Koncern IT
Økonomiforvaltningen

Orienteringssag

Status og risikovurdering af informationssikkerheds-området til Økonomiudvalget 2020

16. februar 2021

Sagsnummer
2021-0051372

Dokumentnummer
2021-0051372-1

Økonomiforvaltningen orienterer Økonomiudvalget (ØU) om status på informationssikkerhedsarbejdet og om informationssikkerhedsbrud i kommunen mindst én gang årligt, som det fremgår af forretningscirkulære for organisering af informationssikkerhed § 4, stk. 4.

I 2020 er der gennemført en række indsatser, der imødekommer truslerne mod kommunens generelle drifts- og datasikkerhed. Arbejdet med at sikre en høj informationssikkerhed tager bl.a. afsæt i konklusionerne fra de tilsynsaktiviteter og risikovurderinger, som Databeskyttelsesrådgiveren og Koncern IT gennemfører årligt.

Det er Økonomiforvaltningens vurdering, at de kendte sikkerhedsrisici mod kommunens it-systemer befinder sig på et acceptabelt niveau, samt at det nuværende beskyttelsesniveau af kommunens it-infrastruktur generelt ligger på et passende beskyttelsesniveau. Konklusionerne og vurderingerne forelægges til Økonomiudvalgets orientering.

Problemstilling
Indsatsen på informationssikkerhedsområdet planlægges ud fra en risikobaseret tilgang og er dermed en afvejning mellem de sikkerhedsmæssige risici og kommunens behov for effektivitet og høj borgerservice. Dette skal bl.a. sikre, at enhver håndtering af personoplysninger og værdioplysninger i Københavns Kommune sker på en betryggende og tillidsvækkende måde i forhold til kommunens borgere og virksomheder, og at kommunen følger de regler for behandling af personoplysninger, der er fastsat i reglerne om databeskyttelse. Se bilag 1 for Databeskyttelsesrådgiverens statusrapport.

I 2020 har der i Københavns Kommune været behov for en særlig indsats på informationssikkerhedsområdet grundet covid-19 situationen, hvor kommunens ansatte og borgere i højere grad end normalt, har kommunikeret via online platforme.

Løsning

Trusselvurdering

Koncern IT (KIT) udarbejder årligt en vurdering af truslerne mod kommunens informationssikkerhed. Trusselsvurderingen er udarbejdet med input fra flere eksterne parter bl.a. Center for Cybersikkerhed. Sammen med anerkendte standarder danner trusselsvurderingen udgangspunktet for kommunens arbejde med informationssikkerhed.

Koncern IT
Sikkerhed
Borups Allé 177
2400 København NV

EAN-nummer
5798009809308

Trusselsvurderingen i KK svarer til den, de fleste offentlige myndigheder oplever, hvor særligt to trusler vurderes høje:
1. Der ses en høj trussel fra cyberkriminelle, der gennem phishingforsøg forsøger at opnå økonomisk berigelse.
2. Risikoen for utilsigtede datalæk vurderes til at være høj.

Sikkerhedsmæssige tiltag som følge af Covid-19
Grundet covid19-krisen har Koncern IT iværksat en række tiltag for at imødekomme den nye arbejdssituation for kommunens medarbejdere. Initiativer på informationssikkerhedsområdet fordeler sig på tre områder:

- Monitorering og særlige netværk
- Sikkerhedsopdateringer
- Kommunikation.

Monitorering og særlige netværk
Koncern IT tilrettede i den helt tidlige fase af Corona-krisen KK's sikkerhedsmonitorering af netværket til den nye situation med hyppig brug af hjemmearbejde. Den primære tilpasning var her med fokus på det nye brugsscenarie, hvor mange flere af KK's medarbejdere begyndte at tilgå KK's it-infrastruktur hjemmefra. Tidligt i forløbet sikrede KK desuden, at der var den nødvendige kapacitet til VPN-forbindelser (sikker og krypteret adgang til KK's netværk).

Sikkerhedsopdateringer
Et helt afgørende sikkerhedsmæssigt tiltag ved hjemmearbejde er, at computere skal have de seneste sikkerhedsopdateringer. I forbindelse med Corona-krisen har Koncern IT dels sikret, at de normale sikkerhedsopdateringer gennemføres, når computere tilgår KK's it-infrastruktur via VPN, dels gennemført tiltag, der muliggør, at der kan hentes sikkerhedsopdateringer via det almindelige internet, fx fra medarbejdernes egne internetforbindelser.

Kommunikation
Endelig har Økonomiforvaltningen i et tæt samarbejde med Den Administrative Krisestab og kredsen af digitaliseringschefer i KK gennemført en række målrettede kommunikationstiltag.

Kommunikationen har både handlet om at gøre medarbejderne opmærksomme på nødvendigheden af, at deres computere skal være tændt og koblet på nettet med henblik på sikkerhedsopdateringer, og om en række anbefalinger om sikker anvendelse af hjemmearbejdspladser, bl.a. fra Center for Cybersikkerhed.

Informationssikkerhedshændelser
Når en medarbejder foretager en indmeldelse, undersøges omfanget, risiciene og konsekvenserne af det indmeldte forhold. Derefter vurderes

det, om der er tale om et persondatabrud, om der skal ske anmeldelse til Datatilsynet, eller om der snarere er tale om en bekymring fra en medarbejder.

Antallet af persondatabrud i KK der indmeldes til Datatilsynet er i 2020 på samme niveau som i 2019 og ligger dermed på et stabilt niveau.

Antallet af persondatabrud som medarbejdere i KK indmelder internt er stødt stigende, se bilag 2.

At der er sket en stigning i indmeldelser fra medarbejdere, kan være en indikation på, at der er øget opmærksomhed om datasikkerhed blandt kommunens medarbejdere. Udbredelse og gennemførelse af obligatoriske e-læringsmoduler vedr. it-sikkerhed og databeskyttelse er formentlig en væsentlig faktor. Men stigningen kan også skyldes initiativer i den enkelte forvaltning i form af awareness-kampagner, quizzer, vejledninger mv.

Når de flere indmeldte persondatabrud ikke resulterer i flere indmeldelser til Datatilsynet, kan det begrundes i, at Datatilsynet løbende offentliggør afgørelser, udarbejder vejledninger m.m., der understøtter de dataansvarlige i deres arbejde med at vurdere, hvornår der skal anmeldes. Dermed er forvaltningernes databeskyttelsesfunktioner blevet bedre rustet til at vurdere, hvornår et persondatabrud skal indmeldes til Datatilsynet.

Konklusioner fra informationssikkerhedstilsyn og risikovurdering 2020
Koncern IT fører årligt tilsyn med informationssikkerheden i forvaltningerne og gennemfører risikovurderinger af kommunens it-systemer. Se bilag 3. Det er vurderingen, at forvaltningerne rent systemteknisk lever op til væsentlige it-sikkerhedskrav. Fokus på forbedringer bør ske på de krav, der følger af Databeskyttelsesforordningen (GDPR).

Resultatet af informationssikkerhedstilsynet og risikovurderingerne giver forvaltningerne mulighed for at træffe beslutning om sikkerhedsniveauet inden for egen forvaltning, som det følger af forretningscirkulæret for organisering af informationssikkerhed.

Kommunens forvaltninger har på baggrund af risikovurderingerne udarbejdet handleplaner, der er godkendt af forvaltningernes direktioner. Kommunens kreds af it-ansvarlige direktører orienteres løbende i It-kredsen om status på implementeringen af disse. Forvaltningerne anbefales ligeledes på baggrund af informationssikkerhedstilsynet at udarbejde forvaltningsspecifikke handleplaner.

