Undersøgelse af datahåndteringen i politiet og anklagemyndigheden

April 2021

pwc

Indholdsfortegnelse

Ledelsesresumé

Baggrund og formål med undersøgelsen

Politiet og anklagemyndigheden er en del af straffesagskæden. Politiet og anklagemyndigheden håndterer dagligt mange fortrolige og følsomme oplysninger om borgerne, herunder bl.a. CPR-numre, fingeraftryk, dna og fotos.

Korrekt og sikker håndtering af borgenes oplysninger er afgørende, da fejl i datahåndteringen i værste fald kan få stor betydning for udfaldet af fx en straffesag – og dermed for borgernes retssikkerhed og tilliden til politiet og anklagemyndigheden. Justitsministeriet har derfor en ambition om, at politiet og anklagemyndigheden, sammen med de øvrige myndigheder på Justitsministeriets område, skal være rollemodeller, når det kommer til at håndtere data korrekt og sikkert.

Som opfølgning på gennedsættelsen af Tibetkommissionen og for at indfri ambitionen om at blive rollemodel igangsatte Justitsministeriet i oktober 2019 en undersøgelse af datahåndteringen hos politiet og anklagemyndigheden. Undersøgelsen har karakter af en kulegravning, da den bygger på en struktureret og risikobaseret gennemgang af datahåndteringen i og omkring politiets og anklagemyndighedens it-systemer.

Undersøgelsens formål har været at vurdere, om datahåndteringen er korrekt og sikker, samt om det kan gøres lettere for medarbejderne at håndtere data korrekt og sikkert. Undersøgelsen har endvidere haft til formål at komme med anbefalinger, der kan gøre politiet og anklagemyndigheden i stand til at blive rollemodeller, når det kommer til at håndtere data. At blive en rollemodel kræver organisatoriske og tekniske forandringer samt en prioritering af ressourcer. Undersøgelsens anbefalinger skal derfor ses som sigtelinjer for, hvordan politiet og anklagemyndigheden med tiden kan blive rollemodeller.

Datahåndteringen i politiet

PwC har peget på ti overordnede problemstillinger, som er vurderet til at skabe udfordringer ift. korrekt og sikker datahåndtering på tværs af politiets systemer. De ti tværgående problemstillinger har både en direkte og en indirekte indflydelse på datahåndteringen. Det er PwC's vurdering, at omfanget og typen af problemstillingerne ligner dem, som kendes fra andre organisationer med tilsvarende størrelse og kompleksitet. Den samfundsmæssige konsekvens ved uautoriseret adgang, tab og forvanskning af data hos politiet er dog efter PwC's vurdering langt større end i andre organisationer med samme størrelse og kompleksitet.

For hver af de ti tværgående problemstillinger har PwC udarbejdet en anbefaling til et initiativ med tilhørende aktiviteter. Initiativerne og de underliggende aktiviteter kan ses som sigtelinjer for, hvordan politiet med tiden kan blive en rollemodel. Initiativerne er udarbejdet på baggrund af de principper, som PwC har for, hvad der skal til for at være en rollemodel ift. korrekt og sikker datahåndtering. De ti problemstillinger og PwC's anbefalinger er:

1. Overblik over systemer

Politiets systemoverblik består af flere systemlister, som indeholder oplysninger om de it-systemer, politiet råder over og anvender. Undersøgelsen har vist, at systemoverblikket ikke er fuldt dækkende og ensartet. PwC anbefaler, at politiet udarbejder *en ensartet og opdateret systemliste*. Politiet har igangsat implementeringen af initiativet i foråret 2020 parallelt med undersøgelsen.

2. Governance og processer

Politiet har udarbejdet governance- og procesbeskrivelser, der bl.a. beskriver ansvarsfordelingen og ejerskabet for opgaverne omkring systemerne, som skal bidrage til at sikre korrekt og sikker datahåndtering. Undersøgelsen har vist, at politiets governancemodel og processer ikke er fuldt implementeret. PwC anbefaler, at politiet *opdaterer og forankrer sit systemejerskabskoncept*, og dermed arbejder videre med at kvalificere og implementere det arbejde, som er igangsat på området.

3. Læring

Politiet har i dag en række både formelle og uformelle læringsindsatser i forhold til datahåndtering. Undersøgelsen indikerer, at medarbejderne ikke altid er sikre på, hvordan de skal foretage en korrekt og sikker datahåndtering. Undersøgelsen viser desuden, at læringsindsatsen ikke er koordineret og struktureret på tværs af politiet. PwC anbefaler, at der sker *en styrket og koordineret læringsindsats*, der med fordel kan tage udgangspunkt i en række af de initiativer, som er igangsat lokalt, fx obligatorisk e-læring.

4. Systemunderstøttelse af arbejdsprocesser

Politiets arbejde er understøttet af ca. 1.100 it-systemer, databaser, infrastrukturkomponenter mv.og en lang række manuelle og papirbaserede arbejdsgange. Undersøgelsen har vist, at der er manuelle arbejdsgange, som med fordel kan systemunderstøttes bedre, da de ikke understøtter, at medarbejderne nemt kan foretage en korrekt og sikker datahåndtering. PwC anbefaler, at politiet arbejder med at sikre en *bedre systemunderstøttelse af arbejdsprocesserne*. Som led i Aftale om politiets og anklagemyndighedens økonomi 2021-23, skal politiet igangsætte en række initiativer med henblik på at forbedre systemunderstøttelsen af arbejdsprocesserne.

5. Sletning

Medarbejderne i politiet har behov for at kunne opbevare oplysninger ift. deres videre sagsbehandling. Undersøgelsen har vist eksempler på, at der opbevares personoplysninger i længere tid uden for systemerne. PwC anbefaler, at politiet arbejder med at styrke *overvågning og opfølgning på sletning.* Det kan med fordel ske med en videre implementering af politiets nye dataovervågningsværktøj (DLP).

6. Dataklassifikation

Politiet skal klassificere sine data. Politiet og anklagemyndigheden anvender to forskellige klassifikationsmodeller. PwC kan konstatere, at klassifikationen sker på systemniveau. Dvs. at alle data i et system klassificeres på samme niveau. For at blive en rollemodel, så anbefaler PwC, at politiet arbejder med en *effektivisering og forenkling af dataklassifikationen*, hvilket fx kan være i et samarbejde på tværs af Justitsministeriets område. Herudover er visse af politiets informationer klassificeret efter sikkerhedscirkulæret, men disse har ikke været en del af undersøgelsen og er derfor ikke omfattet af PwC's anbefaling.

7. Brugerstyring

Politiets brugerstyringsprincipper afspejler, at politiet er en operativ myndighed, der er understøttet af en række systemer, som afhængig af opgaverne, skal være tilgængelige for medarbejderne, når behovet opstår. Undersøgelsen viser, at der ikke altid sker en systematisk opdatering af brugerrettigheder. PwC anbefaler, at politiet arbejder med en *mere aktiv brugerstyring*, hvilket bl.a. kan ske ved implementering af det nye IAM-system, som politiet er ved at anskaffe.

8. Logning

Politiet har implementeret logning og en bearbejdning af logdata på en lang række systemer. Undersøgelsen har vist, at selv om politiet et højt logningsniveau, så dækker det ikke fuldt ud på de mange ældre og specialudviklede systemer. PwC anbefaler en *øget udbredelse og anvendelse af logning*, hvilket kan ske ved at bygge videre på det arbejde politiet har igangsat på området.

9. Kryptering

Politiet anvender kryptering til at sikre fortroligheden af data under kommunikationen, delingen og lagringen af oplysninger i politiet. Undersøgelsen har vist, at der er data, hvor sikkerheden kan øges med kryptering. PwC anbefaler, at der sker en øget *beskyttelse af data ved benyttelse af kryptering*.

10. Legacy-systemer

Politiet foretager løbende en opdatering og udskiftning af deres systemer, men har fortsat en række ældre systemer (legacy-systemer), som bygger på udfaset eller forældet teknologi. Undersøgelsen har vist, at den udfasede og forældede teknologi kan medføre en række alvorlige sikkerhedsmæssige udfordringer. PwC anbefaler, at politiet på kort sigt arbejder på at skabe en *sikker datahåndtering i legacy-systemerne*, samt at politiet på længere sigt fortsætter arbejdet med at udskifte sine legacy-systemer.

