

**Deloitte.**



## **Undersøgelse af Rigspolitiets håndtering af historiske teledata**

1. oktober 2019

# Indhold

1	Sammenfatning	4
2	Baggrund og formål for undersøgelsen	9
3	Introduktion til historiske teledata	11
4	Undersøgelsens metode	21
5	Sammenligning af rådata og konverterede data	32
6	Potentielle fejlkilder og usikkerheder ved anvendelse af historiske teledata	60
7	Gennemgang af Rigspolitiets systemer til opbevaring og behandling af historiske teledata	69
8	Undersøgelse af kvalitetskontrol af historiske teleoplysninger	74
9	Bilag: Introduktion til historiske teledata og teleinfrastruktur	81



# 1 Sammenfatning

## Undersøgelse af Rigspolitiets håndtering af historiske teledata

Rigspolitiet har igangsat en uvildig ekstern undersøgelse af politiets brug og behandling af historiske teledata i straffesager, der er gennemført af Deloitte i et komprimeret forløb fra ultimo august frem til 1. oktober 2019.

Undersøgelsen har belyst den samlede teledataværdikæde med et primært fokus på Rigspolitiets håndtering af historiske teleoplysninger. Undersøgelsen har belyst Rigspolitiets Telecenters konvertering af rådata modtaget fra teleudbyderne, de it-systemer, der anvendes til opbevaring og behandling af historiske teledata, samt kvalitetskontrol i forbindelse med håndteringen af historiske teledata. Hertil er der foretaget en afdækning af potentielle fejkilder og usikkerheder ved anvendelsen af historiske teledata i straffesager.

Samlet set vurderes de identificerede problemer vedrørende håndteringen af historiske teledata blandt andet fremadrettet at kunne adresseres ved (i) at adressere en række fundamentale IT-mæssige forhold vedrørende håndtering og opbevaring af historiske teledata på kort sigt og på længere sigt at gennemføre IT-investeringer, der også håndterer den tekniske gæld; (ii) at styrke samarbejdet mellem Rigspolitiet og teleudbyderne vedrørende historiske teledata, herunder både på strategisk og operationelt niveau; (iii) at tilsi­k­re at alle straffesagens aktører er bekendt med de potentielle fejkilder og usikkerheder, der er ved anvendelsen af historiske teledata som bevismiddel.

Resultaterne af undersøgelsens fire delanalyser sammenfattes kort i det nedenstående.

### 1.1 Sammenligning af rådata og konverterede data

Der er gennemført en sammenligning af rådata modtaget fra teleudbyderne med det konverterede data, som er udsendt af Rigspolitiets Telecenter til politikredse mv. Undersøgelsen dækker historiske teledata fra perioden 3. januar 2011 til 27. august 2019. Den gennemførte analyse adresserer konverteringsfejl både på række- og feltniveau. Undersøgelsen identificerer for perioden 2011-2019 en række konverteringsfejl mellem rådata og konverteret data.

Undersøgelsens datagrundlag udgøres af 24.028 rekvisitioner af historiske teledata, hvor der er identificeret både rådata og konverteret data. Dette udgør knap 58 pct. af de tilgængelige rekvisitioner for rådata i undersøgelsens periode. Heraf er der 19.386 rekvisitioner, hvor der er identificeret både en rådatafil og en konverteret datafil med indhold, svarende til 46 pct. af de tilgængelige rekvisitioner for rådata. Disse rekvisitioner stammer fra 5.551 journalnumre (sager).

Analysen af Rigspolitiets konvertering af historiske teledata på rækkeniveau viser samlet set, at der har været uoverensstemmelser i antal rækker

mellem konverterede data og rådata i ca. 6,9 pct. at de undersøgte rekvisitioner. Heraf er der rækketab (dvs. færre rækker i konverterede data end i rådatafilen) i 1.131 rekvisitioner i undersøgelsesperioden svarende til ca. 5,8 pct. af rekvisitionerne. Det svarer til 4,5 mio. tabte rækker. Undersøgelsen viser, at rækketabet overvejende er koncentreret i 2016, hvor der er identificeret 361 rekvisitioner med rækketab. Omfanget af rækketab er ligeledes belyst. Der er identificeret 142 rekvisitioner med en divergens på én række, 260 rekvisitioner, der mangler 2-10 rækker, 275 rekvisitioner, der mangler 11-100 rækker og 453 rekvisitioner, der mangler mere end 100 rækker i forhold til konverteret data. Omfanget af rækketab skal ses i lyset af antallet af rækker i en rekvisition, hvor det gennemsnitlige antal rækker til sammenligning er ca. 3.900 rækker, mens medianen er ca. 400 rækker. Deloitte identificerer samlet set et mindre procentuelt rækketab end det, Rigspolitiet har identificeret i sin interne screening af 2018.

Undersøgelsen omfatter ligeledes en analyse af ca. 48,7 millioner rækker i forhold til konverteringsfejl, der påvirker *indholdet* af de enkelte felter i den enkelte række. Samlet set identificerer undersøgelsen en række forskelligartede konverteringsfejl på feltniveau i perioden 2011-2019, som optræder i varierende omfang. Der er identificeret et begrænset antal konverteringsfejl vedrørende f.eks. opkaldende nummer, modtagende nummer og konvertering af mastekoordinater, mens der f.eks. er identificeret et højere antal uoverensstemmelser for bl.a. tjenestetype. Undersøgelsen identificerer i al væsentlighed resultater, der svarer til de fund, som Rigspolitiet har identificeret i interne undersøgelser og en stikprøvekontrol.

Betydningen af en konverteringsfejl varierer afhængig af feltets indhold og fejls karakter. En meget betydelig andel af de identificerede konverteringsfejl vurderes uden praktisk betydning, mens andre kan have betydning afhængigt af situationen. Deloitte har ikke nærmere belyst betydningen af de identificerede konverteringsfejl i et strafferetligt perspektiv. Undersøgelsens fund – herunder koblingen af specifikke konverteringsfejl til rekvisitionsnumre og journalnumre (dvs. sager) – stilles til rådighed for politiet og anklagemyndigheden.

Endelig viser en analyse af konvertering af mastekoordinater, at der i perioden 2011-2019 er sket forskydninger af mastekoordinater i forbindelse med Telecenterets konvertering af mastepositioner. Den langt overvejende del af disse forskydninger udgøres af konverteringsfejl, der resulterer i forskydninger af mastekoordinater på hhv. ca. 100 og ca. 220 meter.

## **1.2 Potentielle fejlkilder og usikkerheder ved anvendelsen af historiske teledata**

Der er foretaget en afdækning af potentielle fejlkilder og usikkerheder ved anvendelsen af historiske teledata. Undersøgelsen er baseret på en afdækning af forhold på tværs af hele teledataværdikæden, idet der dog fokuseres på Rigspolitiets håndtering af historiske teledata. Der er i forbindelse med undersøgelsen inddraget ekspertbistand fra teledataeksperter, strafferetseksperter og en forsvarsadvokat, ligesom der bl.a. er gennemført interviews med teleudbydere og Teleindustrien.