Centrale initiativer til sikring af informationssikkerheden 2020
Der gennemføres årligt en række større initiativer, der skal understøtte et tilfredsstillende informationssikkerhedsniveau i KK. Foruden tidligere nævnte initiativer, der er udført i forbindelse med covid-19, har KK udført følgende tværgående initiativer:

Tværgående aktivitetsplan for databeskyttelsesindsatser i KK
Hver af kommunens forvaltninger har etableret en

databeskyttelsesfunktion, der har til formål at rådgive om databeskyttelse internt i forvaltningen, udføre opgaver relateret til databeskyttelsesområdet og igangsætte løbende indsatser. For at styrke koordineringen af arbejdet og sikre en effektiv databeskyttelsesindsats i KK, er der i 2020 udarbejdet en fællesadministrativ forretningsgang, der har til formål at sikre og rammesætte tværgående koordinering mellem forvaltningernes interne databeskyttelsesfunktioner.

Opdatering af KK's regler for informationssikkerhed
Kommunens regler for informationssikkerhed er i 2020 blevet evalueret efter implementeringen mhp. at foretage konsekvensrettelser og opdatere andre uhensigtsmæssigheder. Evalueringen, som førte til en opdatering af reglerne for informationssikkerhed, har ført til en større synergi mellem forretningscirkulærerne under Informationssikkerhedsregulativet og har tilføjet en række afsnit, som skaber klarere rammer for forvaltningernes daglige arbejde med informationssikkerhed og databeskyttelse.

Implementering af logopfølgningssystem (SIEM) i KK
Logopfølgningssystemet i KK har til formål at øge informationssikkerheden for håndtering af data og anvendelse af fagsystemer. Systemet udsender notifikationer til forvaltningerne ved mistænkelig brugeradfærd i udvalgte fagsystemer. Logopfølgningen er ét af flere centrale elementer i at beskytte borgernes persondata mod uautoriseret adgang, herunder f.eks. ved uretmæssige opslag på CPR-numre i udvalgte fagsystemer. Logopfølgningssystemet SIEM er i løbet af 2020 fuldt implementeret, og alle revisionsbemærkninger fra den lovpligtige eksterne revision er i den forbindelse håndteret. KK' s SIEM-system bidrager også til KK's generelle it- og cybersikkerhed via logning af komponenter i it-infrastrukturen.

Phishingspillet fra Hoxhunt
For at imødekomme den stigende cybertrussel i KK indførte Økonomiforvaltningen i 2020 et phishingspil fra firmaet Hoxhunt. Spillet baserer sig på en gamificeret tilgang til awareness, hvor brugerne modtager simulerede phishingforsøg i deres Outlook, som de skal forsøge at opdage. Efter aftale med flere MED-udvalg i KK er den enkelte brugers resultater anonyme. Spillet er bredt ud til administrative medarbejdere i hele kommunen.

Bilag
Bilag 1 – Statusrapport fra Databeskyttelsesrådgiveren for perioden 1. oktober 2019 til 1. oktober 2020

Bilag 2 – It-sikkerhedshændelser og persondatabrud 2020

Bilag 3 – Uddybende konklusioner fra tilsyn med informationssikkerheden og risikovurderinger 2020.

Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 1: Statusrapport fra Databeskyttelsesrådgiveren for perioden 1. oktober 2019 til 1. oktober 2020

17. februar 2021

Sagsnummer
2021-0051372

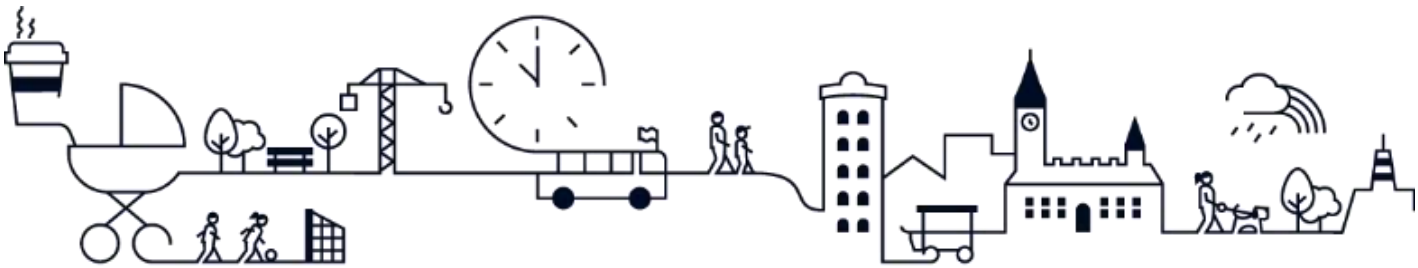
Dokumentnummer
2021-0051372-5

I bilaget er Statusrapporten fra Databeskyttelsesrådgiveren for perioden 1. oktober 2019 til 1. oktober 2020 vedlagt.

Koncern IT
Sikkerhed
Borups Allé 177
2400 København NV

EAN-nummer
5798009809308

INTERN REVISION



STATUSRAPPORT FRA DATABESKYTTELSESRÅDGIVEREN

For perioden 1.oktober 2019 til 1.oktober 2020

MODTAGER

Borgerrepræsentationen
Økonomiudvalget
Revisionsudvalget
Forvaltningerne

Indhold

1. Indledning

I overensstemmelse med Københavns Kommunes Informationssikkerhedsregulativ og Forretningscirkulære for persondatabeskyttelse, dokumentation og compliance, udarbejder Databeskyttelsesrådgiveren årligt pr. 1. oktober en statusrapport. Rapporten indeholder en vurdering af databeskyttelsen samt øvrige forhold i relation til databeskyttelse i Københavns Kommune.

Rapporten fremsendes til forvaltningernes direktioner, til Revisionsudvalget og til Borgerrepræsentationen efter forudgående indhentet erklæring fra Økonomiudvalget.

I § 12-erklæringen vedr. statusrapporten 2019 angav ØKF bl.a.:

"Økonomiudvalget bemærker, at der alene foreligger en statusrapport, som omfatter kommunen som helhed. Økonomiudvalget har noteret sig, at Databeskyttelsesrådgiveren i indledningen, side 2, har beskrevet, at baggrunden herfor er, at risikovurderingerne stort set er identiske for de enkelte forvaltninger i 2019. Økonomiudvalget forventer, at der i takt med opbygning af erfaringer på området fremadrettet vil foreligge risikovurderinger pr. forvaltning og for kommunen som helhed, som det fremgår af funktionsbeskrivelsen."

Der foreligger på nuværende tidspunkt ikke en risikovurdering for de enkelte forvaltninger. Derfor er der i lighed med 2019 kun udarbejdet en rapport for kommunen som helhed, der omhandler arbejdet med databeskyttelse i perioden 1.oktober 2019 til 1. oktober 2020. Der henvises til rapportens pkt. 2.2. Risikovurderingskoncept, for yderligere oplysninger om arbejdet med risikovurderinger.

2. Status

2.1. Den overordnede status for databeskyttelse i Københavns Kommune

Samlet set er det Databeskyttelsesrådgiverens vurdering:

- at Københavns Kommune på nuværende tidspunkt har en klar og tydelig rolle- og ansvarsfordeling samt passende regler og retningslinjer, der medvirker til at sikre en betryggende databeskyttelse i Københavns Kommune.

- at de databeskyttelsesretlige regler administreres på et fornuftigt grundlag i Københavns Kommune. Databeskyttelsesrådgiveren er ikke bekendt med områder, hvor der ikke er fokus på databeskyttelse.

- at alle ledelseslag i Københavns Kommune arbejder bevidst med og respekterer de databeskyttelsesretlige regler.

- at der er den nødvendige opbakning og forståelse for Databeskyttelsesrådgiver-funktionens rolle og ansvar.

I statusrapporten for 2019 pegede Databeskyttelsesrådgiveren på nogle konkrete forhold, der burde forbedres for at sikre den nødvendige fremdrift i databeskyttelsen i Københavns Kommune.

De konkrete forhold der blev peget på, var:

- koordinering af den samlede indsats på databeskyttelsesområdet
- overblik over udmøntningen/operationalisering af ansvarsområder
- overblik over de ressourcer, der anvendes samlet i Kommunen på databeskyttelse

Efter drøftelse og godkendelse i IT-kredsen tog Databeskyttelsesrådgiveren i januar 2020 initiativ til at opstarte en række arbejdsgrupper, som skulle håndtere Databeskyttelsesrådgiverens observationer og anbefalinger. Forvaltningerne var repræsenteret i arbejdsgrupperne via DPO Business Partnerne og Vejledende Sikkerhed i Koncern IT.