Politiet har igennem en længere årrække været bekendt med og arbejdet på at løse flere af de problemstillinger, som PwC har peget på. Det er PwC's vurdering, at politiet på en række områder har haft en relativt lang implementeringstid.

Politiet har udarbejdet og igangsat implementeringen af en ny it-handlingsplan, som bl.a. omfatter initiativer, der styrker datahåndteringen. Der er afsat midler til implementeringen af it-handlingsplanen med Aftale om politiets og anklagemyndighedens økonomi 2021-23. Det er PwC's vurdering, at der også efter 2023 vil være behov for at arbejde med at implementere initiativer til at styrke korrekt og sikker datahåndtering.

Datahåndteringen i anklagemyndigheden

Den centrale anklagemyndighed er væsentlig mindre i størrelse og har også en langt mindre kompleksitet i sit systemlandskab sammenlignet med politiet.

PwC har peget på fire tværgående problemstillinger hos anklagemyndigheden, som er vurderet til at skabe udfordringer ift. korrekt og sikker datahåndtering. Det er PwC's vurdering, at omfanget og typen af problemstillingerne er mindre end hos lignende organisationer med tilsvarende størrelse og kompleksitet. Det skyldes bl.a., at anklagemyndigheden har implementeret ISO27001 og GDPR samt det arbejde, Rigsadvokaten har foretaget ifm. overgangen til Statens It.

For hver af de fire tværgående problemstillinger har PwC udarbejdet en anbefaling til et initiativ med tilhørende aktiviteter. Initiativerne og de underliggende aktiviteter kan ses som sigtelinjer for, hvordan den centrale anklagemyndighed med tiden kan blive en rollemodel. Initiativerne er udarbejdet på baggrund af de principper, som PwC har for, hvad der skal til for at være en rollemodel ift. korrekt og sikker datahåndtering. De fire problemstillinger og PwC's anbefalinger er:

1. *Governance og processer*

   Anklagemyndigheden har implementeret en praksis for rolle- og ansvarsfordelingen samt processerne forbundet med systemejerskabet. Undersøgelsen har vist, at governance og processer ikke er fuldstændigt operationaliseret og dokumenteret, hvilket kan gøre det personafhængigt. PwC anbefaler, at *systemejerskabet i højere grad dokumenteres* for, at anklagemyndigheden kan blive en rollemodel. Det kan med fordel kan ske med udgangspunkt i den eksisterende praksis.

2. *Dataklassifikation*

   Anklagemyndigheden skal klassificere sine data. Politiet og anklagemyndigheden anvender to forskellige klassifikationsmodeller. PwC kan konstatere, at klassifikationen sker på systemniveau. Dvs. at alle data i et system klassificeres på samme niveau. For at blive en rollemodel, så anbefaler PwC, at anklagemyndigheden arbejder med en *effektivisering og forenkling af dataklassifikationen*, hvilket fx kan være i et samarbejde på tværs af Justitsministeriets område.Herudover er visse af anklagemyndighedens informationer klassificeret efter sikkerhedscirkulæret, men disse har ikke været en del af undersøgelsen og er derfor ikke omfattet af PwC's anbefaling.

3. *Logning*

   Anklagemyndigheden skal logge data. Undersøgelsen indikerer, at anklagemyndigheden generelt set har implementeret et fornuftigt niveau af logning, dog med enkelte afvigelser hvis anklagemyndigheden skal blive rollemodel inden for logning. PwC anbefaler en *proaktiv anvendelse af log-data*, hvilket skal ske i samarbejde med Statens IT.

4. *Kryptering*

   Anklagemyndigheden anvender kryptering til at sikre fortroligheden af data under kommunikationen, delingen og lagringen af oplysninger i anklagemyndigheden. Undersøgelsen har vist, at der er data, hvor sikkerheden kan øges med kryptering. For at anklagemyndigheden kan blive en rollemodel, anbefaler PwC, at der sker en *øget udbredelse af anvendelsen af kryptering*, under hensynstagen til systemernes tilgængelighed og følsomheden af data.

Anklagemyndigheden er bevidste om de udfordringer, som PwC har påpeget. Anklagemyndigheden har oplyst, at problemstillingerne er i fokus, herunder i forbindelse med overgangen til Statens IT.

Vejen til at blive en rollemodel

Det er PwC's vurdering, at en implementering af initiativerne og de enkelte aktiviteter må anses for at være en betydelig opgave for enhver organisation. Implementering af de anbefalede initiativer vil bl.a. kræve, at der prioriteres betydelige ressourcer til arbejdet med at styrke rammerne for sikker og korrekt datahåndtering. Det gælder især for politiet, som fx i sin systemportefølje har en stor teknisk gæld samt behov for omfattende it-moderniseringer, som politiet ikke forventer er fuldt ud løst med den politiske aftale om politiets og anklagemyndighedens økonomi for 2021-23.

Det er derfor PwC's anbefaling, at politiet og anklagemyndigheden udarbejder en handlingsplan, hvor de under hensyn til øvrige aktiviteter og økonomi prioriterer, i hvilken rækkefølge initiativerne og de enkelte aktiviteter i disse initiativer implementeres mest hensigtsmæssigt. Prioriteringen af, hvad myndighederne skal starte med kan bl.a. tage udgangspunkt i, hvad myndighederne allerede har af planer, fx i regi af deres it-handlingsplaner, samt om det er vigtigst at højne en korrekt eller sikker datahåndtering eller at gøre det nemmere for medarbejderne at håndtere data.

Det er PwC's anbefaling, at politiet og anklagemyndigheden sikrer en ledelsesmæssig forankring af handlingsplanerne, således at der internt i myndighederne er fokus på implementeringen af anbefalingerne. Det er endvidere PwC's anbefaling, at Justitsministeriet i relevant omfang følger op på, om politiet og anklagemyndigheden implementerer handlingsplanerne.

For at sikre bedre rammer for, at medarbejderne kan håndtere data både korrekt, sikkert og nemt, så er det endelig PwC's anbefaling, at myndighederne på baggrund af undersøgelsen igangsætter et arbejde med at vurdere, om de interne retningsliner for datahåndtering kan forsimples yderligere, således at det bliver lettere at lave en god systemunderstøttelse, samt at den enkelte medarbejder lettere kan forstå reglerne.

1. Baggrund og formål

Baggrunden og formålet med undersøgelsen

Justitsministeriet har en ambition om, at myndighederne inden for Justitsministeriets område, herunder politiet og anklagemyndigheden, skal være rollemodeller, når det kommer til at håndtere data korrekt og sikkert. Det er en ambition, som vil kræve organisatoriske og systemmæssige forandringer i koncernen – og som derfor vil tage tid af indfri. Justitsministeriets ambition om, at politiet og anklagemyndigheden skal være rollemodeller, betyder, at myndighederne inden for visse områder sætter barren højt.

Som opfølgning på gennedsættelsen af Tibetkommissionen og for at begynde arbejdet med at indfri ambitionen om at blive rollemodel igangsatte Justitsministeriet i oktober 2019 en undersøgelse af datahåndteringen hos politiet og anklagemyndigheden.

Undersøgelsen har for det første haft til formål at vurdere, om politiet og anklagemyndigheden håndterer data *korrekt* og *sikkert*. Med *korrekt* fokuseres på den praksis, som medarbejderne har ifm. databehandlingen. Det vil fx sige, om medarbejderne registrerer, gemmer og sletter data korrekt og inden for de gældende retningslinjer. Med *sikker* fokuseres der på sikkerheden og rammerne omkring de it-systemer, hvor der behandles data. Det vil fx sige, om der er en tilstrækkelig kryptering og logning af data.

Undersøgelsen har for det andet til formål at vurdere, om politiet og anklagemyndigheden kan gøre det *nemmere for medarbejderne* at håndtere data korrekt og sikkert, fx ved at de styringsmæssige, organisatoriske, uddannelses og/eller de it-mæssige rammer bedre understøtter datahåndteringen i det daglige arbejde.

Justitsministeriet ønsker, at undersøgelsen kommer med anbefalinger, der kan håndtere myndighedernes konkrete udfordringer med datahåndtering samt bruges som sigtelinjer for, hvordan politiet og anklagemyndigheden – med tiden – kan blive rollemodeller.

