninger videregives til den forkerte, uberettiget offentliggørelse af fortrolige oplysninger, utilsigtet sletning af oplysninger eller hændelser hvor personoplysninger har været utilgængelige i længere perioder.

Frederikssund Kommune har implementeret en fast proces for administrationens håndtering af brud på persondatasikkerhed. Det kan konstateres at der i perioden 1.1.2019 – 31.12-2019 er blevet registreret 48 antal brud på persondatasikkerheden i Frederikssund Kommune. Heraf er 22 blevet indberettet til Datatilsynet, og i 17 tilfælde har kommunen valgt at underrette de registrerede om sikkerhedsbruddet.

Typer af brud

Når vi kigger nærmere på typen af disse hændelser tegner der sig dette billede:



I forhold til typer af persondatabrud er adgang til oplysninger og uberettiget videregivelse, de to poster der samlet tegner sig for langt størstedelen af brud i Frederikssund Kommune.

Typen "adgang til oplysninger", dækker dette over situationer, hvor utilstrækkelige sikkerhedsforanstaltninger har gjort det muligt for uvedkommende at få adgang til kommunens personoplysninger. Denne type af brud er generelt kendetegnet ved at de opstår i forbindelse med systemfejl hos en af kommunens IT-leverandører. Erfaringen viser at denne type fejl hurtigt bliver rettet efter de er blevet konstateret, og at de samme fejl sjældent gentager sig.

Det bemærkes dog at kommunen i forbindelse med sine tilsyn med leverandører, skal være opmærksom på en leverandørs historik i forhold til brud på persondatasikkerheden.

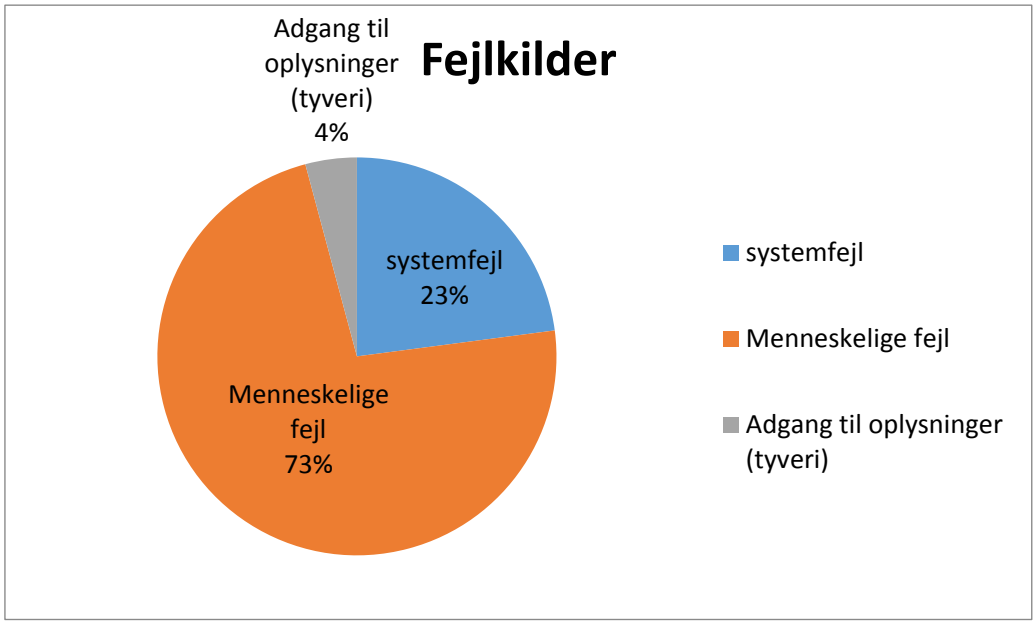
Typen "uberettiget videregivelse" dækker derimod typisk den situation, hvor en kommunal medarbejder har sendt konkrete oplysninger til den forkerte modtager, enten med digital eller fysisk post. Disse hændelser kan have forskellige karakter, men er overordnet kendetegnet ved at de grundlæggende skyldes menneskelige fejl. De pågældende medarbejdere er i disse situationer blevet instrueret i at vise større agtpågivenhed i fremtiden. Oftest har fejlene skyldtes uhensigtsmæssige arbejdsgange eller travlhed.

Typerne "offentliggørelse af oplysninger" dækker over - papirer med personoplysninger efterladt i åbent kælderrum og "sendt usikkert" dækker over flere tilfælde hvor en kommunal medarbejder har sendt digital post indeholdende personfølsomme data og glemt at anvende funktionen "send sikkert" i mail-systemet.

På baggrund af en gennemgang af hændelserne vedrørende "uberettiget videregivelse", er det konstateret, at medarbejderen ofte opdager fejlen kort tid efter at vedkomne har sendt til den forkerte modtager. Det betyder at en stor del af disse hændelser sandsynligvis kunne være undgået, hvis der i afsendelsen af digital post, havde været en ganske kort forsinkelse, der

kunne gøre IT-afdelingen i stand til at stoppe forsendelsen. Hermed vil et databrud være undgået og oplysningerne vil ikke være kommet til uvedkommendes kendskab.