Følgende værktøjer/materialer skulle udarbejdes:

- Uddybende funktionsbeskrivelser for DPO Business Partner, Vejledende Sikkerhed og Databeskyttelsesrådgiveren (Værktøj 1), som består af:
    - Bilag 1 – Uddybende funktionsbeskrivelse Databeskyttelsesrådgiver
    - Bilag 2 – Uddybende funktionsbeskrivelse – Vejledende Sikkerhed
    - Bilag 3 – Uddybende funktionsbeskrivelse DPO Business Partner
    - Bilag 4 - Snitflade-og opgavebeskrivelsesoverblik

- Værktøj 2 – Årshjul og aktivitetsplaner, som består af:
    - Bilag 5 - Skabelon for Aktivitetsplan
    - Bilag 6 - Procesbeskrivelse Årshjul og aktivitetsplaner

- Værktøj 3 – Tilsyn, som består af:
  - Bilag 8 - Procesbeskrivelse for tilsyn
  - Bilag 9 – Tilsynsorienteringsskabelon
  - Bilag 10 – Skabelon for tilsynsrapport

- Værktøj 4 – Journalisering og dokumentation, som består af:
  - Bilag 7 – Procesbeskrivelse for journalisering og dokumentation (DPO BP)

Arbejdet for fire af arbejdsgrupperne blev afsluttet maj måned 2020. Grundet Covid-19 blev arbejdet afsluttet senere end forventet.

Den 23. oktober 2020 godkendte IT-kredsen:

- Uddybende funktionsbeskrivelse for forvaltningens DPO Business Partner (værktøj 1)
- Fællesadministrativ forretningsgang for årshjul og aktivitetsplan på databeskyttelsesområdet (værktøj 2). Forud for dette forslag blev graden af fælles aktivitet- og tidsstyring drøftet mellem Databeskyttelsesrådgiveren og forvaltningernes DPO Business Partnere. Der var tilslutning til tæt koordination på aktivitetsområdet med et fælles årshjul og dertilhørende aktivitetsplaner.

Arbejdet med værktøj 3 om tilsyn viste, at snitfladen mellem DPO'en og forvaltningerne på enkelte områder kunne tolkes forskelligt, herunder særligt på it-tilsynsområdet. På den baggrund aftaltes det den 11. september 2020 mellem IT-kredsen og Databeskyttelsesrådgiveren, at der sker en præcisering således, at det formaliserede tilsyn med overholdelsen af de databeskyttelsesretlige regler på tværs af alle forvaltninger, foretages af Databeskyttelsesrådgiveren. Forvaltningerne foretager almindeligt ledelsestilsyn som led i forvaltningens arbejde med databeskyttelse. IT-kredsen godkender samtidig, at der i forbindelse med opgaveflyttet permanent tilføres to årsværk til Databeskyttelsesrådgiveren.

- Under drøftelserne vedrørende værktøj 4 – Journalisering og dokumentation (DPO BP) var det forvaltningernes vurdering, at de eksisterende vejledninger og retningslinjer for journalisering i Københavns Kommune dækker databeskyttelsesområdet, og at værktøj 4 derfor ikke vurderes relevant at implementere.

Databeskyttelsesrådgiveren tager til efterretning, at der ikke kunne opnås tilslutning til forslaget om at skabe et overblik over de samlede ressourcer, der er til rådighed og anvendes til databeskyttelse, ligesom der ikke var opbakning til en særlig journalisering og dokumentation af DPO Business Partnernes arbejde.

Herudover er der taget initiativ til, at Økonomiforvaltningen i samarbejde med DPO Business Partner Forum og digitaliseringscheferne udarbejder et kommissorium for DPO Business Partner Forum. Business Partner Forum får fremover til opgave, i tæt samarbejde med Databeskyttelsesrådgiveren, at varetage koordineringen af databeskyttelsesindsatser i kommunen, herunder koordinering af forvaltningernes aktivitetsplaner og årshjul samt prioritering, tilrettelæggelse og udførelse af tværgående complianceindsatser.

Endelig er det besluttet, at DPO Business Partnere fremover betegnes med en mere sigende titel. Databeskyttelsesrådgiveren og forvaltningerne har oplevet forveksling mellem Databeskyttelsesrådgiveren og forvaltningernes DPO Business Partnere. Dette sammenholdt med de ændringer om roller og ansvar, der seneste er aftalt, gør, at det er besluttet, at titlen fremover er GDPR Business Partner.
Databeskyttelsesrådgiverens ser frem til, at der for 2021 foretages en koordinering af den samlede operationelle indsats i Københavns Kommune på databeskyttelsesområdet.

2.2. Risikovurderingskoncept

Af Databeskyttelseslovgivningen fremgår det, at den dataansvarlige (Københavns Kommune) skal udvise ansvarlighed i enhver henseende i forhold til de registreredes (borgere, medarbejder mv.) personoplysninger. Det er desuden et krav, at de foranstaltninger, der skal sikre denne ansvarlighed, er baseret på en risikovurdering. En risikovurdering skal identificere risikoen for de registreredes rettigheder og frihedsrettigheder ved enhver behandling af personoplysninger.

Databeskyttelsesrådgiveren vurderede i 2019, at kommunens største risiko er, at der ikke i tilstrækkelig grad arbejdes risikobaseret. I samarbejde med Koncern IT har Databeskyttelsesrådgiveren igangsat et projekt, der skal medvirke til at skabe overblik, forståelse og effektivitet i kommunens risikovurderingsproces:

1. OVERBLIK

En fælles tilgang til risikostyring på tværs af enheder i kommunen.

2. FORSTÅELSE

Indsigt i samspillet mellem risici for forretning, it og privatlivet.

3. EFFEKTIVITET

En nemmere proces til identificering og kvalificering af risici.

Projektet gennemføres med ekstern bistand, og de relevante enheder i kommunen, som arbejder med risikovurderinger, inddrages i arbejdet med optimering og samordning af de nuværende modeller. Risikovurderingskonceptet udarbejdes i overensstemmelse med ISO-standarderne.

Grundet Covid-19 forventes arbejdet at blive afsluttet i slutningen af Q1 2021 og implementeret i løbet af 2021.

Databeskyttelsesrådgiveren ser frem til, at der fremadrettet implementeres en ensartet og standardiseret risikovurdering på hele informationssikkerhedsområdet på tværs af alle enheder, således at indsatsen (foranstaltningerne) bliver mere effektiv i forhold til at reducere de identificerede risici.

2.3. Henvendelser til Databeskyttelsesrådgiveren

Databeskyttelsesrådgiveren ønsker at blive opfattet som en ressource frem for en autoritet, selv om opgaverne også omfatter overvågning og tilsyn samt rapportering heraf til BR, ØU og forvaltningernes ledelse. Det er den umiddelbare vurdering, at forvaltningerne er gode til at kontakte Databeskyttelsesrådgiveren, når der er behov for det.

Siden 1. oktober 2019 har Databeskyttelsesrådgiveren ført statistik over, hvor mange henvendelser der har været fra de enkelte forvaltninger. Henvendelserne giver Databeskyttelsesrådgiveren et indblik i, hvordan de databeskyttelsesretlige regler forvaltes. En henvendelse bliver registreret, når Databeskyttelsesrådgiveren kontaktes for rådgivning og vejledning.

Nedenstående tabel viser henvendelser fra den 1.oktober 2019 til 1.oktober 2020.

Forvaltning	**Antal henvendelser**
Beskæftigelses-og Integrationsforvaltningen	16
Børne-og Ungdomsforvaltningen	28
Kultur-og Fritidsforvaltningen	25
Socialforvaltningen	39
Sundheds-og Omsorgsforvaltningen	19
Teknik-og Miljøforvaltningen	19
Økonomiforvaltningen	32

Databeskyttelsesrådgiveren opfordrer til, at forvaltningerne ikke er tilbageholdende med at kontakte Databeskyttelsesrådgiver-funktionen, da det er med til at skabe opmærksomhed på tværgående problemstillinger og indblik i forvaltningsspecifikke udfordringer m.v.