Denne rapport er opdelt i fire afsnit foruden baggrunds- og formålsafsnittet:

- I afsnit *2. Datahåndtering i politiet og anklagemyndigheden* beskrives den datahåndtering, der typisk foregår i politiet og anklagemyndigheden på tværs af processer, systemer og medarbejdergrupper.
- I afsnit 3. *Sigtelinjer* for *datahåndteringen hos politiet* peges på tværgående problemstillinger og initiativer vedr. en korrekt og sikker datahåndtering hos politiet.
- I afsnit 4. *Sigtelinjer for datahåndteringen hos anklagemyndigheden* peges på tværgående problemstillinger og initiativer vedr. en korrekt og sikker datahåndtering hos anklagemyndigheden.
- I afsnit *5. Grundlaget for gennemførelsen af undersøgelsen* beskrives den metodiske tilgang og de væsentligste afgrænsninger.

2. Datahåndtering i politiet og anklagemyndigheden

Organisatorisk afgrænsning

Undersøgelsen af datahåndteringen er foretaget hos politiet og anklagemyndigheden.

Politiet er organiseret i Rigspolitiet (herunder PET) samt 12 politikredse i Danmark. Anklagemyndigheden er organiseret i Rigsadvokaten, Statsadvokaten i København og Statsadvokaten i Viborg, Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK) samt den lokale anklagemyndighed i politikredsene.

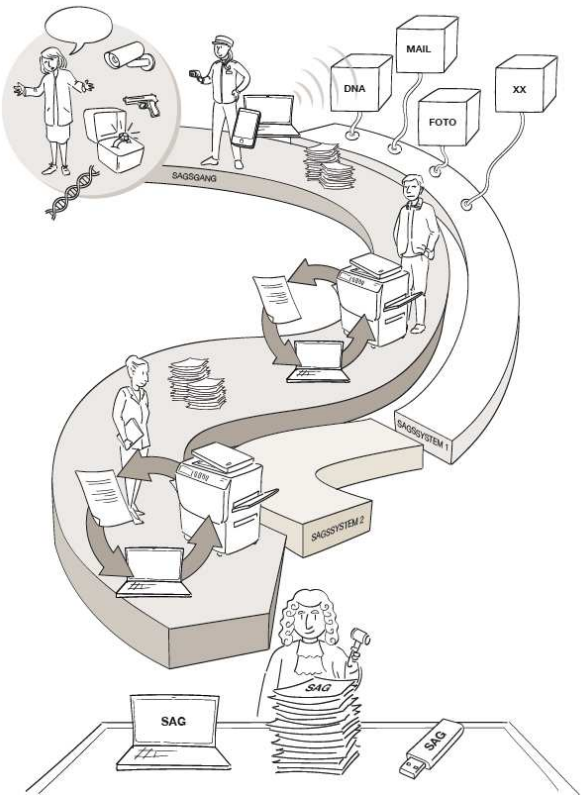
Da den lokale anklagemyndighed og SØIK anvender politiets it-udstyr, it-systemer og sikkerhedsprocedurer mv. indgår de i undersøgelsen, som en del af politiet. Undersøgelsen af anklagemyndigheden omfatter således alene Rigsadvokaten, Statsadvokaten i København og Statsadvokaten i Viborg, og henvisninger til "anklagemyndigheden" skal således i regi af undersøgelsen forstås som en henvisning til disse tre myndigheder. PET samt politiet og anklagemyndigheden i Grønland og på Færøerne er ikke en del af undersøgelsen.

Rent organisatorisk er politiet med ca. 16.500 medarbejdere langt større og mere kompleks end anklagemyndigheden, der betjener ca. 300 medarbejdere. Politiet har derudover flere forskellige typer af medarbejdere end anklagemyndigheden, idet at der både er forskellige typer af administrative medarbejdere, sagsbehandlere og politifolk.

Systemunderstøttelsen af datahåndteringen

Datahåndteringen ifm. behandlingen af en sag kan være relativt kompleks – især i politiet – da sagsbehandlingen oftest foregår delvist digitalt og delvist fysisk, *jf. figur 1.*

Figur 1. Eksempel på et straffesagsforløb



En straffesag kan starte på flere forskellige måder. Ofte foregår det ved, at borgeren henvender sig til politiets vagtcentral via 112. I mange tilfælde udføres en mindre sagsbehandling af sagen ved sagens opstart, hvorefter sagen visiteres.

Sager med en vis kompleksitet, registreres direkte i politiets sagsstyringssystem og kræves behandlet af en efterforsker, som ofte arbejder med en fysisk sag, der afspejler den digitale sag i sagsstyringssystemet. Efterforskeren har under sin sagsbehandling ofte behov for at indsamle og opbevare data fra sagsakter, som ligger i flere andre systemer eller på fysiske medier. Det kan fx være foto- eller fingeraftryksdata, videofiler og fysiske beviser. Det sker ofte, fordi det ikke er muligt at opbevare al data på sagen digitalt eller i ét system, samt fordi systemerne ikke altid integrerer med hinanden effektivt.

Når en straffesag er færdigbehandlet af en efterforsker i politiet, overdrages sagen typisk til den lokale anklagemyndighed, som varetager den videre håndtering af sagen, herunder navnlig stillingtagen til tiltalespørgsmålet. Her er det særligt vigtigt, at den ansvarlige anklager både via den fysiske og den digitale sag kan få et fuldt overblik over sagens oplysninger, herunder hvem der har haft ansvaret for sagen og hvem der ved hvad om sagen hos politiet.

Statsadvokaterne i Viborg og København (de regionale statsadvokater) varetager bl.a. udførelsen af ankesager ved landsretterne og behandler klager over afgørelser, som er truffet af politikredsene vedrørende strafforfølgning. Rigsadvokaten varetager bl.a. straffesager ved Højesteret og behandler klager over afgørelser truffet af statsadvokaterne i 1. instans. I forbindelse med bl.a. anke af en sag eller klage over en afgørelse, vil sagen således blive sendt til en af de regionale statsadvokater eller til Rigsadvokaten.

Opmærksomhedspunkter ved politiet og anklagemyndighedens datahåndtering

Politiets og anklagemyndighedens forskellige opgaver betyder, at datahåndteringen hos de to myndigheder adskiller sig fra hinanden på visse centrale punkter.

De centrale arbejdsprocesser i en politikreds involverer ofte mange forskellige interne aktører (politibetjente, anklagere fra den lokale anklagemyndighed i politikredsen, og sagsbehandlere) og eksterne aktører fra fx kommunerne. Politiets centrale processer omfatter endvidere mange it-systemer, som understøtter forskellige behov for registrering og behandling af data. Anklagemyndighedens arbejdsprocesser er typisk mere enkle/ensartede, involverer færre aktører og har en mere simpel systemunderstøttelse.

Politiet står i modsætning til anklagemyndigheden også selv for videreudviklingen og driften af nogle af sine forretningskritiske systemer, mens anklagemyndighedens systemer primært videreudvikles og driftes af eksterne leverandører. Politiet har samtidig, i modsætning til anklagemyndigheden, i højere grad løbende behov for at modernisere og videreudvikle sin it-systemportefølje, fordi behovene for især den operative og beredskabsmæssige del af politiets forretning ændres i takt med ændringer i kriminalitetsbilledet, ny lovgivning, politiske initiativer og den teknologiske udvikling mv., og fordi en stor del af politiets centrale og forretningskritiske systemer stammer tilbage fra 1980'erne og 1990'erne og derfor må betegnes som "legacy-systemer".

Politiets løbende modernisering og videreudvikling af it-systemerne kræver, at politiet til enhver tid har et fuldstændigt overblik over sin it-systemportefølje, herunder at politiet har et overblik over, hvem der har det interne forretningsmæssige og tekniske ansvar over, hvilke systemer der er hos politiet.

Både politiet og anklagemyndigheden har et behov for at registrere mange forskellige typer af data i forbindelse med oprettelse og behandling af fx straffesager, herunder almindelige, fortrolige og følsomme personoplysninger og forretningskritiske data. Det er fx fingeraftryk, dna, fotos samt CPR-numre og andre fortrolige og følsomme personoplysninger samt oplysninger om strafbare forhold. Her er det særligt vigtigt, at data klassificeres korrekt og at håndtering af data logges tilstrækkeligt, ligesom det er vigtigt, at de systemer, hvor data håndteres, herunder registreres og deles, har en tilstrækkelig kryptering især de kommunikationskanaler, der bliver anvendt til selve dataregistreringen og dataudvekslingen.