Ved anvendelse af historiske teledata i straffesager er det grundlæggende centralt at forstå, at der er tale om data, som teleudbydere indsamler i forretningsøjemed, bl.a. med henblik på taksering af ydelser og fakturering

af kunder samt optimering af netværket. Generelt er gældende, at telekommunikationens rejse mellem mobilenhed og antenne, som er placeret på en given mast, påvirkes af tekniske forhold, herunder justering af antennen, højden på antennens placering og den anvendte transmissionsteknologi, samt en række eksterne forhold, bl.a. vejrlig, landskab, vegetation, bygningsmasse mv. Endvidere er data forbundet med en række usikkerheder og fejlkilder givet forhold hos teleudbydere, herunder både af teknisk og processuel karakter.

Konverteringen af historiske teledata hos Rigspolitiets Telecenter har ligeledes medført en række fejlkilder af varierende karakter, jf. ovenstående afsnit. Nogle fejlkilder vil have medført manglende data i konverteret data, hvoraf nogle mangler vil være åbenlyse og andre ikke mulige at identificere med mindre der sammenlignes direkte med rådata. Hertil er der identificeret en række eksempler på fejlkonverterede data, som afhængig af det konkrete feltindhold kan have haft betydning eller ej.

Endelig er der en række usikkerheder forbundet med arbejdsgange og kompetencer vedrørende håndtering af historiske teledata i politikredse mv.

På baggrund af undersøgelsen har Deloitte udarbejdet et uvildigt notat om anvendelsen af historiske teledata, der redegør for de særlige opmærksomhedspunkter, man bør være opmærksom på, når historiske teledata anvendes til efterforskning og som strafferetligt bevis. Notatet henvender sig til politi, anklagere, dommere og forsvarere og vil fremadrettet blive fremlagt af anklagemyndigheden i straffesager, således at det sikres, at alle straffesagens aktører er bekendt med de potentielle fejlkilder og usikkerheder, der er ved anvendelsen af historiske teledata som bevismiddel.

### **1.3 Gennemgang af Rigspolitiets systemer til opbevaring og behandling af historiske teledata**

Der er foretaget en gennemgang af Rigspolitiets systemer til opbevaring og behandling af historiske teledata med henblik på at vurdere funktionalitet, teknisk integritet og driftsstabilitet for de it-systemer, der anvendes til opbevaring og behandling af historiske teleoplysninger, samt processer og dokumentation for it-kontroller. Gennemgangen har taget udgangspunkt i ISO 27001:2013 (Information Security Management) samt ITIL (Information Technology Infrastructure Library) rammeværktøjerne for sikker drift. Der er på baggrund af gennemgangen udarbejdet anbefalinger på kort og lang sigt.

Systemerne og den tilhørende infrastruktur kan kort beskrives som utidssvarende og kompleks og omfatter en række forskellige systemer, integrationer mellem systemer og dataoverførslers. IT-miljøet har løbende været udviklet i takt med at nye dataformater, behov mv. er opstået. Udviklingen kan bedst beskrives som 'knopskydning'.

Undersøgelsen viser, at den samlede systemplatform, herunder procedurer for udvikling og drift, er på et helt utilstrækkeligt niveau.

Kortsigtede anbefalinger bør af hensyn til karakteren af de observerede risici og hvad der teknisk og processuelt er muligt, gennemføres hurtigst muligt. Det er anbefalinger, der vil kunne adressere helt fundamentale IT-mæssige forhold og derved i noget omfang kunne adressere systemrisikoen og operationelle fejl. De kortsigtede anbefalinger omfatter blandt andet

forbedringer i visse processer samt IT-mæssige forhold, der i noget omfang vil kunne reducere risikoen for fejl i selve konverteringsprocessen.

Infrastrukturen til håndtering af historiske teledata har over tid oparbejdet en meget stor teknisk gæld. Der er således betydelige risici forbundet med den fremadrettede driftsstabilitet, det vil sige sikkerheden for, at der fortsat kan leveres konverteret teledata. Gennemførelse af de kortsigtede anbefalinger kombineret med selv betydelige investeringer i den nuværende infrastruktur, vil ikke kunne fjerne den tekniske gæld, endsiige reducere den væsentligt. Derfor er der samlet set behov for, at der implementeres en ny og mere tidsvarende infrastruktur. Foruden infrastrukturen bør selve arkitekturen nytænkes med henblik på at sikre, at den nuværende kompleksitet ikke videreføres i en ny infrastruktur. Det indebærer en betydelig investering samt et ikke uvæsentligt ressourcetræk.

#### **1.4 Undersøgelse af kvalitetskontrol af teleoplysninger der modtages, opbevares og behandles**

Der er foretaget en undersøgelse af kvalitetskontrol med henblik på at beskrive Rigspolitiets behandling og konvertering af historiske teledata på tværs af teledataværdikæden, ud fra et retssikkerhedsmæssigt hensyn. På baggrund af gennemgangen af kvalitetskontrol i Telecenterets håndtering af historiske teledata er der identificeret risici, som medfører en moderat til høj risiko for usikkerheder og fejl. Disse risici er tilstede på tværs af den samlede dataværdikæde fra mast til retssag, herunder iboende usikkerheder givet historiske teledatas beskaffenhed samt manuelle og systemmæssige processer og procedurer i forbindelse med rekvisitioner af historiske teledata. Der er udarbejdet løsningsforslag til kvalitetskontroller, som forventes at kunne imødegå de identificerede risici.

Det anbefales overordnet, at der implementeres et samlet rammeværk for identifikation af risici, design og implementering af kvalitetskontroller. Som basis for dette rammeværk anbefales det at anvende kvalitetsstandarden ISO 27001 om informationssikkerhed. Standarden benyttes allerede som en del af Rigspolitiets rammeværk for IT-sikkerhed, da Rigspolitiet ligesom andre statslige myndigheder er pålagt at følge denne standard.

Overgang til en ny infrastruktur i Rigspolitiets Telecenter, jf. 1.3, vil på sigt adressere mange af de identificerede risici, herunder usikkerheder i forbindelse med håndtering af historiske teledata i politikredsene mv. blive væsentligt reduceret ved aflevering og bearbejdning af historiske teledata i den infrastruktur, som politiet også anvender til andre formål. Som følge af observationer og anbefalinger omkring Rigspolitiets Telecenters infrastruktur anbefales ikke, at der udvikles og implementeres ny systemudvikling i nuværende systemer og infrastruktur, udover hvad der skal til for at sikre den fremadrettede driftsstabilitet i en periode frem til en fremtidssikret løsning vil kunne være anskaffet og implementeret. Implementering af en infrastruktur vil være et større udviklings- og implementeringsprojekt.