3. Afgørelser fra Datatilsynet

Fremadrettet vil Databeskyttelsesrådgiveren i statusrapporterne orientere om væsentlige afgørelser og henvendelser fra Datatilsynet. Der henvises endvidere til afsnit 4.2 vedrørende sager om persondatabrud.

3.1. Anvendelse af SharePoint

Den 15. oktober 2019 udtalte Datatilsynet **alvorlig kritik** af Københavns Kommune for den behandling, som havde fundet sted i SharePoint. Datatilsynet undersøgte en specifik behandling, og det var derfor ikke udtryk for en generel undersøgelse af al behandling i SharePoint.

I den specifikke sag var behandlingen ikke sket i overensstemmelse med databeskyttelsesforordningens artikel 32. Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger for at sikkerhedsniveauet passer til de identificerede risici. Til dette udtalte Datatilsynet, at Københavns Kommune ikke i tilstrækkeligt omfang havde iagttaget denne bestemmelse.

Datatilsynet lagde bl.a. vægt på, at flere medarbejdere, end hvad der måtte anses for værende nødvendigt, havde haft adgang til de filer sagen vedrørte. Københavns Kommune havde desuden en omfattende mængde filer i SharePoint, herunder filer med oplysninger af fortrolig og følsom karakter. Datatilsynet lagde vægt på, at den etablerede logning og de oplyste interne retningslinjer om, at følsomme og fortrolige oplysninger ikke må opbevares i endelig dokumentform på fælles drev i mere end 30 dage, ikke i sig selv udgør tilstrækkelig grad af sikkerhed, og derfor ikke kunne anses for en passende sikkerhedsforanstaltning.

Det var derfor Datatilsynets opfattelse, at personoplysninger, der behandles i SharePoint, hurtigst muligt – efter en risikovurdering – skulle overføres til København Kommunes sagsbehandlingssystem.

Københavns Kommune har efterfølgende igangsat et omfattende oprydningsarbejde i SharePoint og etableret en governance struktur, der skal skabe grundlag for den løbende vedligeholdelse af SharePoint.

3.2. CPR-abonnementer

Datatilsynet har den 25. oktober 2019 udtalt **kritik** af Københavns Kommune i forbindelse med at kommunen har abonneret på CPR-oplysninger om en borger, som ikke har haft bopæl i Københavns Kommune siden 1999.
På baggrund af borgerens første henvendelse konkluderede Københavns Kommune, at man ikke havde behov for at behandle borgerens CPR-nummer og abonnementet hos Det Central Personregister, der derfor blev opsagt.

Efterfølgende viste det sig, at abonnementet på oplysninger om klager i CPR automatisk var blevet gentegnet, fordi der i kommunens journaliseringssystem var registreret en aktuel sag vedrørende klager, som var blevet oprettet på baggrund af klagers henvendelse af 17. januar 2018 om kommunens abonnering af oplysninger om ham.

Københavns Kommune angav som begrundelse for at genoptage CPR-abonnementet, at det var nødvendigt at oprette et CPR-abonnement med henblik på entydig identifikation og som journalnummer, så kommunen havde retvisende og aktuelle identifikationsoplysninger om borgeren. Identifikationsoplysningerne skulle anvendes til at kunne håndtere eventuelle aktindsigts- eller rettighedsanmodninger, eller andre retskrav, efter bl.a. offentlighedsloven, forvaltningsloven og databeskyttelsesreglerne.

Datatilsynet udtalte på den baggrund, at behandling af oplysninger med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, skal være *nødvendig*. Efter Datatilsynets opfattelse anses det ikke for nødvendigt, at oprette automatiske personabonnementer i CPR med det formål, at kunne håndtere eventuelle aktindsigts- eller rettighedsanmodninger, idet man i kommunen har mulighed for at lave enkeltopslag i CPR, når der viser sig et aktuelt behov for at ajourfører personoplysninger.

Udtalelsen konkluderer, at CPR-abonnementer kun må oprettes, hvis der er et sagligt behov herfor. Ligesom aktive abonnementer løbende skal slettes, når der ikke længere er et sagligt behov for at modtage oplysninger fra Det Central Personregister.

På baggrund af udtalelsen blev det besluttet, at

- CPR-abonnementer på borgere i KK slettes snarest (17.099 abonnementer)
- CPR-abonnementer på udenbys borgere slettes ultimo januar 2020, efter opgraderingen af kommunens ESDH-system (230.730 abonnementer)

3.3. Mangel på oplysningspligt

Datatilsynet har den 4.september 2020 udtalt **kritik** af Københavns Kommunes Børne-og Ungdomsforvaltning fordi oplysningspligten, ikke var iagttaget i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 13, jf. artikel 12, stk. 1.

Opfyldelse af oplysningspligten er en vigtig grundrettighedsbeskyttelse i databeskyttelsesforordningen, da den sikrer gennemsigtighed overfor borgerne.

Datatilsynet udtaler:

"Efter databeskyttelsesforordningens artikel 13, stk. 1, skal den dataansvarlige, på det tidspunkt hvor oplysningerne indsamles, give den registrerede alle de oplysninger der fremgår af artikel 13, stk. 1 og 2. Oplysningerne skal gives i den form og på den måde der fremgår i artikel 12, stk. 1.

I overensstemmelse med det af Københavns Kommune Børne- og Ungeforvaltningen erkendte, lægges det til grund, at de påkrævede oplysninger, ikke er givet til klager på tidspunktet hvor oplysningerne blev indhentet."

Det er ikke Databeskyttelsesrådgiverens umiddelbare oplevelse, at forvaltningerne ikke generelt efterlever oplysningspligten overfor borgerne. Databeskyttelsesrådgiveren vil på baggrund af udtalelsen og et observeret eksempel foretage tilsyn med forvaltningernes efterlevelse af oplysningspligten i 2021.

3.4. Tilsyn med Robotic Proces Automation (RPA) og Kunstig Intelligens (AI)

Datatilsynet varslede den 17. januar 2020 Københavns Kommune et tilsynsbesøg. Emnet var Robotic Proces Automation (RPA) og Kunstig Intelligens (AI). Forud for mødet skulle kommunen udarbejde en liste med:

- Alle systemer der benytter RPA teknologi, fordelt på forvaltningsområder
- På de identificerede systemer, skal der i punktform, fremgå en beskrivelse af hvilke oplysninger der behandles, behandlingshjemmel samt i hvilket omfang den brugte automatisering danner grundlag for nye registreringer i sagsbehandlings- eller andre fagsystemer
- Alle systemer der – i ordets bredeste forstand – benytter AI. Dette omfatter også systemer der måtte benyttes til ledelsesinformation og systemer der benytter data på aggregeret niveau, uanset om data af kommunen selv anses for anonymiseret.
- På de identificerede systemer, skal der i punktform, fremgå en beskrivelse af hvilke oplysninger der behandles, behandlingshjemmel samt i hvilket omfang den brugte logik og resultaterne heraf, danner grundlag for nye afgørelser og/eller registreringer i sagsbehandlings- eller andre fagsystemer

Koordineringen i forbindelse med tilsynet blev varetaget af ØKF/KIT og Databeskyttelsesrådgiveren.

Tilsynsbesøget blev afholdt den 24. februar 2020.
Under mødet var repræsentanter fra de forvaltninger, som ejede systemerne BUF, BIF og SOF, og KIT.

Københavns Kommune er forsat i proces med Datatilsynet. Det forventes, at der kan gå op til et år, før tilsynet er afsluttet. Det er på nuværende tidspunkt ikke muligt at vurdere, hvilket udfald tilsynet vil få for Københavns Kommune.