De mange systemer og data betyder, at det er vigtigt, at medarbejderne har fået den rette oplæring i korrekt og sikker datahåndtering, og at medarbejderne ved, hvornår data som registreres bør slettes igen.

3. Sigtelinjer for datahåndteringen hos politiet

Overblik over tværgående problemstillinger og initiativer

Baseret på PwC's observationer fra såvel spørgeskemaer, systemgennemgang og dataflowanalyser (se afsnit 5 om metoden) har PwC peget på ti tværgående problemstillinger, som skaber udfor-dringer i forhold til korrekt og sikker datahåndteringen på tværs af politiets systemer. Det er PwC's vurdering, at omfanget og typen af problemer ligner det andre organisationer med samme kompleksitet har.

De ti tværgående problemstillinger, PwC har peget på påvirker både en korrekt og sikker data-håndtering indirekte og direkte.

Undersøgelsen viser, at datahåndteringen påvirkes indirekte ved fx, at politiet ikke har et fuldt dækkende og ensartet systemoverblik, samt at governance og processer ikke er fuldt implemente-ret. En korrekt datahåndtering påvirkes desuden direkte af den læringsindsats, systemunderstøt-telse, sletning og dataklassifikation, som politiet har i dag. Endvidere påvirkes en sikker data-håndtering direkte af udfordringer omkring logning, kryptering og legacysystemer.

Flere af problemstillingerne kan dog også påvirke både en korrekt og sikker datahåndtering. Fx læring, legacyproblemstillinger mv.

Justitsministeriet har en ambition om, at myndighederne inden for Justitsministeriets område skal blive rollemodeller i forhold til at håndtere data korrekt og sikkert. Justitsministeriet forventer, at ambitionen vil tage tid at indfri, da det vil kræve betydelige investeringer samt større organisatoriske og tekniske forandringer.

PwC har udarbejdet ti initiativer der tilsammen indeholder 52 aktiviteter, som vil kunne imødegå de ti tværgående problemstillinger. Det ti initiativer omfatter:

1. Ensartet og opdateret systemliste
2. Opdateret og forankret systemejerskabskoncept
3. Styrket og koordineret læring
4. Bedre systemunderstøttelse af arbejdsprocesserne
5. Overvågning og opfølgning på sletning
6. Effektivisering og forenkling af dataklassifikationen
7. Mere aktiv brugerstyring
8. Udbredelse og anvendelse af logning
9. Beskyttelse af data ved benyttelse af kryptering
10. Sikker datahåndtering i legacy-systemer

Det er PwC's vurdering, at det vil være en ressourcekrævende og stor opgave at implementere alle initiativerne og de tilhørende aktiviteter, hvorfor det naturligt vil strække sig over en årrække, og der vil skulle ske en prioritering af implementeringen af initiativerne hos politiet og anklagemyndigheden. Aktiviteterne under hvert initiativ har en vis kronologisk sammenhæng, men kan i mange tilfælde godt igangsætte parallelt eller enkeltvist samt på enkelt system- eller sagsbehandlingsområde, hvis myndigheden vurderer, det er hensigtsmæssigt.

Initiativ 1. Ensartet og opdateret systemliste

Et ensartet og opdateret overblik over de systemer, hvor der behandles data i, er et vigtigt grundlag for at kunne sikre en korrekt og sikker datahåndtering.

Politiet har en stor og kompleks systemportefølje, som er forankret forskellige steder i organisationen. Undersøgelsen har vist, at politiets systemoverblik ikke har været fuldt dækkende og ensartet. Politiet havde ved undersøgelsens begyndelse flere uens systemlister, der indeholdt oplysninger om de it-systemer, som politiet råder over og anvender. Endvidere har undersøgelsen vist, at governance og processer for opdatering af systemoverblikket ikke var implementeret.

For at sikre en ensartet og opdateret systemliste, anbefaler PwC, at der igangsættes seks aktiviteter:

a. Etablering af en governancestruktur for udarbejdelsen af systemoverblikket

b. Etablering af en klar procedure for vedligehold af oplysninger i systemlisten

c. Sikring af compliance

d. Kvalificering af eksisterende oplysninger om systemlisten

e. Etablering af en fælles kultur omkring opbygning og vedligeholdelse af systemlisten

f. Systemunderstøttelse af systemlisten til sikring af en effektiv vedligeholdelse og administration

I foråret 2020 igangsatte politiet et arbejde for at forbedre systemoverblikket med afsæt i de aktiviteter, som PwC har anbefalet.

Initiativet forudsætter mindre ændringer af vejledninger mv., men det forudsætter også en større forandringsledelsesopgave, idet en lang række systemejere og ledere skal ændre praksis.

Initiativ 2. Opdateret og forankret systemejerskabskoncept

Et systemejerskabskoncept definerer, hvem der har ansvaret for et system. Det kan fx være ansvaret for at uddanne og træne brugerne i korrekt datahåndtering og implementere sikkerhedstiltag, så som logning og kryptering, der understøtter en sikker datahåndtering.

Politiet forvalter mange systemer, som både Rigspolitiet, de enkelte kredse (herunder den lokale anklagemyndighed) og SØIK anvender. Der er i dag etableret en central sikkerhedsorganisation og databeskyttelsesenhed i Rigspolitiet. Politiet har desuden i 2017 udarbejdet et systemejerskabskoncept, men det er ikke implementeret og forankret i hele politiet.

For at sikre en klar rolle- og ansvarsfordeling omkring systemejerskabet anbefaler PwC, at der igangsættes syv aktiviteter:

a. Fælles systemejerskabskoncept på tværs af politiet

b. Proces for risikovurdering og informationssikkerhedskontinuitet

c. Proces for tildeling af systemejerskab

d. Uddannelse og oplæring i systemejerskabsrollen

e. Opfølgning på systemejerskabet

f. Implementeringsplan for systemejerskabskonceptet

g. Central organisatorisk forankring af systemejerskabskonceptet

Initiativet vurderes at understøtte, at det bliver lettere at håndtere data korrekt. Initiativet kræver imidlertid en større ændring af praksis hos mange medarbejdere og ledere. Det vil derfor kunne tage tid at implementere initiativet fuldt ud.

Initiativ 3. Styrket og koordineret læring

Viden omkring korrekt og sikker datahåndtering er en forudsætning for, at medarbejderne håndterer data på den bedst mulige måde. Politiet er en stor organisation med flere forskellige faggrupper, der har forskellige opgaver. En stor andel af medarbejderne er politiuddannede med operative opgaver. De har adgang til mange systemer, som de ikke altid anvender, men skal vide, hvordan de anvender, hvis de får behov for det med kort varsel som led i deres operative arbejde. En række af systemerne indeholder fortrolige og følsomme personoplysninger, og det er derfor vigtigt at vide, hvordan de behandles korrekt og sikkert.

Undersøgelsen indikerer, at der er medarbejdere, som er usikre på, hvordan de skal foretage en korrekt og sikker datahåndtering, samt at medarbejderne oplæres på en uensartet måde. PwC har i forbindelse med undersøgelsen fundet gode eksempler på læringsaktiviteter. Undersøgelsen har dog vist, at der ikke findes en samlet koordination, implementering og opfølgning på uddannelse omkring korrekt og sikker datahåndtering på tværs af politiet og dets forskellige personalegrupper.

For at sikre, at viden omkring korrekt og sikker datahåndtering forankres bedst muligt, anbefaler PwC, at der igangsættes seks aktiviteter:

a. Governance og rolle/ansvarsfordeling for læring vedr. korrekt og sikker datahåndtering

b. Læringsstrategi vedr. korrekt og sikker datahåndtering

c. Fokuseret løft af vidensniveauet omkring korrekt og sikker datahåndtering

d. Obligatorisk, årligt e-læringskursus og -test

e. Øget vidensniveau omkring håndteringen af data relateret til systemerne

f. Opfølgning på praksis og tilpasning af læringsindsatsen

Det er PwC's vurdering, at initiativet vil gøre det lettere for medarbejderne at håndtere data korrekt, da de har et bedre vidensgrundlag at handle ud fra. PwC vurderer samtidig, at initiativet vil kræve en ændret praksis hos medarbejdere, ledere og centrale læringsagenter (Politiskolen, kredsene, DPO'en og systemejere mv.), hvilket PwC's erfaring tilsiger vil tage tid.