Det anbefales derfor på kort sigt, at der hurtigst muligt etableres en uvildig kvalitetskontrol i form af 3. parts validering af alle konverterede historiske teledata. Der vil herigennem blive etableret en sideløbende og uvildig kvalitetskontrol af konverteringen af historiske teledata. Kvalitetskontrollen skal systemmæssigt understøtte en paralleliseret proces, som kan validere data uafhængigt af Rigspolitiets Telecenters egen konverteringsproces. Af

hensyn til at etablere den fornødne uvildighed, anbefales det, at lade en ekstern leverandør varetage valideringsopgaven.

Endelig anbefales det, at samarbejdet mellem teleudbyderne og Rigspolitiet bør styrkes. Det er vurderingen, at et styrket samarbejde i væsentlig grad vil være til gavn for begge parter og styrke den generelle tillid til anvendelse af historiske teledata i straffesager. Et fremadrettet samarbejde bør både angå et strategisk niveau, men også på et mere dagligdags operationelt niveau.



# 2 Baggrund og formål for undersøgelsen

## 2.1 Baggrund for analysen

Rigspolitiet har jf. Rigsadvokatens brev af 13. juni 2019, konstateret en systemfejl i det it-program, der anvendes af politiet til at konvertere såkaldte rådata fra teleudbyderne i forbindelse med indhentning af historiske teleoplysninger i straffesager. Fejlen i IT-systemet er rettet den 8. marts 2019. I forlængelse heraf har Rigspolitiet igangsat en gennemgang af alle straffesager, hvori der er indhentet historiske teleoplysninger, i perioden 2012 til 2019.

Rigspolitiet har i forbindelse med gennemgangen af konkrete straffesager, der kan være berørt af fejlen, også identificeret fejl i forbindelse med konverteringen af geografiske koordinater for telemasters placering, jf. orientering til Retsudvalget af 18. august 2019. Der er ligeledes konstateret flere forskellige fejl i den rådata, som politiet modtager fra teleudbyderne. Rigspolitiet har i forlængelse af disse fund og med henblik på hurtigst muligt at afklare den usikkerhed, der er opstået om anvendelse af historiske teledata i straffesager, igangsat en uvildig ekstern undersøgelse af politiets brug og behandling af historiske teledata i straffesager.

Deloitte har på den baggrund gennemført en uvildig ekstern undersøgelse af politiets anvendelse og håndtering af historiske teledata i straffesager.

## 2.2 Undersøgelsens formål og rammer

Undersøgelsens genstandsfelt udgøres af fire opgaveområder:

- i. En uafhængig validering af Rigspolitiets Telecenters databehandling og -konvertering af historiske teledata fra modtagelse af rådata fra teleudbyderne til levering af konverteret data til politikredsene mv.
- ii. Et notat vedrørende mulige fejlkilder og usikkerheder ved historiske teledata, som politi og anklagemyndighed, forsvarere og domstole altid bør være opmærksomme på ved anvendelse af historiske teledata i straffesager
- iii. En uafhængig gennemgang af Rigspolitiets it-systemer, der benyttes til opbevaring og behandling af historiske teledata. Gennemgangen skal munde ud i anbefalinger til, hvordan Rigspolitiets systemer til opbevaring og behandling af historiske teledata kan styrkes
- iv. En uafhængig gennemgang af den nuværende kvalitetskontrol, der udføres af historiske teledata, der modtages, opbevares og behandles i Rigspolitiets Telecenter fra de modtages fra teleudbyderne, til de afleveres til politikredsene mv. Gennemgangen skal munde ud i anbefalinger til, hvordan kvalitetskontrollen kan styrkes fremadrettet

Undersøgelsen skal endvidere afrapportere eventuelle øvrige fejl mv. i håndteringen af historiske teledata, som måtte være identificeret i forløbet, der er skitseret ovenfor.

Undersøgelsen er gennemført i et komprimeret forløb fra ultimo august frem til 1. oktober 2019.

# 3 Introduktion til historiske teledata

## 3.1 Formål og lovgrundlag for anvendelse af historiske teledata i straffesager

Teleoplysninger er oplysninger om kommunikation, som teleudbydere er i besiddelse af, og som politiet til brug for efterforskningen af strafbare forhold kan indhente hos teleudbydere. Efter retsplejelovens § 786, stk. 4, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring i 1 år af teleoplysninger til brug for efterforskning og retsforfølgning af strafbare forhold.

Indhentelse af teleoplysninger er et straffeprocessuelt tvangsindgreb, der er omfattet af retsplejelovens kapitel 71 om indgreb i meddeleleshemmeligheden og i et vist omfang retsplejelovens kapitel 74 om edition. Det fremgår af retsplejelovens bestemmelser, at udlevering af teleoplysninger til politiet sker på baggrund af rettens kendelse eller på øjemedet efterfulgt af rettens kendelse, hvis det af efterforskningsmæssige grunde har været nødvendigt at iværksætte indgrebet straks.

Indhentelse af teleoplysninger kan opdeles i tre kategorier. Den ene kategori er i lovgivningen kaldet 'teleoplysning' og indhentes af politiet med hjemmel i retsplejelovens § 780, stk. 1, nr. 3. Denne type af teleoplysning vedrører hvilke telefoner og mobile kommunikationsenheder der i et givent tidsrum har været sat eller kan sættes i forbindelse med en bestemt telefon eller tilsvarende kommunikationsenhed.

Den næste kategori betegnes 'udvidet teleoplysning' og teledata indhentes med hjemmel i retsplejelovens § 780, stk. 1, nr. 4. De oplysninger, der er omfattet af dette indgreb, er data om, hvilke telefoner eller andre tilsvarende kommunikationsenheder der inden for et angivet geografisk område har været sat eller kan sættes i forbindelse med telefoner eller andre tilsvarende enheder. Indgrebet bliver også benævnt 'mastesug'. De data, som politiet modtager, er indeholder oplysninger om, hvilke mobilenheder der inden for et bestemt tidsrum og en given geografi har benyttet én eller flere identificerede telemaster til kommunikation.

Den sidste kategori af teleoplysninger er historiske masteoplysninger, der indhentes med hjemmel i retsplejelovens regler om edition, § 804, stk. 1. Disse data vedrører én given enhed og viser, hvilke telemaster telefonen har været registreret på inden for en afgrænset periode. Historiske masteoplysninger indeholder ikke oplysninger om, hvilke andre enheder mv. der kan have været sat i forbindelse med den telefon indgrebet vedrører.

Historiske teledata i form af teleoplysninger, udvidede teleoplysninger og historiske masteoplysninger kan grundlæggende anvendes på to forskellige måder i forbindelse med straffesager; dels til at sætte retning for politiets efterforskning, dels som et led i anklagemyndighedens bevisførelse i forbindelse med straffesagers behandling i retten.