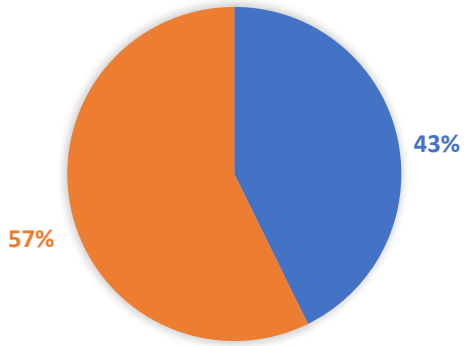
4. Persondatabrud

Det er Databeskyttelsesrådgiverens opfattelse, at forvaltningerne har en god proces for håndteringen og koordineringen af persondatabrud, samt at medarbejderne har en god forståelse af, hvad et persondatabrud er samt evnen til at identificere hændelser. Databeskyttelsesrådgiveren vil foretage tilsyn på området i 2021.

Databeskyttelsesrådgiveren oplever forsat, at antallet af brud på tværs af kommunens forvaltninger varierer en del.

I perioden 1. juli 2019 til den 1. oktober 2020 er der blevet registeret 593 persondatabrud i Københavns Kommune.

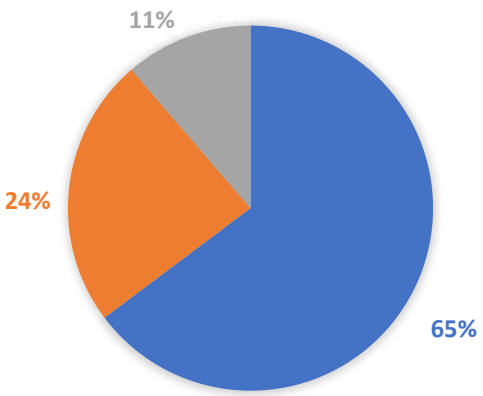
Figur 1. Sager der har været anmeldt til Datatilsynet i det tilfælde sagen har haft karakter af et persondatabrud:



Viser antal sager (272), hvor forvaltningen har vurderet, at der ikke har været behov for at anmelde sagen til Datatilsynet.

Viser antal sager (203), hvor forvaltningen har vurderet, at sagen skal anmeldes til Datatilsynet.

Figur 2. Fordeling af, hvorvidt sagerne har haft karakter af persondatabrud eller ej, samt ikke afsluttede sager:



Viser antal sager (67), som endnu ikke er afsluttet.

Viser antal sager (384), hvor forvaltningerne har vurderet, at der var tale om et persondatabrud.

Viser antal sager (142), hvor forvaltningerne har lukket sagen, fordi det er blevet vurderet, at der ikke var tale om et persondatabrud.

De hyppigste årsager til persondatabrudende er forsat hændelser, som resulterer i utilsigtet videregivelse på grund af menneskelige fejl.

Databeskyttelsesrådgiveren foretager tilsyn med forvaltningernes indsats rettet mod at undgå gentagelse af persondatabrud i 2021, samt den konkrete håndtering.

4.1. Alvorlig kritik - Sagerne gengivet i kort resumé

Hvad Databeskyttelsesrådgiveren har kendskab til, har Københavns Kommune i alt modtaget 97 afsluttende breve fra Datatilsynet for indberettede persondatabrud siden 1. juli 2019 til 1. oktober 2020.

I 94 af sagerne har der ikke været anledning til udtalelse fra Datatilsynet. I 2 sager har Københavns Kommune modtaget alvorlig kritik, samt 1 udtalelse med kritik.

Den første sag vedrører implementeringen af et system i Københavns Kommune. I den forbindelse foretog man nogle test af produktionsmiljøet, hvor man benyttede oplysninger fra en række testpersoner, som havde underskrevet en samtykkeerklæring på, at deres personoplysninger måtte bruges til test. Alle var ansatte i Københavns Kommune og der var tale om ca. 14 medarbejdere. Da man overgik til drift, havde man ikke fået slettet alle testoplysningerne, hvilket fik retsvirkende konsekvenser for medarbejderen, som i øvrigt ikke havde givet samtykke til at vedkommendes oplysninger blev brugt til test.

Den anden sag vedrørte manglende kontrol med brugerautorisationer i forbindelse med skiftende opgavevaretagelse og stillingsbetegnelse. Dette bevirkede, at medarbejderen havde autorisationer til at foretage ændringer i systemet, som denne ikke burde have været tillagt. Der var tale om medicinsk behandling, hvilket kræver særlig opmærksomhed ift. håndteringen og kommunens kontrolforanstaltninger.

I begge henseender lagde Datatilsynet vægt på, at Københavns Kommune ikke havde truffet de nødvendige tekniske og organisatoriske foranstaltninger, hvilket understreger behovet for brugen af risikovurderinger fremadrettet til at kunne dokumentere tiltag m.v.

Forvaltningerne har udarbejdet handleplaner for at sikre, at lignende tilfælde ikke gentages. Databeskyttelsesrådgiveren foretager en opfølgning på forvaltningens handleplaner i 2021.

5. Databeskyttelsesrådgiverens afsluttede opgaver

5.1. KK "Benspændskatalog"

I januar 2020 meldte Kommunernes Landsforening (KL) ud at: "GDPR spænder ben for velfærden. Hver eneste dag slås landets kommuner nærmest helt bogstaveligt med implementeringen af den nye databeskyttelsesforordning, i daglig tale blot kaldet GDPR".

KL havde i den forbindelse samlet et udsnit af eksempler på, hvordan GDPR efter kommunernes opfattelse spænder ben for kommunernes arbejde. Med det nye benspændskatalog i hånden ville KL tage sagen op med regeringen og EU.

Datatilsynet offentliggjorde kort efter en publikation, hvor Datatilsynet gennemgik og besvarede KL's eksempler. En stor del af de eksempler, som KL havde anført i "benspændskataloget", er ikke benspænd, men mere basale borgerrettigheder, ifølge Datatilsynet.

Datatilsynet anførte i den forbindelse, at det gælder generelt for reglerne i GDPR, at de er fleksible og kan tilpasses de mange forskellige situationer, hvor man behandler personoplysninger. Datatilsynet tilføjede, at det til gengæld også betyder, at reglerne ikke tager stilling til konkrete scenarier og teknologier, og at man som dataansvarlig selv skal foretage en vurdering af, hvad der er nødvendigt og rimeligt over for borgerne. Datatilsynet anerkendte i den forbindelse, at det kan være svært for den enkelte medarbejder på et plejehjem, i en børnehave e.l. at skulle forholde sig til juraen. Datatilsynet foreslog derfor, at man lader kommunens jurister sætte rammerne for arbejdet.
I kølvandet på KL's "benspændskatalog" og de eksempler vi har set i forbindelse med KL's erfaringsindsamling, har Databeskyttelsesrådgiveren igangsat et arbejde med at opspore eventuelle "benspænd" fra databeskyttelseslovgivningen i Københavns Kommune, ved at opfordre alle kommunens ansatte til at fremsende de udfordringer i forhold til databeskyttelse, de oplever i hverdagen.

Dette vil der blive arbejdet på i Q4 2020. Resultatet bliver et katalog, der håndterer hverdagsproblemstillinger, som f.eks. kan være, om der må hænge billeder af børn i en institution og lignende.

5.2. Tilsyn med Uddannelsesplaner

Databeskyttelsesrådgiveren afsluttede i september måned 2019 sit tilsyn med forvaltningernes uddannelsesplaner. Tilsynet omfattede en gennemgang af, hvorvidt forvaltningerne havde lavet et design der sikrer, at de ansatte modtager en relevant uddannelse i håndteringen af personoplysninger, hvorvidt dette design har været implementeret tilstrækkeligt (kendt af de ansatte og ledelserne), samt hvorvidt design og proces fungerer effektivt, altså om det tilsigtede resultat opnås.

Tilsynet blev gennemført for alle syv forvaltninger.