Initiativ 4. Bedre systemunderstøttelse af arbejdsprocesserne

Politiet er en stor organisation med mange brugere, som løser mange forskelligartede opgaver. Særligt i politikredsene, hvor en stor del af den daglige sagsbehandling og den operative drift foregår, er det vigtigt, at de systemer, som understøtter behandling af forskellige typer af sager, samt det arbejde, der relaterer sig til den interne operative drift, ikke unødigt stiller krav til datahåndteringen. Mange af politiets centrale systemer er i dag præget af, at de er forældede (legacy-systemer) og ikke er opbygget, så de understøtter de nutidige behov ift. datahåndtering samt løsningen af opgaver.

Undersøgelsen har vist, at mange brugere oplever, at der i dag ikke er tilstrækkelig systemunderstøttelse af fx journalisering, sagsbehandling eller løbende opbevaring af data. Det gælder særligt sager med anden karakter end straffesager og løsning af andre driftsrelaterede opgaver som fx håndtering af budgetter, indkøb eller tilsyn.

For at sikre en bedre systemunderstøttelse, anbefaler PwC, at der igangsættes seks aktiviteter:

a. Etablering af et fælles dialogforum omkring systemunderstøttelse

b. Afdækning af kritiske udfordringer ved systemunderstøttelsen i dag

c. Udarbejdelse af principper for systemunderstøttelse og roadmap for gennemførelse af kritiske initiativer

d. Etablering af en effektiv implementeringsproces

e. En løbende opfølgning og evaluering af implementerede initiativer.

Initiativet vurderes i høj grad at bidrage til, at det bliver nemmere for medarbejderne at håndtere data korrekt og sikkert. Initiativet vil medføre større systemtilpasninger og dermed tage tid at implementere.

Initiativ 5. Overvågning og opfølgning på sletning

Sletning af data er afgørende for at opnå en korrekt og sikker datahåndtering.

Undersøgelsen viser, at politiets medarbejdere opbevarer bl.a. CPR-numre og fingeraftryk på personlige drev og fællesdrev i længere tid. PwC vurderer, at udtrukne data ikke har samme høje sikringsniveau, som data opbevaret i de pågældende systemer. Fx er der ikke samme sporbarhed via logning af, hvem der tilgår eller ændrer data på et fællesdrev.

For at sikre øget overvågning og opfølgning på sletning af data, anbefaler PwC, at der igangsættes fem aktiviteter:

a. Afdækning af systemers mulighed for at indføre automatisk sletning

b. Implementering af automatisk identificering af uhensigtsmæssige dataudtræk, såvel som uhensigtsmæssig opbevaring eller udprintning

c. Implementering af automatisk underretning til brugere omkring sletning af data

d. Implementering af automatisk underretning til ledere omkring sletning af data i fællesmapper og funktionspostkasser

e. Minimere behovet for fysiske print

Initiativet forventes at gøre det nemmere for medarbejderne at vide, hvornår noget data potentielt håndteres forkert, så de lettere kan handle på det. Initiativet vurderes primært at kræve en tilretning af politiets anvendelse af DLP-system, samt ændret praksis hos ledere og medarbejdere, som skal handle på den nye information.

Initiativ 6. Effektivisering og forenkling af dataklassifikationen

En tydelig markering af dataklassifikation af fysiske og logiske data reducerer risikoen for enten overbeskyttelse af mindre væsentlige data eller utilstrækkelig beskyttelse af mere væsentlige data.

Politiet og anklagemyndigheden anvender to forskellige klassifikationsmodeller. PwC kan konstatere, at klassifikationen sker på systemniveau. Dvs. at alle data i et system klassificeres på samme niveau. Herudover er visse af politiets informationer klassificeret efter sikkerhedscirkulæret, men disse har ikke været en del af undersøgelsen og er derfor ikke omfattet af PwC's anbefaling.

For at sikre en bedre dataklassificering, anbefaler PwC, at der, efter en risikobaseret tilgang, igangsættes fem aktiviteter:

a. Forenkling af retningslinjerne for dataklassifikation

b. Teknisk understøttelse og kontrol af dataklassifikation

c. Elektronisk påtrykning af dataklassifikation på relevante data

d. Hjælpefunktioner til dataklassifikationer af nye data

e. Proces for op- og nedklassificering af data

Initiativet vurderes at bidrage til, at det bliver nemmere for brugerne at håndtere data korrekt og sikkert, idet det må forventes, at implementering af en teknisk understøttelse, regelforenkling samt automatisk påtrykning af dataklassifikation kan lette den enkelte i det daglige arbejde. Initiativet vurderes at have en høj kompleksitet, da det forudsætter ændring i eksisterende systemer, vejledninger og datamodeller samt implementering af yderligere løsninger. Samtidig vurderes initiativet at kræve, at medarbejderne mere aktivt begynder at klassificere data, hvilket vil kræve en ændret praksis.

Initiativ 7. Mere aktiv brugerstyring

Brugerstyring er med til at sikre, at medarbejderne kun har adgang til de systemer, som de har et arbejdsbetinget behov for at benytte. Politiet har valgt at have en bred brugeradgang til sine systemer, hvilket skyldes, at politiet er en operativ myndighed, hvor mange medarbejdere hurtigt vil skulle kunne tilgå forskellige systemer fx i en krisesituation.

For at sikre en bedre brugerstyring, anbefaler PwC, at der igangsættes fire aktiviteter:

a. Opdeling og gruppering af medarbejdere i forhold til arbejdsbetinget behov for adgang

b. Etablering af automatik omkring livscyklussen for brugerkonti og deres rettigheder, for de systemer der understøtter integrering med brugerstyringssystemet

c. Afklaring af processer til brugerkonti og rettighedsattestering for manuelt håndterede systemer

d. Afklaring af mulighed for etablering af personhenførbare konti i systemer, hvor der benyttes fællesbrugere

Politiet er i gang med at anskaffe et nyt Identity & Access Management (IdM/IAM)-system, som til enhver tid vil kunne give et præcist billede af, hvilke brugere der har adgang til hvilke systemer, samt hvilke adgange de har i systemerne og dermed give bedre mulighed for at foretage løbende opfølgning og kontrol.

Det er PwC's vurdering, at initiativet, herunder politiets anskaffelse af et IAM-system, vil bidrage til at sikre, at politiet lever op til de krav og udfører de kontroller, som understøtter en aktiv brugerstyring. Initiativet vurderes ikke at påvirke medarbejdernes datahåndtering direkte. Initiativet vurderes at kræve ændrede processer samt evt. systemtilpasninger.

Initiativ 8. Udbredelse og anvendelse af logning

Logning bidrager til at skabe en sporbarhed i benyttelsen af data. Konsistent logning af høj kvalitet på tværs af en kompleks systemportefølje er en udfordring for mange organisationer. Det er det også for politiet, som har et høj logningsniveau, men som ikke fuldt ud dækker de mange ældre og specialudviklede systemer.

For at sikre udbredelse og anvendelse af logning, anbefaler PwC, at der igangsættes fem aktiviteter:

a. Definition af log-typer og prioritering af anvendelse

b. Benyttelse af log-registreringer i forhold til identificering af brug af systemer

c. Central indsamling af log-registreringer

d. Monitorering og proaktiv alarmering

e. Fuldt dækkende log-registreringer

Initiativet forventes at kræve omkodning af log-funktionalitet og dermed en systemtilpasning.

Initiativ 9. Beskyttelse af data ved benyttelse af kryptering

Formålet med kryptering er at sikre, at uvedkommende ikke kan få adgang til politiets fortrolige og følsomme data, når de opbevares og deles.

Politiet behandler og deler mange følsomme personoplysninger omkring borgerne. Derfor er det vigtigt, at datatransmissionerne altid er beskyttede med effektiv kryptering. Kryptering kan være en udfordring, når man ligesom Rigspolitiet har meget specialiserede og forældede systemer.