### 3.2 Logning af historiske teledata

Teleudbydere er med hjemmel i retsplejelovens bestemmelser forpligtet til at registrere og opbevare oplysninger om teletrafik (bekendtgørelse nr. 988 af 28. september 2006, ændret ved bekendtgørelse nr. 660 af 19. juni 2014). Hovedkravet for at være omfattet af logningsforpligtelsen er, at der udbydes elektroniske kommunikationsnet eller -tjenester på kommercielt grundlag til slutbrugere. I praksis er der på nuværende tidspunkt fire teleudbydere, der leverer teleoplysninger til Rigspolitiets Telecenter. Det drejer sig om TDC, Telenor, Hi3G og Telia. De øvrige teleudbydere lejer sig ind på disse fire udbyderes net, og leverancer fra en af de øvrige teleudbydere vil derfor komme fra en af de fire.

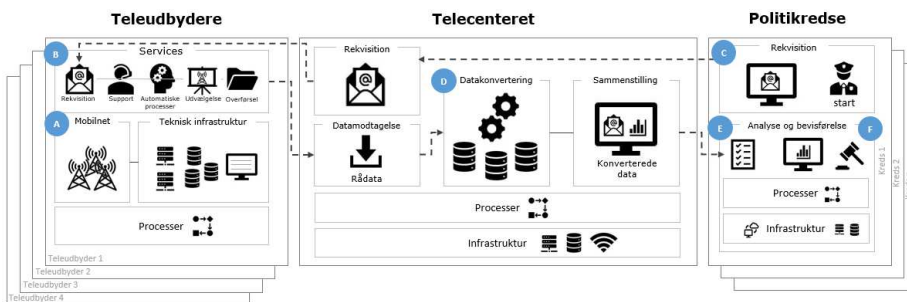
Logningsbekendtgørelsen forpligter teleudbyderne til at registrere (logge) oplysninger, der genereres eller behandles i udbyderens net. Oplysninger om teletrafik, der f.eks. af tekniske grunde ikke genereres eller behandles i udbyderens net, skal derfor ikke logges. De specifikke typer af oplysninger, som udbyderne har pligt til at logge, reguleres i bekendtgørelsens §§ 4-6. Fælles for bestemmelserne er, at der er tale om trafikoplysninger. Udbyderne skal derfor ikke registrere og opbevare selve *indholdet* af kommunikation, hverken i forbindelse med telefonsamtaler mv., brug af internettet eller brug af udbyderens e-mailtjenester. Se bilagsmateriale for yderligere detaljer om logningspligtige data.

Teleudbydernes leverancer til politiet er omfattet af ydelsesaftaler, der er indgået mellem Rigspolitiet og teleudbyderne. Aftalerne indebærer, at politiet kan anvende en række abonnementsydelse til fast pris (dvs. 'flat-rate'-aftaler), mens enkelte ydelser fortsat afregnes omkostningsbaseret med afsæt i medgået tid. Afregningen af abonnementsydelser til en fast pris udgør en ændring fra tidligere, hvor teleudbyderne blev betalt for de enkelte leverancer. Ydelsesaftalerne indeholder et katalog over de ydelser, som politikredse mv. kan rekvirere hos udbyderne. Aftalerne indebærer ikke en nærmere specifikation af de dataformater, som historiske teledata skal leveres til politiet i, ligesom der ikke i ydelsesaftalerne er stillet krav til datakvalitet eller øvrige datakontroller. Aftalerne genforhandles hvert andet år og er i de store linjer ens på tværs af teleudbydere, idet der dog kan iagttages visse forskelle i bestemmelser og forpligtelser på tværs af udbyderne.

### 3.3 Teledatas værdikæde og typer af teleaktivitet

En dataværdikæde angiver og visualiserer den overordnede proces fra skabelsen af data, til behandling af data og til den videre anvendelse og brug af data. Teledataværdikæden er således en betegnelse for den samlede proces fra generering, sammenstilling, rekvirering, konvertering og anvendelse af historiske teledata i forbindelse med straffesagsbehandlingen i en politikreds, et efterforskningsfællesskab eller en anden kompetent myndighed (herefter politikreds mv.). Teledataværdikæden involverer en række organisationer, herunder teleudbydere, Rigspolitiet, politikredse mv., anklagemyndighed og domstole. Undersøgelsen har primært fokuseret på Rigspolitiets Telecenters konvertering af historiske data og mindre på teleudbydernes processer for generering og sammenstilling af rådata. Givet undersøgelsens genstandsfelt omfatter undersøgelsen ikke teleudbydernes anvendelse af historiske teledata i forretningsøjemed. Der har tillige været mindre fokus på de dele af teledataværdikæden, der ligger hos politikredse mv. og anklagemyndighed.

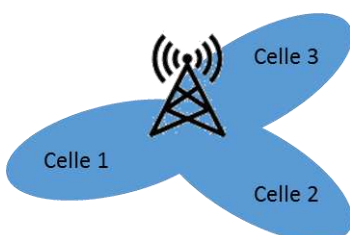
Af nedenstående illustration fremgår den overordnede teledataværdikæde. Illustrationen viser overordnet, at mobile enheder kommunikerer med mobilnettet, hvilket registreres på master (A). Denne information konsolideres ved teleselskaberne og kan rekvireres af politikredse mv. i forbindelse med straffesager (B). Rekvisitioner vedrørende historiske teledata afsendes fra politikredse mv. i forbindelse med efterforskning af straffbare forhold mv. (C). Disse rekvisitioner afsendes via Rigspolitiets Telecenter til teleudbydere, der sender data retur til Rigspolitiets Telecenter i deres respektive formater. Herefter konverteres data hos Rigspolitiets Telecenter til et ensartet format før det sendes til politikredse mv. sammen med rådata (D). I politikredse mv. anvendes historiske teledata til efterforskning og analyse (E), ligesom anklagemyndigheden kan fremlægge historiske teledata som del af sagens beviser ved hovedforhandlingen i straffesager (F). I enkelte tilfælde er det afdækket, at politikredse mv. rekvirerer og modtager supplerende data fra teleselskaberne via Rigspolitiets Telecenter. Det er sker dog kun i sjældne tilfælde. De enkelte elementer i værdikæden er beskrevet mere uddybende herunder.



### 3.3.1 Mobile enheders kommunikation på mobilnettet (A)

Teledataværdikæden starter med en enheds kommunikation med teleudbydernes telenet og infrastruktur i form af master, antenner og udstyr til opsamling og lagring af historiske teledata. Enheder kan være mobiltelefoner, tablets eller andet kommunikationsudstyr, som kommunikerer over telenettet.

En enheds kommunikation sker gennem en specifik celle, som er identificeret ved et celle-id. En celle er en betegnelse for det areal, som dækkes af en antenne, jf. nedenstående figur. Antenner er monteret på telemaster, der er placeret i landskabet (en adresse og et koordinat) med henblik at sikre mobildækning til teleselskabernes kunder. På hver telemast kan der sidde en eller flere antenner. En mast har typisk tre celler, som hver især dækker ca. 120 grader rundt om sendemasten. Der findes ligeledes omni-direktionelle antenner, der dækker 360 grader rundt om telemasten.