De vigtigste observationer viste bl.a., at:

- retningslinjerne var designet i tilstrækkelig grad i flere af forvaltningerne, dog måtte enkelte forvaltninger genbesøge uddannelsesplanen
- implementeringen af retningslinjerne var mangelfuld i flere forvaltninger

- der i flere forvaltninger var et større antal ansatte, der ikke havde modtaget undervisning i håndtering af persondatabrud
- der generelt set manglende den ledelsesmæssige opfølgning på, om de ansatte havde gennemført uddannelsen eller ej
- data i uddannelsessystemet ikke blev holdt tilstrækkeligt vedlige ift. hvorvidt medarbejderne var ansat i forvaltningerne

Databeskyttelsesrådgiveren igangsætter en opfølgning for sidste års tilsynsrapport Q4 2020. Dette sker i forbindelse med, at det er 2 år siden størstedelen af Københavns Kommune sidst modtog undervisning, og at frekvensen for uddannelse netop er fastsat til 2 år.

6. National evaluering af databeskyttelsesreglerne

Databeskyttelsesforordningen og den supplerende databeskyttelseslov har været gældende siden den 25. maj 2018. Som led i en national evaluering af databeskyttelsesreglerne vil Justitsministeriet undersøge mulighederne for at begrænse anvendelsen af databeskyttelsesforordningen og forenkle reglerne i databeskyttelsesloven på særligt udvalgte områder.

Ifølge Justitsministeriets udkast til en procesplan for en national evaluering af databeskyttelsesreglerne vil ministeriet afdække mulighederne for at lempe disse. Den nationale evaluering skal udarbejdes med afsæt i dels en erfaringsindsamling fra relevante interessenter, dels en række juridiske undersøgelser, som foretages af Justitsministeriet selv.

Erfaringsindsamlingen vil ske ved en bred høring af relevante interessenter herunder kommuner. Formålet med høringen er blandt andet at få belyst de konkrete situationer, der er uklare og giver anledning til tvivl, når databeskyttelsesreglerne skal efterleves i praksis.

Formålet med de juridiske undersøgelser, der skal foretages af Justitsministeriet selv, er blandt andet at belyse mulighederne for henholdsvis:

- at begrænse databeskyttelsesforordningens anvendelse på "mindre aktører, herunder frivillige foreninger"
- at indføre en påbudsordning, hvorefter Datatilsynet i videre omfang skal meddele påbud, før Datatilsynet anmelder den dataansvarlige virksomhed, forening, myndighed mv. til politiet med indstilling om bøde, eller før der udstedes et administrativt bødeforelæg
- at indføre en ordning, hvorefter tilsynsmyndigheden på anmodning kan afgive udtalelse om sin vurdering af lovligheden af en påtænkt aktivitet, der indebærer en behandling af personoplysninger
- at forenkle reglerne i databeskyttelsesloven.

Evalueringen forventes færdiggjort primo 2021.

Databeskyttelsesrådgiveren vil i 2021 have fokus på eventuelle ændringer, som påvirker Københavns Kommunes indsats på databeskyttelsesområdet.

7. Selvejende institutioner med driftsoverenskomst

I Københavns Kommune er det besluttet, at kommunens Databeskyttelsesrådgiver også kan fungere som Databeskyttelsesrådgiver for de selvejende institutioner med driftsoverenskomst. Denne funktion DPOSI fungerer p.t. som databeskyttelsesrådgiver for 153 selvejende institutioner fordelt på 220 lokationer.

I første kvartal af 2020 er Legal Complianceprojektet for de selvejende institutioner afsluttet. Projektet er gennemført på 12 måneder, der er anvendt 9.714 timer. Både timer og varighed er under budget. I projektet er der afholdt 418 møder med institutionerne og gennemgået mere end 300 dokumenter i form af databehandleraftaler, samtykker mv. Hver af de 160 institutioner har modtaget en afsluttende compliancerapport, som har givet institutionen indsigt i deres complianceniveau og et springbræt til forbedringer.

DPOSI har gennem året fokuseret på at understøtte institutionerne i den reelle implementering af GDPR. Dette er sket gennem en "en-til-en" rådgivning på væsentlige områder og en gennemgang af dokumenter, der er et krav for institutionerne anvende, samt en uddannelsesdag for 100 institutioner. Målet har været at gøre institutionerne klar til at overgå til drift og at etablere en solid governance med afsæt i DPOSI's anbefalinger og værktøjer. DPOSI har modtaget 1-2 henvendelser om dagen med spørgsmål, hvoraf der har været 46 større rådgivningssager.

Det har været væsentligt for DPOSI at skabe et omdømme som tilgængelig og effektiv rådgiver. Derfor har DPOSI lagt vægt på at besvare alle henvendelser hurtig, og at sikre praktiske og forståelige anbefalinger. Det har desuden været væsentligt at få opbygget et tillidsfuldt samarbejde, hvor institutionerne er komfortable med at søge hjælp og har en positiv indstilling til tilsynsaktiviteter i det kommende år.

Sideløbende med de kunderettede aktiviteter har DPO brugt året til at færdigudvikle en samlet proces, et framework og værktøjer for DPO-funktionens arbejde. Dette er baseret på de erfaringer, der er indsamlet i Legal Complianceprojektet og med ISO-standarder som grundlag.

København, den 30. november 2020

Københavns Kommune Databeskyttelsesrådgiverfunktion

Jesper Gjøtterup Andersen

Databeskyttelsesrådgiver for Københavns Kommune

Nicholai Mandrup	Line Nymann Schoop	Christian Sonn Kjelmann
Lone Forsberg	Jonathan Brix	Io Alexandra Sarroe-Brinkløv

Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 2: It-sikkerhedshændelser og persondatabrud 2020

16. februar 2021

Sagsnummer
2021-0051372

Dokumentnummer
2021-0051372-3

I bilaget præsenteres opgørelserne over kommunens informationssikkerhedshændelser opdelt i:

- Persondatabrud
- It-sikkerhedshændelser

Informationssikkerhedshændelser
En medarbejder, der trykker på et link i en falsk mail, ulåste døre på områder med følsomme personoplysninger, fejl i it-systemer, en medarbejder, der sender mail til en forkert person mv., er alle eksempler på typer af hændelser, der øger sandsynligheden for, at kommunens og borgernes data kommer i de forkerte hænder. Nogle gange er hændelserne af en sådan karakter, at det er sandsynligt, at det indebærer en risiko for fysiske personers rettigheder. I de tilfælde er kommunen forpligtet til at indberette bruddene til Datatilsynet.

En hændelse, der medfører indberetning til Datatilsynet, kategoriseres altid som et *persondatabrud*. Er der tale om en hændelse, hvor der ikke er risiko for brud på persondatasikkerheden, kategoriseres og behandles den i kommunen som en *it-sikkerhedshændelse*.

Persondatabrud i 2018, 2019 og 2020
Et persondatabrud er kendetegnet ved, at det fører eller kan føre til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

I KK registreres anmeldelser af persondatabrud via selvbetjeningsløsningen i et centralt system. Opgørelserne nedenfor baserer sig på data fra systemet indberettet i perioden fra den 25. maj 2018 til 31. december 2020. Medarbejderne i KK uddannes løbende til at indmelde hændelser, hvis de har mistanke om et brud på persondatasikkerheden. Antallet af persondatabrud anmeldt til Datatilsynet fremgår af Tabel 1 nedenfor. Antallet i tabellens parentes udgør antallet af indmeldte brud internt i KK.