For at sikre bedre beskyttelse af data ved benyttelse af kryptering, anbefaler PwC, at der igangsættes fem aktiviteter:

a. Fuldstændig afdækning af hvilke systemer der effektivt krypterer kommunikation imellem slutbrugere og selve systemet

b. Prioritering og implementering af effektiv kryptering på kritiske systemer, hvor der er behov for dette

c. Vurdering af behov for alternativ kryptering af kommunikation imellem slutbrugere og systemerne

d. Vurdering af behov for implementering af effektiv kryptering af data opbevaret i systemerne

e. Kontinuerlig opfølgning på benyttelsen af kryptering på netværket samt ved dataopbevaring

Initiativet forventes at kræve systemtilpasninger, som kan være vanskelig på særligt de ældre systemer.

Initiativ 10. Sikker datahåndtering i legacy-systemer

Legacy-systemer er en kendt problemstilling i mange organisationer, herunder specifikt inden for sektorer, hvor der benyttes højt specialiserede systemer. Det gør sig i høj grad også gældende i politiet, hvor digitaliseringen blev påbegyndt tidligt. Legacy-systemer bygger på udfaset eller forældet teknologi. Det betyder, at der for en række systemer forventes at være alvorlige såvel sikkerhedsmæssige som performancemæssige problemstillinger, der direkte påvirker sikkerheden samt indirekte påvirker datahåndteringen i systemerne. Undersøgelsen har vist, at det også gør sig gældende for politiets forældede systemer.

For at sikre en mere korrekt og sikker datahåndtering i legacy-systemerne, anbefaler PwC, at der igangsættes fire aktiviteter:

a. Kvalificer og prioriter listen over identificerede legacy-systemer

b. Afdæk den tekniske tilstand samt behov for yderligere sikringstiltag og implementer dem

c. Løbende overvågning af om sikkerhedstiltagene er tilstrækkelig

d. Udskiftning af eksisterende legacy-systemer

Legacy-problemstillingen er noget, som politiet har arbejdet med længe og med aftalen for politiets og anklagemyndighedens økonomi for 2021-23 er der sat et ekstra og særskilt fokus på fremadrettet at håndtere de udfordringer, som legacy-systemerne medfører.

Initiativet forudsætter en række systemtilpasninger af ældre, specialiserede og ofte udokumenterede systemer ifm. indarbejdelsen af visse sikkerhedstiltag. Særligt aktivitet 4 omkring udskiftning af de eksisterende legacy-systemer vil medføre betydelige merudgifter og tage lang tid at implementere.

4. Sigtelinjer for datahåndteringen hos anklagemyndigheden

Overblik over tværgående problemstillinger og initiativer

Baseret på PwC's observationer fra såvel spørgeskemaer, systemgennemgang og uddybende interviews har PwC peget på fire tværgående problemstillinger, som skaber udfordringer i forhold til korrekt og sikker datahåndteringen på tværs af anklagemyndigheds systemer.

De fire tværgående problemstillinger, PwC har peget på påvirker både en korrekt og sikker datahåndtering indirekte og direkte. Det er PwC's vurdering, at omfanget og typen af problemstillingerne er mindre end hos lignende organisationer med tilsvarende størrelse og kompleksitet. Det skyldes bl.a., at anklagemyndigheden har implementeret ISO27001 og GDPR samt det arbejde, Rigsadvokaten har foretaget ifm. overgangen til Statens It.

Undersøgelsen viser, at datahåndteringen potentielt kan påvirkes indirekte ved fx, at anklagemyndigheden ikke har dokumenteret governance og processer fuldt. En korrekt datahåndtering kan desuden blive påvirket, hvis der er uklarhed omkring dataklassifikationen. Endvidere kan en sikker datahåndtering blive påvirket direkte af udfordringer omkring logning og kryptering.

Justitsministeriet har en ambition om, at myndighederne inden for Justitsministeriets område skal blive rollemodeller i forhold til at håndtere data korrekt og sikkert. Justitsministeriet forventer, at ambitionen vil tage tid at indfri, da det vil kræve betydelige investeringer samt større organisatoriske og tekniske forandringer.

PwC har udarbejdet fire initiativer, der tilsammen indeholder 12 aktiviteter, som vil kunne imødegå de fire tværgående problemstillinger. Det fire initiativer omfatter:

1. Dokumenteret systemejerskab
2. Effektivisering og forenkling af dataklassifikationen
3. Proaktiv anvendelse af logning
4. Udbredelse af kryptering

Det er PwC's vurdering, at det vil være en ressourcekrævende og stor opgave at implementere alle initiativerne og de tilhørende aktiviteter, hvorfor det naturligt vil strække sig over en årrække, og der vil skulle ske en prioritering af implementeringen af initiativerne hos politiet og anklagemyndigheden. Aktiviteterne under hvert initiativ har en vis kronologisk sammenhæng, men kan i mange tilfælde godt igangsætte parallelt eller enkeltvist samt på enkelt system- eller sagsbehandlingsområde, hvis myndigheden vurderer, det er hensigtsmæssigt.

Initiativ 1. Dokumenteret systemejerskab

Et systemejerskabskoncept definerer, hvem der har ansvaret for et system. Det kan fx være ansvaret for at uddanne og træne brugerne i korrekt datahåndtering og implementere sikkerhedstiltag, så som logning og kryptering, der understøtter en sikker datahåndtering.

Anklagemyndigheden er en mindre organisation. De centrale processer omkring datahåndteringen og systemejerskabet er derfor styret af få personer, som i praksis sikrer, at alle ved, hvad de skal, og at processerne kører effektivt. Undersøgelsen har dog vist, at anklagemyndigheden ikke har en konkret og operationaliseret beskrivelse af, hvilke opgaver og processer, der knytter sig til systemejerskabet. Det medfører en risiko for, at systemejerskabet og de processer, der knytter sig til systemejerskabet, bliver for personafhængige.

For at sikre en klar rolle- og ansvarsfordeling omkring systemejerskabet anbefaler PwC, at der igangsættes følgende aktivitetet:

a. Beskrivelse af rolle og ansvarsfordelingen for systemejerskab

Initiativet vurderes at understøtte, at det bliver lettere at håndtere data korrekt. Initiativet vil kræve, at de allerede implementerede roller og processer dokumenteres og formidles.

Initiativ 2. Effektivisering og forenkling af dataklassifikationen

En tydelig markering af dataklassifikation af fysiske og logiske data reducerer risikoen for enten overbeskyttelse af mindre væsentlige data eller utilstrækkelig beskyttelse af mere væsentlige data.

En væsentlig del af de data anklagemyndigheden behandler kommer fra politiet, og det afstedkommer et implicit krav om, at dataklassifikationen kan bæres over fra én myndighed til den næste for at skabe en sammenhængende dataklassifikation og sikkerhed. Politiet og anklagemyndigheden anvender to forskellige klassifikationsmodeller. PwC kan konstatere, at klassifikationen sker på systemniveau. Dvs. at alle data i et system klassificeres på samme niveau. Herudover er visse af politiets informationer klassificeret efter sikkerhedscirkulæret, men disse har ikke været en del af undersøgelsen og er derfor ikke omfattet af PwC's anbefaling.

For at sikre en bedre dataklassificering, anbefaler PwC, at der med afsæt i en risikobaseret tilgang igangsættes fem aktiviteter:

a. Forenkling af retningslinjerne for dataklassifikation

b. Teknisk understøttelse og kontrol af dataklassifikation

c. Elektronisk påtrykning af dataklassifikation på relevante data

d. Hjælpefunktioner til dataklassifikationer af nye data

e. Proces for op- og nedklassificering af data

Initiativet vurderes at bidrage til, at det bliver nemmere for brugerne at håndtere data korrekt og sikkert, idet det må forventes, at implementering af en teknisk understøttelse, regelforenkling samt automatisk påtrykning af dataklassifikation kan lette den enkelte i det daglige arbejde. Initiativet vurderes at have en høj kompleksitet, da det forudsætter ændring i eksisterende systemer, vejledninger og datamodeller samt implementering af yderligere løsninger.