Der skal mange master til at dække Danmark. En celle har to egenskaber, der begge er med til at afgøre det præcise antal: dækning og kapacitet. Cellernes størrelse og dækning afgøres af en række faktorer, eksempelvis:

- Mastens højde
- Antennens sendeeffekt
- Antennens sendefrekvens
- Antennens konfigurering ('downtilt', 'Azimuth')
- Vegetation
- Bebyggelse
- Landskabets topografi

Ovenstående er ikke udtømmende faktorer, blot en angivelse af eksempler med indvirkning på cellers dækning. Cellestørrelser ændres således dynamisk baseret på forhold som trafikbelastning, ændringer i netværket og sæsonvariationer.

Frekvenser er inddelt i bånd, der definerer hvilken frekvens, der anvendes. Eksempelvis vil en telefon, der fungerer på 900 MHz båndet, sende og modtage på frekvenser der er ca. 900 Mhz. Den præcise frekvens afgøres af teleudbyderens (operatørens) licens. Bånd i de lavere frekvenser giver som udgangspunkt bedre dækning, men der kan være forskel på kapaciteten, eller bredden af frekvensbåndet, og derfor benyttes de højere frekvensbånd også.

Alle celler i en operatørs mobilnet anvender normalt den samme frekvens, da det giver den bedste udnyttelse af det spektrum en operatør har til rådighed. En undtagelse er 2G (GSM) mobilnet, hvor naboceller altid anvender forskellige frekvenser.

Mobilnettet i Danmark består af forskellige teknologier til anvendelse af mobilkommunikation (2G, 3G, 4G/LTE), og på sigt udvides mobilnettet også med 5G-teknologi. De mobile enheder anvender alle teknologierne og til bestemte formål. Den anvendte teknologi har betydning for, hvordan teleudbyderne registrerer og logger disse data.

En mobilenheds kommunikation består af forskellige typer kommunikationsaktiviteter på mobilnettet. For at kunne kommunikere på teleudbydernes mobilnet, skal en enhed have et aktivt og registreret simkort og være oprettet i en teleudbyders database med abonnenter i nettet (Home Subscriber Server (HSS)). Når en mobil enhed kommunikerer på mobilnettet, registreres aktivitet på teleudbydernes telemaster og tilhørende infrastruktur. En kommunikation mellem en mobil enhed og en celle på en telemast genererer en såkaldt CDR (Call Detail Record), der registrerer den anvendte celles id decentralt. Denne registrering indeholder tekniske oplysninger om kommunikationen og afhænger af kommunikationsaktiviteten. CDR er således de genererede historiske teledata fra mobil enhed til registrering på telemasterne, og således basis for den videre konsolidering og behandling hos teleudbyderne.

### **3.3.2 Registrering og konsolidering af historiske teledata ved teleudbyderne (B)**

Teleudbydernes registrering af telekommunikation sker først på den enkelte mast. Registreringen af CDR konsolideres og behandles herefter hos teleudbyderne, bl.a. med henblik på at kunne balancere trafikken på den enkelte mast og foretage den korrekte taksering af de aktiviteter, som den mobile enhed anvender (B). Konsolideringen af historiske teledata hos den

enkelte udbydere er forbundet med en betydelig kompleksitet, idet data trækkes fra et stort antal platforme og systemer, som er leveret af et stort antal underleverandører. Alle platforme og systemer konfigureres med et stort antal parametre, og forskellige konfigurationer vil medføre forskelle i rapportering, som der skal tages højde for i konsolideringen. Selve konsolideringen og den efterfølgende lagring af historiske teledata i databaser varierer ligeledes i et vist omfang mellem teleudbydere, herunder i forhold til om de logningspligtige data opbevares i særskilt database eller ej.

Formatet for det konsoliderede data varierer også i et vist omfang mellem teleudbydere. Det skal ses i lyset af, at logningsbekendtgørelsen angiver hvad der skal logges, men ikke specificerer formatet herfor nærmere. Der er således variation i bl.a. datastruktur og navngivning af data teleudbydere imellem. Undersøgelsen har identificeret 100 forskellige formater af rådata, der er afleveret fra teleudbydere i perioden 3. januar 2011 og frem til 27. august 2019 på trækningstidspunktet. De 100 forskellige formater er repræsenteret i to helt forskellige filtyper. De 100 formater afspejler en stor spredning i antallet af rekvisitioner. Tredive procent af formaterne repræsenterer cirka 99,9 pct. af alle rådata. Heraf repræsenterer tre af de 100 formater i alt 78 pct. af alle rådata. Dette er beskrevet i den detaljerede analyse i kapitel 5.

Rådata afleveres i et format, hvor kolonnenavne angiver dataindholdet i de underliggende rækker. Det svarer til, at øverste række i et regneark er en kolonneoverskrift for alle nedenstående rækker i kolonnen. Denne struktur er vist nedenfor, hvor der er illustreret to forskellige formater med forskelligt indhold, der er direkte sammenlignelige for de menneskelige øje, men som af et IT-system ikke er umiddelbart sammenlignelige.

**Eksempel 1**

Navn	Beskæftigelse
Jens Jensen	Erhvervsdrivende
Hans Hansen	Gårdejer
Frederikke Frederiksen	-

← **Datatype (format 1)**  
 ← Datapost med to felter  
 ← Datapost med to felter  
 ← Datapost med manglende værdi

**Eksempel 2**

Kunde	Job
Jens Jensen	Erhvervsdrivende
Hans Hansen	Gårdejer
Frederikke Frederiksen	◆gproducent

← **Datatype (format 2)**  
 ← Datapost med to felter  
 ← Datapost med to felter  
 ← Datapost med to felter og datafejl

De 100 formater repræsenterer variationen over tid i takt med at dataudtrækkene hos teleudbydere har ændret sig, samt forskelle mellem teleudbydere, hvis IT-systemer, processer og udtræk er forskellige. Variationerne i formater afspejler således den kompleksitet i rådata, som Rigspolitiet skal kunne håndtere i konverteringen af historiske teledata.

**3.3.3 Rekvirering af historiske teledata (C)**

Politikredse mv. kan via Rigspolitiets Telecenter bestille (rekvirere) historiske teledata hos teleudbydere i forbindelse med efterforskning af strafbare forhold (C) på baggrund af en kendelse (Internationalt kendt som en Liid 'Lawful Interception ID'). Rekvisitioner kan fremsendes på flere

måder, herunder via en web-portal, standardiseret blanket (sendes via e-mail) eller per e-mail. Generelt er det efterforskere, som rekvirerer historiske teledata via web-portalen. I særlige tilfælde foretages rekvirering af historiske teledata af en teledataanalytiker efter aftale med en efterforsker.