Tabel 1: Antal af brud på persondatasikkerheden i 2018, 2019 og 2020

	2018 (25. maj – 31. december)	2019	2020
Anmeldte brud til Datatilsynet	61 (128)	179 (283)	179 (391)

Koncern IT
Sikkerhed
Borups Allé 177
2400 København NV

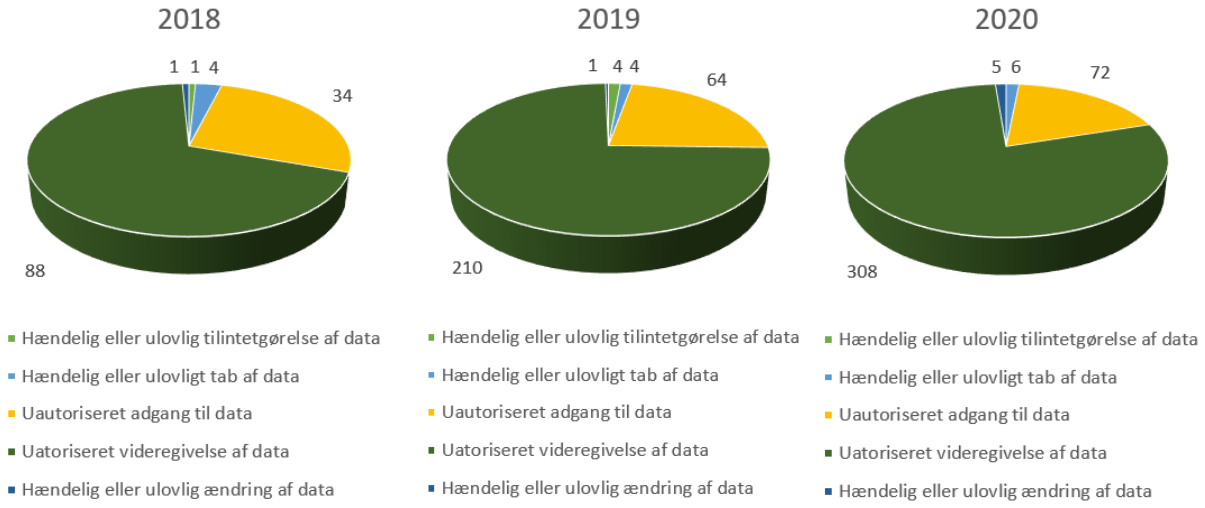
EAN-nummer
5798009809308

Typer af persondatabrud

Alle brud registreres efter type jf. figur 1 nedenfor. Typerne dækker over en uhensigtsmæssig omgang med data, der har medført:

- Tilintetgørelse – f.eks. at data slettes i et it-system
- Tab – f.eks. at data mistes ved tyveri
- Videregivelse – f.eks. at data sendes til forkerte personer uden-for kommunen
- Ændring – f.eks. at data redigeres fejlagtigt i en sagsakt
- Adgang – f.eks. at data er blevet set af en uvedkommende sags-behandler.

Figur 1: Persondatabrud fordelt på typer



Persondatabrud i de enkelte forvaltninger

Når persondatabrud indmeldes som en sag, vil én forvaltning/enhed være ansvarlig for sagen, men et brud vil kunne vedrøre data og områ-der, der går på tværs af forvaltningerne jf. tabel 2:

Tabel 2: Persondatabrud registreret i de enkelte forvaltninger, hvor forvaltningerne er henholdsvis: 1) dataansvarlige eller 2) berørt af et brud

2018 (25. maj - 31. december)			**2019**		**2020**	
Forvalt-ning/enhed	**Dataan-svarlig**	**Be-rørt af**	**Dataan-svarlig**	**Be-rørt af**	**Dataan-svarlig**	**Be-rørt af**
Intern Revi-sion	0	2	0	2	0	1
Borgerrådgi-veren	0	2	6	10	0	1
BIF	30	36	49	54	86	97
BUF	25	31	62	83	82	133
KFF	10	13	18	22	18	27
SOF	30	37	65	81	83	102
SUF	3	8	11	23	13	32

TMF	10	16	11	18	6	12
ØKF	20	25	61	40	103	60
I alt	**128**	**170**	**283**	**333**	**391**	**465**

Anmeldelser til Datatilsynet
Medfører et brud en sandsynlig risiko for en fysisk persons rettigheder, skal dette anmeldes til Datatilsynet. Af tabel 3 nedenfor fremgår det, hvor mange brud de respektive forvaltninger har anmeldt til Datatilsynet.

Tabel 3: Antal anmeldelser til Datatilsynet

2018 (25. maj - 31. december)			**2019**		**2020**	
Forvaltning/enhed	**Anmeldt til Datatilsynet**	**Ikke anmeldt**	**Anmeldt til Datatilsynet**	**Ikke anmeldt**	**Anmeldt til Datatilsynet**	**Ikke anmeldt**
Intern Revision	0	0	0	0	0	0
Borgerrådgiveren	0	0	5	1	0	0
BIF	16	14	47	2	60	26
BUF	16	9	49	13	45	37
KFF	3	7	8	10	2	16
SOF	19	11	50	15	47	36
SUF	0	3	3	8	4	9
TMF	4	6	3	8	5	1
ØKF	3	17	14	47	16	87
I alt	**61**	**67**	**179**	**104**	**179**	**212**

Tidligere har Datatilsynet kvartalsvis opgjort antallet af anmeldelser, som myndigheden har modtaget på landsplan. Datatilsynet har imidlertid ændret opgørelsesmetode således, at det ikke længere er muligt at sammenholde antallet af persondatabrud i Københavns Kommune med antallet på landsplan.

It-sikkerhedshændelser i 2018, 2019 og 2020
Når en medarbejder bliver opmærksom på forhold, der kan udgøre en form for sikkerhedstrussel, indberettes forholdet som en it-sikkerhedshændelse via it-portalen til Koncern IT. Hændelserne kan være forbundet med et persondatabrud, men som oftest er det en teknisk sårbarhed eller en hændelse i relation til menneskelige fejl/forsøg på udnyttelse af disse fejl. Det kan f.eks. være snitfladerne mellem to it-systemer, der ikke er sikret korrekt, eller en medarbejder, der ved en fejl har aktiveret ondsindet kode på KK's computere.

Når et forhold indmeldes, undersøges omfanget, risiciene og konsekvenserne af forholdet. Herefter igangsættes initiativer til at udbedre de konkrete forhold. Denne proces giver kommunen mulighed for at

identificere generelle sårbarheder og trends på tværs af kommunens samlede it-landskab. I tabel 4 ses udviklingen af it-sikkerhedshændelser.

Tabel 4: Antal af it-sikkerhedshændelser i 2018, 2019 og 2020

	2018	2019	2020
It-sikkerhedshændelser	120	87	124

På baggrund af tabellen ses det, at antallet af it-sikkerhedshændelser er på samme niveau som i 2018. Dog lå antallet i 2019 lidt lavere. På baggrund af den endnu korte tidsserie må det konkluderes, at antallet af informationssikkerhedshændelser i 2020 ligger på et nogenlunde stabilt niveau.

Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 3: Uddybende konklusioner fra tilsyn med informationssikkerheden og risikovurderinger 2020

16. februar 2021

Sagsnummer
2021-0051372

Dokumentnummer
2021-0051372-4

Dette bilag er en uddybende gennemgang af:

1. Koncern IT's tværgående tilsyn med informationssikkerheden i forvaltningerne 2020 og
2. Koncern IT's risikovurderinger af forvaltningernes idriftsatte it-systemer 2020.

Koncern IT fører årligt tilsyn med informationssikkerheden i forvaltningerne og gennemfører risikovurderinger af kommunens it-systemer. Resultatet af informationssikkerhedstilsynet og risikovurderingerne giver forvaltningerne mulighed for at træffe beslutning om sikkerhedsniveauet inden for egen forvaltning, som det følger af forretningscirkulæret for organisering af informationssikkerhed.

Kommunens forvaltninger udarbejder på baggrund af risikovurderingerne handleplaner, som godkendes af forvaltningernes direktioner. Kommunens kreds af it-ansvarlige direktører orienteres løbende i It-kredsen om status på implementeringen af disse. Forvaltningerne anbefales ligeledes på baggrund af informationssikkerhedstilsynet at udarbejde handleplaner.

Tilsyn med informationssikkerheden 2020

I 2020 udvalgte KIT fem tilsynsemner, som tilsynet med informationssikkerheden tager udgangspunkt i. Udvælgelse af tilsynsemner tager afsæt i en risikobaseret tilgang. Som en del af udvælgelseskriterierne er der bl.a. taget udgangspunkt i emner, hvor der tidligere er oplevet konkrete uregelmæssigheder eller skærpede krav.