Initiativ 3. Proaktiv anvendelse af logning

Logning bidrager til at skabe en sporbarhed i benyttelsen af data. Undersøgelsen har vist, at anklagemyndigheden generelt set har implementeret et fornuftigt niveau af logning, dog med enkelte afvigelser, hvis anklagemyndigheden skal blive rollemodel inden for logning.

For at sikre en proaktiv anvendelse af logning, anbefaler PwC, at der igangsættes tre aktiviteter:

a. Fuldt dækkende log-registreringer

b. Central indsamling af log-registreringer

c. Monitorering og proaktiv alarmering

Med fuldt dækkende logregistreringer mener PwC, at logregistreringen skal afspejle de til enhver tid gældende lovgivningskrav og interne regler, samt det af ledelsen godkendte logningsniveau. Initiativet forventes at kræve en systemtilpasning i samarbejde med Statens IT, hvilket der skal tages højde for i implementeringen.

Initiativ 4. Udbredelse af kryptering

Formålet med kryptering er at sikre, at uvedkommende ikke kan få adgang til anklagemyndighedens fortrolige og følsomme data, når de opbevares og deles.

Anklagemyndigheden behandler mange følsomme personoplysninger. Derfor er det vigtigt, at datatransmissionerne altid er beskyttede med effektiv kryptering.

For at sikre bedre beskyttelse af data ved benyttelse af kryptering, anbefaler PwC, at der igangsættes fem aktiviteter:

a. Afdækning af hvilke systemer der effektivt krypterer kommunikation imellem slutbrugere og selve systemet

b. Prioritering og implementering af effektiv kryptering på kritiske systemer, hvor der er behov for dette

c. Vurdering af behov for implementering af effektiv kryptering af data opbevaret i systemerne

. Initiativet forventes at kræve systemtilpasninger, og skal vurderes ift. de driftsmæssige konsekvenser det kan have.

5. Grundlaget for gennemførelsen af undersøgelsen

PwC's metodiske anvendelse i undersøgelsen

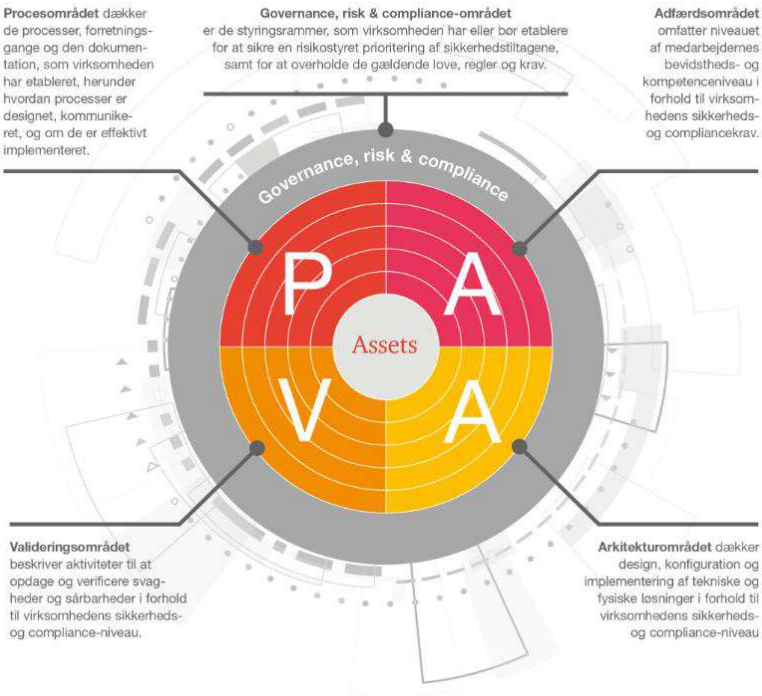
PwC har i undersøgelsen baseret sig på en metode, som har haft til formål at sikre, at undersøgelsen havde karakter af en kulegravning. PwC har indsamlet et stort og bredt datagrundlag fra medarbejderne i politiet og anklagemyndigheden i form af udsendelse af bl.a. mere end 60.000 spørgeskemaer og gennemførsel af ca. 120 uddybende interviews.

Undersøgelsen af medarbejdernes datahåndtering i politi og anklagemyndigheden har været foretaget under krav om fuldstændig anonymitet. Det har medført, at information fra fx spørgeskemaundersøgelsen ikke har kunnet verificeres direkte med opfølgende interviews med respondenter lige som oplyste problemer ikke i alle tilfælde har kunnet nuanceres.

PwC´s PAVA-koncept har dannet grundlag for en struktureret gennemgang af governance, processer, adfærd, validering og arkitektur, *jf. figur 2,* dvs. de områder, som PwC vurderer, der skal undersøges for at forstå og vurdere datahåndteringen hos politiet og anklagemyndigheden.

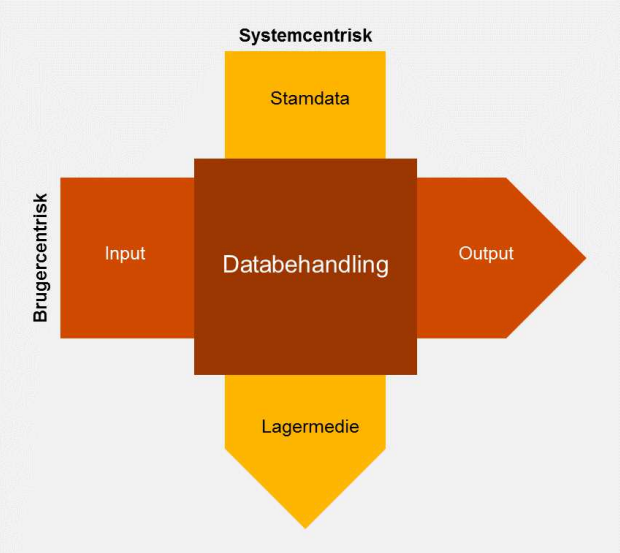
Ved at afdække de fem områder i PAVA, klarlægges dels de styrings- og regelmæssige rammer, dokumentationsgraden, medarbejdernes adfærd samt medarbejdernes egen bevidsthed omkring deres adfærd, dels hvor godt myndighederne anvender beskyttende og opdagende teknologier i form af fx logning og kryptering, i relation til brugernes datahåndtering i it-systemerne samt verificering af de tekniske opsætninger og de interne kontroller.

Figur 2. Præsentation af PwC's PAVA-koncept



PwC's undersøgelse af korrekt og sikker datahåndtering i politiet og anklagemyndigheden har kombineret en system- og brugercentrisk undersøgelsestilgang med fokus på henholdsvis brugernes korrekte datahåndtering og sikkerhed i tilknytning til systemunderstøttelsen, *jf. figur 3*.

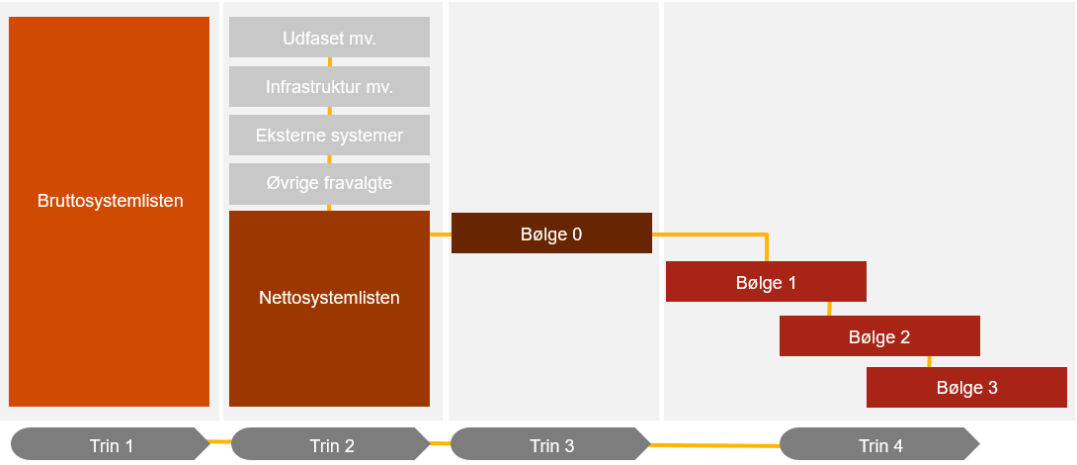
Figur 3. Undersøgelsens forskellige vinkler på korrekt og sikker datahåndtering