Rigspolitiet sender på baggrund heraf en krypteret rekvisition til teleselskabet. Rekvisitionen sendes af Rigspolitiets Telecenter i et standardformat, hvor det bl.a. angives hvilke selskaber teleoplysningerne skal indhentes hos, hvorvidt rekvisitionen angår teleoplysninger, udvidede teleoplysninger eller mastesug, ligesom tidsmæssig afgrænsning for rekvisitionen fremgår.

Rekvireringerne tilgår teleudbydernes 'politigrupper', der består af sikkerhedsgodkendte medarbejdere. Disse medarbejdere kvalitetssikrer de modtagne rekvisitioner, bl.a. ift. hjemmel og korrekt udfyldelse af skema, hvorefter de efterspurgte data indhentes. I denne proces anvendes typisk datasøgninger/-modeller til rekvirering af data fra teleudbydernes database(r). Der observeres en vis variation på tværs af teleudbydere, herunder i forhold til graden af manuelle vs. automatiserede processer. Det rekvirerede data sendes herefter til Rigspolitiet.

### 3.3.4 Rigspolitiets konvertering af rådata (D)

Når Rigspolitiets Telecenter modtager rådata på baggrund af en rekvisition foretages en automatiseret konvertering, som danner et sæt behandlet (konverteret) data (D). Data konverteres for at sikre, at de historiske teleoplysninger fremstår ensartede og genkendelige under efterforskningen og i forbindelse med en eventuel efterfølgende fremlæggelse i retten. Behovet for konvertering og ensretning af historiske teledata skyldes, at politiet modtager data fra teleudbydere i forskellige formater. Foruden modtagelsen af forskellige formater, er der for politiet et behov for at kunne sammenstille data fra teleudbydere og analysere på tværs af disse data.

De konverterede data oversendes herefter automatisk til den rekvirerende politikreds mv. sammen med rådatasættet og en vejledning vedrørende historiske teledata. Vejledningen giver efterforskere og sagsbehandlere indblik i anvendelsen af data, herunder hvilken kvalitetskontrol, der skal foretages ved modtagelse af konverterede data.

Vejledningen beskriver i hovedtræk:

- **Vigtig information:** angivelse af kvalitetskontroller, der bør udføres på det modtagne dataset
- **Filer fra udbydere:** introduktion til rådatafiler og overordnede bemærkningspunkter
- **Udtræk fra konverteringssystem:** overblik over felter og beskrivelse heraf
- **Anvendelse af udtræk:** forskellige afsnit, der angiver hvordan data skal gemmes, formateres etc. Vejledning er baseret på forskellige versioner af filerne

Vejledningen har været ændret flere gange i undersøgelsesperioden, og er senest ændret 8. marts 2019. Ovenstående er gældende for undersøgelsesperiode. Kommunikation vedrørende opdatering af vejledningen foretages af Rigspolitiets Telecenter, men der er historisk ikke i alle tilfælde sket en præcis kommunikation herom.



I politikredse mv. findes yderligere andre variationer af vejledninger til håndtering af historiske teledata. Hertil har Rigspolitiet udstukket retningslinjer for udførelse af kvalitetskontrol af de modtagne data, samt løbende indberetning af status. Vejledningen er første gang udstedt 21. juni 2019, og efterfølgende revideret 2. juli 2019.

### **3.3.5 Politikredsenes og anklagemyndighedens videre anvendelse af historiske data (E)**

Rekvirentens anvendelse og evt. viderebearbejdning af konverteret historisk teledata til efterforskning kan inddeles i modtagelse af data, kvalitetssikring af data samt behandling og anvendelse af data (E).

Generelt modtages historisk teledata af efterforskere via e-mail på baggrund af den afsendte rekvisition. Det er også muligt at hente data online hos Rigspolitiets Telecenter via rekvisitionsnummeret. Såfremt der er behov for involvering af en teledataanalytiker videresendes data til disse. Teledataanalytikere kan ligeledes hente historiske teledata online hos Rigspolitiets Telecenter med rekvisitionsnummeret.

Generelt har der ikke været foretaget kvalitetssikring af historiske teledata i politikredse mv., herunder har der før årsskiftet 2018/19 ikke været udført fuldstændighedskontrol af modtagne historiske teledata. Siden november 2018 har kredse sammen med historiske teledata modtaget vejledning om at foretage kontrol af modtagne historiske teledata. Undersøgelsen sektion 8 udfolder forhold vedrørende kvalitetssikring.

Anvendelse og behandling af historiske teledata afhænger typisk af sagens omfang. I mindre sager vil efterforskere oftest anvende konverteret data uden yderligere behandling. I større sager involveres ofte en teledataanalytiker eller anden videns person, som foretager en videre behandling af historiske teledata. Denne behandling vil typisk bestå i konsolidering af datafiler fra forskellige teleudbydere samt supplerings af data i analyserapporten med relevante oplysninger f.eks. fra nummeroplysningen 118. Betinget af hvilken politikreds mv., der behandler historiske teledata, anvendes de af kredsen indkøbte eller egenudviklede værktøjer til analyse, visualisering og supplerings af historiske teledata i analyserapporten.

Typisk gemmes kun den del af de modtagne historiske teledata, som er relevante i forhold til bevisførelsen i sagen, mens øvrig arkivering af data er afhængig af den enkelte efterforskers vurdering. Rigspolitiets Telecenter opbevarer ikke en kopi af de data, der konkret er sendt til kredsen. Efter Rigspolitiets Telecenters forretningsregler – der er fastsat ud fra rent kapacitetsmæssige overvejelser – opbevares dog en databaseversion af den konverteret data i 24 måneder, med mindre den rekvirerende politikreds mv. anmoder om at data ikke slettes ved udløbet af denne frist. Data gemt i databasen har ikke nødvendigvis været berørt af de samme problemer, som konverteret data fremsendt til politikredse mv., og kan derfor ikke entydigt benyttes som validering. Der bemærkes, at der ikke har været en konsistent praksis i forhold til Rigspolitiets Telecenters sletning af databaseversionen, hvorfor kopier heraf fortsat forefindes i en række sager, hvor rekvireringen skete for mere end 24 måneder siden.

I enkelte politikredse – og især ved større sager, hvor teledataanalytikere involveres – arkiveres historiske teledata efter en fast struktur og med fuld versionsstyring.

Ud over de af Rigspolitiet og Rigsadvokaten udgivne retningslinjer fra hhv. januar 2018, 21. juni, 2. juli, 18. august, 30. august, 13. september og 18. september 2019 om rekvirering af historiske teledata og anvendelse af historiske teledata under efterforskningen og i retssager, forefindes der generelt ikke formelle nationale eller lokale retningslinjer, procedurer eller instrukser for håndtering af historiske teledata.

### **3.3.5.1 Anklagemyndighedens anvendelse af historiske teledata (F)**

Anklagemyndighedens anvendelse af konverteret historiske teledata, kan inddeles i modtagelse af data i forbindelse med overdragelse af en sag fra politiet, kvalitetssikring af data og fremlæggelse af historiske teledata som del af sagens beviser ved retsmøder under efterforskningen samt hovedforhandlingen i straffesager (F).