Tilsynsemnerne er koordineret med kommunens databeskyttelsesrådgiver og den lovpligtige revisor for Københavns Kommune (KK).

Konklusioner fra tilsynet med informationssikkerheden

Af tabel 1 fremgår tilsynsemnerne for 2020 inklusive det samlede antal henstillinger og anbefalinger, der er givet på tværs af Københavns Kommune. Dernæst følger generelle beskrivelser af tilsynsemnerne.

Koncern IT
Sikkerhed
Borups Allé 177
2400 København NV

EAN-nummer
5798009809308

Tabel 1: Overblik over tilsynsemner på tværs af KK 2020

Tilsynsemne	Anbefalinger	Henstillinger
1. Decentral brugeradministration af systemer, der ikke autoriseres til via KK's løsning IGA/Bruger-administrationen	5	14
2. Ibrugtagningstilladelse af systemer og opfølgning	19	8
3. Backup	5	22
4. Mobile enheder i forvaltningerne	3	18
5. Fysisk sikkerhed	6	8
Total	38	40

Ad 1. Decentral brugeradministration
Forvaltningerne skal i højere grad sikre og dokumentere et tilstrækkeligt overblik over, i hvilke systemer der udføres decentral brugeradministration. Brugeradministrationen skal følge kommunens retningslinjer for adgangsstyring.

Ad 2. Ibrugtagningstilladelser
Forvaltningerne skal generelt i højere grad sikre, at der iværksættes sikkerhedsvurdering og modtages ibrugtagningstilladelser i forbindelse med anskaffelse af nye systemer. I nogle tilfælde skal det sikres yderligere, at systemer ikke idriftsættes uden ibrugtagningstilladelse og at der herefter følges tilstrækkeligt op på, at afklaringspunkter modtaget i forbindelse med afgivne ibrugtagningstilladelser bliver implementeret.

Ad 3. Backup
Forvaltningerne skal generelt i højere grad sikre, at der tages backup af de mest forretningskritiske systemer, og det skal derudover i flere tilfælde sikres, at der forefindes en dokumenteret plan for test af backup og gennemførelse af periodisk restore test.

Ad 4. Mobile enheder
Forvaltningerne skal generelt i højere grad sikre, at der foreligger en opdateret og fyldestgørende fortegnelse samt en tilstrækkelig beskrivelse af livscyklus for mobile enheder. Enkelte forvaltninger skal derudover yderligere sikre, at der vejledes særskilt om brug og sikring af mobile enheder til medarbejdere, som benytter private enheder til opgavevaretagelsen. Koncern IT vil i den forbindelse undersøge og vurdere behovet for særskilt vejledning ved brug af private enheder til opgavevaretagelsen og, hvis relevant, opdatere den eksisterende vejledning om brug af mobile enheder. Der er aftalt, at Koncern IT i den forbindelse vil orientere forvaltningernes digitaliseringsenheder.

Ad 5. Fysisk sikkerhed
Det skal generelt i højere grad sikres, at der udarbejdes og dokumenteres egentlige retningslinjer for fysisk sikkerhed således, at der etableres passende fysisk sikkerhed på forvaltningens lokationer.

Risikovurdering af it-systemer 2020

Koncern IT har afsluttet risikovurderingen af 52 af kommunens it-systemer på tværs af forvaltningerne i 2020. Se tabel 2 for oversigt over antal risikovurderede it-systemer, henstillinger og anbefalinger i den enkelte forvaltning.

Tabel 2 – Oversigt over antal risikovurderede it-systemer, henstillinger og anbefalinger i 2020

Risikovurderede it-systemer	Henstillinger	Anbefalinger
52	60	397

Sammenholdt med risikovurderingerne i 2019, er der givet færre henstillinger i 2020, hvor der i risikovurderingen 2019 blev givet i alt 146 henstillinger. Dette kan begrundes i to forhold. For det første er der risikovurderet lidt færre systemer i 2020[1], og for det andet har forvaltningerne fastsat, dokumenteret og implementeret slettefrister i de risikovurderede it-systemer i 2019, der derfor ikke optræder i 2020.

Manglende sikkerhedsforanstaltninger i KK
På tværs af de risikovurderede it-systemer er der udarbejdet en oversigt over hyppigst forekommende manglende foranstaltninger inden for de enkelte sikkerhedsområder, se tabel 3.

På baggrund af oversigten over de hyppigst manglende foranstaltninger ses det, at 42 manglende foranstaltninger relaterer sig til manglende eller utilstrækkelig periodisk gennemgang af logs og procedurer for gennemgang af logs, og 20 manglende foranstaltninger vedrører manglende sletning af logfiler eller manglende gennemgang af systemets logs.

Herudover relaterer 27 manglende foranstaltninger sig til manglende afprøvning af beredskabsplaner, og 24 manglende foranstaltninger relaterer sig til manglende måling af, hvordan leverandøren leverer i forhold til de aftalte krav/servicemål i leverandørkontrakten.

[1] I risikovurderingen 2019 blev der risikovurderet 61 it-systemer

Tabel 3 – Oversigt over sikkerhedsområder og antal systemer med manglende sikringsforanstaltninger

Sikkerhedsområde	Antal systemer med manglende foranstaltning
Procedurer og roller	
Manglende eller utilstrækkelig periodisk gennemgang af logs	22
Manglende eller mangelfuld procedure for kontrol af logs	20
Manglende etablering af kontroller, der sikrer, at medarbejdere ved fratrædelse får frataget deres rettigheder til systemer	14
En manglende procedure for håndtering, registrering og rapportering af sikkerhedshændelser	14
Lovmæssige krav (GDPR)	
Manglende udarbejdelse af en plan for tilsyn med databehandleren	15
Hvis der ikke er udarbejdet en konsekvensanalyse for behandlingsprocesserne for systemet, kan det betyde manglende vurdering af fysiske personer rettigheder og frihedsretligheder.	13
Manglende eller mangelfulde procedurer og værktøjer, som sikrer at personoplysninger slettes, når de ikke længere er nødvendige at opbevare med videre (herunder som følge af en lovmæssig forpligtelse)	10
Leverandørforhold	
Manglende måling af hvordan, leverandøren præsterer, i forhold til de aftalte krav/servicemål i kontrakt, evt. i den tilhørende SLA (Service Level Agreement)	24
Manglende regelmæssig gennemgang af informationssikkerheden kan betyde utilsigtede hændelser og manglende compliance i forhold til gældende regler i databeskyttelsesforordningen	20
Et mangelfuldt tilsyn med de/den ansvarlige leverandør, kan medføre øget risiko for, at leverandøren ikke lever op til sine kontraktmæssige forpligtelser	19
En manglende procedure for håndtering, registrering og rapportering af sikkerhedshændelser hos leverandøren, kan medføre en øget risiko for, at et sikkerhedsbrud ikke håndteres på en passende og rettidig måde af leverandøren	12
Anskaffelse, udvikling og vedligeholdelse af systemer	
En manglende it-sikkerhedsvurdering og ibrugtagningstilladelse	14
Manglende opdatering af planlægningen og driften af systemet	14
Logning og overvågning	

Manglende sletning af logs kan medføre en øget risiko for, at uautoriseret bruger får adgang til logs, samt manipulerer med data.	10
Manglende regelmæssig gennemgang af systemets logning kan medføre, at systemet kompromitteres	10
Nedbrud, backup og disaster recovery	
Manglende instrukser og kommunikation i henhold til en beredskabsplan	27
Manglende test af evnen til, at genetablere sikkerhedskopieret data	14
Manglende afprøvning af beredskabsplan	13
Manglende eller utilstrækkelige recovery mål (RTO, RPO) for backup og disaster recovery	13
Dokumentation	
Begrænset eller mangelfuldt overblik over system og netværk (arkitekturtegning over systemerne)	11
Fragmenteret eller ingen dokumentation af it-systemet	10