Fejlkilder



Som det fremgår af ovenstående diagram, kan det overordnet konstateres at hovedparten af det samlede antal sikkerhedsbrud skyldes menneskelige fejl. Kommunen forsøger løbende at minimere denne risiko ved løbende oplysning og undervisning af medarbejdere, som det også fremgår af afsnittet nedenfor. Det kan derudover konstateres at kommunen til stadighed foretager opdateringer og tilpasninger af IT-sikkerheden, med det overordnede formål at forhindre både menneskelige og systemmæssige fejl.

Awareness

Frederikssund Kommune har et grundlæggende ansvar for at sikre at medarbejdere der beskæftiger sig med personoplysninger i deres dagligdag, har en forståelse for de regler og forpligtigelser der knytter sig hertil. Det er derfor en forudsætning, at kommunens ansatte løbende instrueres i Databeskyttelsesforordningens regler, for at kommunen kan leve op til sit ansvar.

Frederikssund Kommune har i løbet af 2019 varetaget denne forpligtigelse igennem en række forskelligartede aktiviteter, hvor det overliggende mål har været at højne organisationen kendskab til de persondataretlige regler. Aktiviteterne har primært været organiseret af kommunens informationssikkerhedskoordinator. Vi har i den forbindelse varetaget vores rolle igennem løbende sparring og vejledning.

Som en række eksempler på de aktiviteter der har været igangsat i kommunen kan bl.a. nævnes:

- Nye medarbejdere bliver orienteres omkring de persondataretlige regler ved obligatoriske intromøder, der afholdes en gang om måneden
- Kommunens informationssikkerhedskoordinator er løbende rundt i organisationen og uddanne medarbejdere i god behandling af personoplysninger
- Der tilbydes løbende kurser i informationssikkerhed og databeskyttelse via kommunes kursuskatalog (hvert kvartal)
- Der tilbydes kursus målrettet system- og dataejere via kommunens kursuskatalog
- På Kommunens intranet bliver der løbende delt materiale der skal styrke medarbejdernes kendskab til GDPR
- Kommunen har i deres arbejde med god behandling af persondata, inddraget pårørende til sårbare borgere i kommunale tilbud, med henblik på at sikre de korrekte rammer, i forhold til videregivelse af personoplysninger
- Der er blevet arbejdet målrettet på indholdet af medarbejder kurser, der skal gøre ledere og systemansvarlige bekendte med deres særlige forpligtigelse i forhold til GDPR
- Der er løbende blevet udarbejdet nye vejledninger mv. Disse sendes direkte til relevante interessenter

Compliance og dokumentation

Det er en forudsætning for overholdelse af kravene i Databeskyttelsesforordningen, at den dataansvarlige har et struktureret overblik over de tiltag, der er nødvendige for at organisationen løbende overholder de forpligtigelser der følger af forordningen, herunder kravet om dokumentation. Et eksempel på et sådan overblik kan f.eks. sikres ved anvendelsen af et årshjul, der skal sikre at organisationen løbende får kontrolleret, at de implementerede tiltag lever op til de persondataretlige regler. I et sådan årshjul noteres de primære kontrolpunkter, som organisationen har udpeget, og det kan fremgår hvornår i løbet af året kontrollerne skal udføres.

Frederikssund Kommune har i løbet af 2019 udarbejdet et sådant årshjul, der indeholder en række væsentlige opgaver, der skal varetages i henhold til GDPR. Processen er blevet godkendt i kommunens informationssikkerhedsudvalg.

Ude i centrene, har årshjulet ikke været taget aktiv i brug, i løbet af 2019. Det oplyses at der i forbindelse med udrulningen af årshjulet blev konstateret et behov for at udvikle kompetencerne hos de medarbejdere, der planmæssigt skal varetage opgaverne i det daglige.

Anbefalinger til 2020

Vi anbefaler at:

- Kommunen forsat afsøger muligheden for etablere en løsning der kan forsinke fremsendelse af e-mail og digital post, med det formål at begrænse risikoen for at oplysninger havner i uvedkommendes hænder.
- Kommunen bibeholder fokus på at føre sine tilsyn med databehandlere, og at der afsættes tilstrækkelige ressourcer i centrene, til at løfte denne opgave.
- At organisation i løbet af 2020 gør aktiv brug af GDPR årshjulet og arbejdet med at gøre dette til en integreret del af centrenes arbejdsopgaver.
- Det af Kommunen indkøbte scannings-værktøj (Formpipe kvalitetskontrol), overgår fra test-fase til prod-fase - det kan understøtte fx vedr. sletteregler, oprydning af persondata på fil-drev og minimering af åbne sager i kommunens ESDH system
- At kommunen yderligere undersøger mulighederne for indkøb af en RPA løsning (robot-teknologi), der kan understøtte kommunen i forskellige rutinemæssige arbejdsprocesser.
- At kommunen, som minimum, opretholder den aktuelle GDPR bemanding, og dermed fortsat kan skærpe modenheden på området ang. håndteringen af persondata.