PwC's overordnede tilgang til undersøgelsen

Undersøgelsen har taget udgangspunkt i en indledende gennemgang af politiets og anklagemyndighedens samlede it-systemportefølje, som i deres eget samlede systemoverblik bestod af ca. 1.100 kendte it-komponenter. Dvs. applikationer, databaser, hardware mv., som var i drift, udfaset eller afinstalleret. Herudover har der i undersøgelsen været en erkendelse af, at det samlede overblik kunne være ufuldstændigt, hvorfor undersøgelsen også omfattede en afdækning af skygge-it, der er systemer, som ikke er registreret centralt, som kunne blive inkluderet i undersøgelsen på et senere tidspunkt (trin 1), *jf. figur 4.*

Figur 4. Overordnet tilgang til en risikobaseret systemudvælgelse



PwC har efterfølgende, ud fra en vurdering af omfanget af datahåndtering, afgrænset undersøgelsen fra de systemer, hvor det blev vurderet, at der ikke blev foretaget en direkte datahåndtering. Her blev følgende typer af it-komponenter valgt fra i systemlisterne:

1. Udfasede og afinstallerede systemer
2. Infrastruktur, tekniske installationer og hardware (tvivlstilfælde blev beholdt)
3. Eksterne systemer (systemer hvor det var muligt at ændre i væsentlige data blev beholdt)

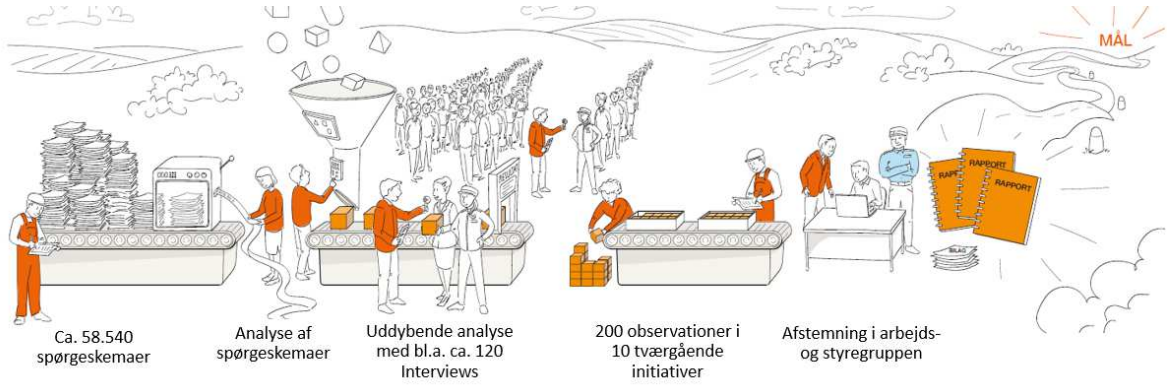
Gennemgangen af politiets og anklagemyndighedens systemoverblik førte til, at der ud af ca. 1.000 kendte it-komponenter blev udvalgt 291 systemer til at indgå i selve datahåndteringsundersøgelsen, hvoraf det inden for undersøgelsens periode var muligt at lade 282 systemer indgå i spørgeskemaundersøgelsen (trin 2).

Systemerne blev inddelt i tre overordnede bølger ud fra forretningskritikalitet, efter at de var blevet vurderet ift. konsekvensparametrene fortrolighed, integritet og tilgængelighed (såkaldt FIT-vurdering). Formålet med denne tilgang har været at sikre, at de mest kritiske systemer som udgangspunkt blev undersøgt først. Herudover blev der udvalgt et udsnit af repræsentative systemer i en såkaldt bølge 0 mhp. at efterprøve og tilpasse de enkelte undersøgelsesmetoder, inden selve undersøgelsen af de mest forretningskritiske systemer gik i gang.

Undersøgelsesaktiviteter i de enkelte bølger

I hver bølge blev systemerne efterfølgende analyseret via tre faser, *jf. figur 5*.

Figur 5. Undersøgelsens faser



I undersøgelsen er der samlet set udsendt ca. 60.000 spørgeskemaer til ansatte, som har registreret brugeradgang til de undersøgte systemer. Der er tilstræbt indhentning af spørgeskemabesvarelser for et repræsentativt udsnit af brugere for hvert system. Der er herudover udsendt ca. 500 spørgeskemaer til systemejere. Spørgeskemaerne er blevet brugt dels til at lave en mere konkret risikoscoring og kritikalitetsvurdering af systemerne og dels til at pege på, hvor der kunne være indikationer på udfordringer ift. en korrekt og sikker datahåndtering. Med udgangspunkt i bl.a. systemernes risikoscore og systemtype, blev 12 systemer hos politiet og tre systemer hos anklagemyndigheden udvalgt til en uddybende analyse fordelt på de tre bølger.

Hver uddybende analyse indeholdt en verifikation af informationen fra spørgeskemaerne, en dokumentgennemgang, interview med centrale funktioner, systemejerne og udvalgte brugere samt en konfigurationsgennemgang af systemerne. De systemspecifikke analyser har givet en mere nuanceret forståelse af udfordringerne omkring korrekt og sikker datahåndtering.

Afslutningsvis har PwC gennemført en procesafdækning af datas rejse og behandling fra "vugge-til-grav" i en straffesagskæde på tværs af flere systemer, processer og brugere, for at forstå udfordringerne med

datahåndteringen og identificere, hvordan det kan gøres nemmere for medarbejderne at håndtere data korrekt og sikkert.

Analyse af datas bevægelse og placering i politiets systemer samt afdækning af skygge-it

For at validere og kvalitetssikre observationerne fra de spørgeskemabaserede analyser og de uddybende analyser samt for at afdække potentiel skygge-it er der gennemført en dataflowanalyse af, hvor politiets medarbejdere lagrer deres data, og af hvor længe data lagres (fx CPR-numre på fælles drev), samt hvor politiets medarbejdere flytter data hen (fx ukendte systemer, USB-nøgler mv.). Dataflowanalysen har bidraget til at afdække den faktiske praksis blandt medarbejderne i relation til arkivering og sletning af data og dermed, hvor der potentielt kan opstå brud på korrekt og sikker datahåndtering. Endvidere har dataflowanalysen bidraget til at vurdere, om der er uregistrerede systemer i politiet, som ikke fremgår af de systemlister, som findes i Rigspolitiet (skygge-it).

Dataflowanalysen blev gennemført ved brug af et dataanalyseværktøj (Data Loss Prevention – DLP), som PwC har fået stillet til rådighed af politiet. Særligt afdækningen af skygge-it blev suppleret med yderligere analyseværktøjer stillet til rådighed af politiet, som blev anvendt til at analysere datatrafikken på politiets forskellige netværk, for at se, om data blev overført til it-komponenter, som på undersøgelsestidspunktet var ukendte for politiet.

DLP-værktøjet var på analysetidspunktet ikke fuldt implementeret, hvorfor PwC ikke har kunne drage fuld nytte af værktøjet på alle systemer. Et tilsvarende værktøj har ikke været tilgængelig hos anklagemyndigheden, hvorfor PwC i stedet lavede stikprøver i fællesmapper.

Særlige forhold omkring undersøgelsen

Undersøgelsen har skullet sikre anonymitet for de medarbejdere, som har medvirket i spørgeskemaundersøgelsen og dataflowanalysen, da det ikke har været et formål med undersøgelsen at undersøge konkrete medarbejderes datahåndtering.

Derfor har udvælgelsen af interviewpersoner i forbindelse med de uddybende analyser været begrænset til udvalgte nøglepersoner i myndighederne. Der blev i sidste periode af undersøgelsen åbnet op for, at medarbejdere frivilligt kunne bidrage med forhold, som de mente kunne gøre det nemmere at foretage korrekt og sikker datahåndtering, ved at de kunne kontakte PwC direkte og stadig være anonyme. PwC fik i den forbindelse kontakt med et mindre antal personer fra såvel den operative som den administrative, sagsbehandlingsmæssige og den operative del af kredsenes personale.

Det er PwC's vurdering, at PwC har fået den information, som har været nødvendig for at udføre en fyldestgørende undersøgelse ift. den fastlagte metode og rammerne for undersøgelsen.