Når politiets efterforskning er afsluttet, afleveres sagen til anklagemyndigheden. Anklagemyndigheden gennemgår herefter sagens beviser, og foretager en vurdering af, om der skal rejses tiltale. Generelt modtager anklageren en sagsrapport samt underliggende konverteret historiske teledata fra efterforskeren. Omfanget af analyserapporten kan variere, men vil vedrørende historiske teledata typisk indeholde et uddrag af de relevante historiske teledata, en objektiv beskrivelse af hændelsesforløb samt et kort med visuelle angivelser. Som bilag til analyserapporten anvendes den konverterede historiske teledatafil fra Rigspolitiets Telecenter, eventuelt med yderligere databehandling og databerigelse med anden relevant information. Den yderligere behandling af data eller berigelse af informationer afhænger af sagens størrelse, hvorvidt teledataanalytikere har været involveret i sagen og den enkelte efterforsker.

I forbindelse med anklagerens forberedelse til fremlæggelse af sagen i retten, vil anklageren typisk foretage en kontrol af, om de historiske teledataoplysninger, der fremgår af analyserapporten kan genfindes i de konverterede data. Typisk vil anklageren fremlægge analyserapporten og det underliggende konverterede data i retten. Til at understøtte dette har Rigsadvokaten udarbejdet en intern og ekstern vejledning til anklagemyndigheden om forberedelse og præsentation af historiske teleoplysninger i retten.

## **3.4 Rigspolitiets Telecenter**

Rigspolitiets Telecenter bistår politikredsene mv. med at tilvejebringe data fra teleudbydere, herunder historiske teledata. Centeret var frem til maj 2014 organisatorisk forankret i Koncern IT i Rigspolitiet. 1. maj 2014 blev centeret flyttet til Politiområdet og forankret i det nyoprettede Nationalt Cyber Crime Center (NC3). Per 24. juni 2019 er Rigspolitiets Telecenter organisatorisk forankret i Nationalt Kriminalteknisk Center (NKC). De forskellige omorganiseringer, som Rigspolitiets Telecenter har været igennem fra 2008 til i dag, uddybes i det efterfølgende afsnit.

Et af Rigspolitiets Telecenters formål er at bistå politikredsene mv. med at rekvirere teleoplysninger fra teleudbydere på et givent nummer inden for et bestemt tidsrum og/eller geografisk afgrænset område, samt at sikre, at politikredsene mv. anmodninger om udlevering af historiske teledata behandles hurtigt og effektivt.

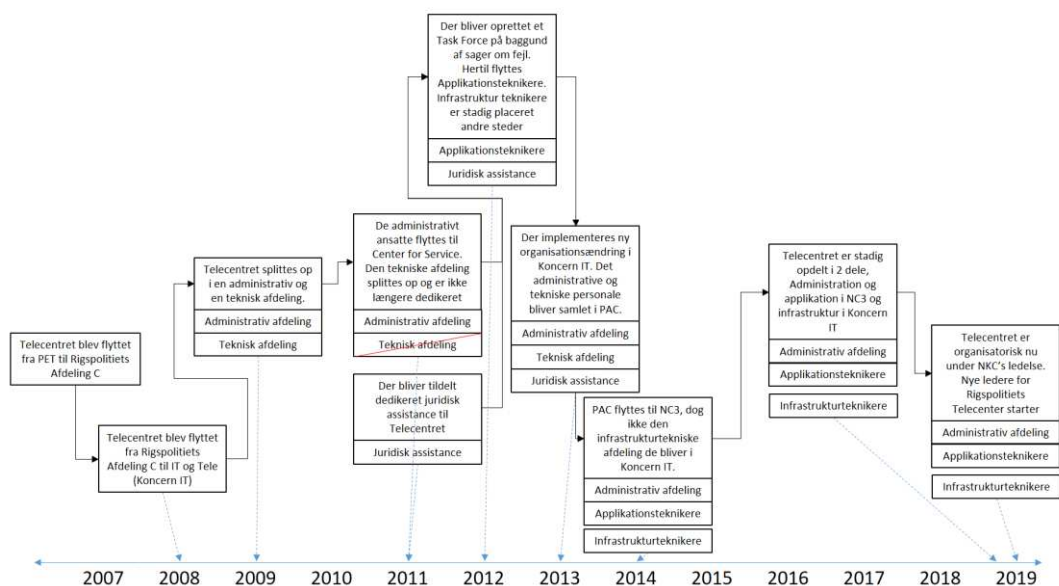
Rigspolitiets Telecenter består overordnet set af to afdelinger; en teknisk og en administrativ. Den tekniske afdeling har ansvaret for applikationer, herunder indsamling og konvertering af data fra teleudbydere samt fremsendelse til efterforskere. Den administrative afdeling står for den generelle personalemæssige administration af Rigspolitiets Telecenter som helhed. Rigspolitiets Telecenter er det centrale kontaktpunkt mellem politikredsene mv. og teleudbydere. Rigspolitiets Telecenters 13 medarbejdere er beskæftiget med support og teknisk drift af systemer i infrastrukturen og varetager desuden andre opgaver herunder modtagelse af rådata vedrørende teleoplysninger og konvertering af rådata. Rigspolitiets Telecenter skal på tværs af disse opgaver bl.a. sikre, at politikredsenes mv. anmodninger om udlevering af historiske teledata behandles hurtigt og effektivt, og at politiet inden for lovens rammer får adgang til de relevante oplysninger fra teleudbydere. Rigspolitiets Telecenter varetager således også i et vidst omfang vejledning af politikredse mv. ift. brug af historiske teledata samt forespørgsler i forbindelse med konkrete sager. Alle medarbejdere i Rigspolitiets Telecenter er sikkerhedsgodkendte.

En kerneopgave for Rigspolitiets Telecenter er konvertering af rådata, så det sikres, at historiske teledata har samme format uafhængig af hvilken teleudbyder, der har leveret rådata. Konverteringen er i det væsentligste automatiseret, men konverteringsudvikling og vedligehold heraf varetages af én medarbejder, mens support vedrørende brug af historiske teledata varetages af tre medarbejdere i Rigspolitiets Telecenter. For alle medarbejdere gælder, at de har andre opgaver ud over historiske teledata. Det samlede ressourceforbrug på opgaven anslås før teledatasagen at have udgjort ca. 1,2 årsværk, hvormed opgaven har udgjort en lille del af Rigspolitiets Telecenters samlede opgaveportefølje.

Rigspolitiets Telecenter understøttes af fem Koncern IT (KIT) medarbejdere, der er sikkerhedsgodkendt til at arbejde med Rigspolitiets Telecenters infrastruktur og data. De fem KIT-medarbejdere arbejder primært med driften af den tekniske infrastruktur for Rigspolitiets Telecenters applikationer. Disse medarbejdere er underlagt ledelsen i KIT, men skal i det væsentligste supportere Rigspolitiets Telecenter.

### **3.4.1 Rigspolitiets Telecenters historiske udvikling**

Der har i perioden fra 2008-2019 været foretaget flere organisatoriske ændringer i Rigspolitiets Telecenter ligesom den organisatoriske forankring af Rigspolitiets Telecenter har udviklet sig. Rigspolitiets Telecenter er i dag underlagt NKC. Herunder opridses den overordnede udvikling.



Rigspolitiets Telecenter blev oprindeligt oprettet under PET, men blev siden organisatorisk flyttet til Rigspolitiets Afdeling C. Grundet organisationsændringer blev Rigspolitiets Telecenter den 1. januar 2008 flyttet til det daværende IT og Tele (Konkern IT). Per 1. december 2009 fik den administrative og den tekniske afdeling i Rigspolitiets Telecenter separat ledelse i forlængelse af en større organisationsændring i Rigspolitiet. I marts 2011 blev administrationsafdelingen flyttet til Center for Service i Konkern IT, og de tekniske medarbejdere blev fordelt på flere forskellige afdelinger. Medarbejderne i administrationsafdelingen var herefter ikke længere dedikeret til alene at servicere Rigspolitiets Telecenter.

I 2013 blev der foretaget en ny organisationsændring i Konkern IT, hvor de administrative og tekniske medarbejdere blev samlet i Rigspolitiets Telecenter i Center for Service. I 2014 blev Rigspolitiets Telecenter flyttet til NC3, mens infrastruktur forblev under Konkern IT. De organisatoriske ændringer har således bl.a. medført, at driften af infrastruktur, udvikling og drift af applikationer i kortere eller længere tid har været underlagt forskellige afdelinger i Rigspolitiet, herunder Konkern IT, og PET. I dag er Rigspolitiets Telecenter organisatorisk forankret i Nationalt Kriminalteknisk Center (NKC).

Det vurderes, at den lave bemanning indebærer en risiko for tab af kontinuitet. En højere redundans i medarbejderstaben vil højne robustheden i Rigspolitiets Telecenters arbejde. At denne risiko endnu ikke er udmøntet afspejler en stor kapacitet, viden, kompetence og vedholdenhed hos medarbejderne i Rigspolitiets Telecenter.

# 4 Undersøgelsesmetode

## 4.1 Introduktion til undersøgelsens datagrundlag

Undersøgelsen af Rigspolitiets håndtering af historiske teledata er baseret på en lang række datakilder. Overordnet kan datagrundlaget inddeles i fire typer:

- i) Rådata modtaget fra teleudbyderne i perioden 3. januar 2011 til 27. august 2019 og konverteret data fra Rigspolitiet fra perioden 23. november 2011 til 27. august 2019 på trækningstidspunktet på dagen.
- ii) Eksisterende dokumentation fra Rigspolitiet og Rigsadvokaten om bl.a. identificerede fejkilder, fejlmeldinger, vejledninger, interne undersøgelser mv.
- iii) Interviews med Rigspolitiet, politikredse, efterforskningsfællesskaber mv. Dette inkluderer interviews med Rigspolitiets Telecenter og Koncern IT omkring arbejdsprocesser, historiske teledata og IT-systemer mv.
- iv) Interviews med interessenter, herunder interviews med Teleindustrien og teleudbydere om teledatas værdikæde og rekvisitiosproces. Hertil interviews og ekspertbidrag fra teledataeksperter, strafferetseksperter samt en forsvarsadvokat. Datagrundlaget for undersøgelsen uddybes i de efterfølgende afsnit.

Mere detaljerede metodebeskrivelser kan af hensyn til sikkerhedsniveauet ikke deles offentligt, men er beskrevet for Rigspolitiet.

## 4.2 Introduktion til undersøgelsens samlede metodiske ramme

Undersøgelsens metodiske ramme kan overordnet deles op i fire lag:

- **Teleinfrastruktur.** Teleudbydernes infrastruktur er afsættet for de historiske teledata, der er undersøgelsens genstandsfelt. Infrastrukturen er ikke i primært fokus men beskrives overordnet med hensyn på at belyse den samlede teledata værdikæde samt karakteristika ved data. Hertil belyses infrastrukturen indirekte via dens afspejling i det analyserede historiske teledata.
- **Dataanalyse af historiske teledata.** Der gennemføres en dataanalyse af historiske teledata, som er genereret i teleinfrastrukturen, som sammenligner rådata fra teleudbyderne med Rigspolitiets konverterede data i perioden 3. januar 2011 – 27. august 2019 på trækningstidspunktet.
- **Systeminfrastruktur.** Den systeminfrastruktur, der anvendes til at behandle og opbevare historiske teledata analyseres med afsæt i et metodisk rammeværk, som tager udgangspunkt i kvalitetsstandarten ISO 27001:2013 samt ITIL-rammeværktøjer for sikker drift. Undersøgelsen fokuserer på generelle it-kontroller, der er væsentlige i forhold til de relevante systemer og tilhørende tekniske platforme.
- **Governance, roller og processer.** Analysen belyser ligeledes governance, roller og processer, der er gældende i forhold til

konvertering af historiske teledata, herunder data- og kvalitetskontrol, samt systeminfrastruktur for historiske teledata.

Lagene i metoderammen, herunder datakilder og analysestrategi, foldes ud i de nedenstående afsnit.

#### 4.3 Afdækning af teleinfrastruktur

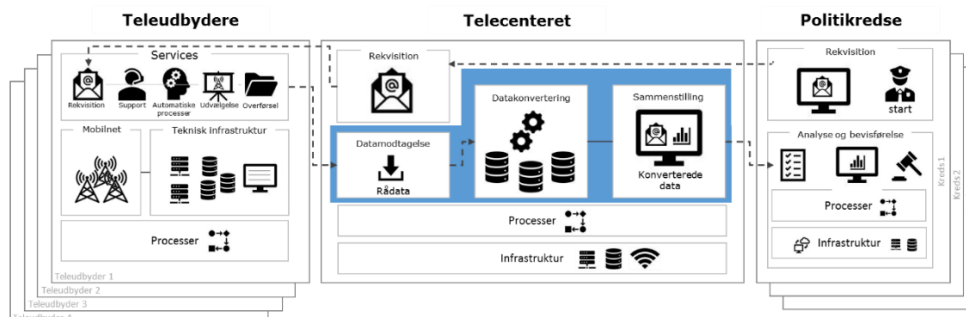
Historiske teledata, der er undersøgelsens genstandsfelt, genereres i teleselskabernes telenet og infrastruktur i form af master, antenner og udstyr til opsamling og lagring af historiske teledata. Der henvises til afsnit 3.3.1 for en gennemgang af mobile enheders kommunikation på mobilnettet.

Oplysninger om infrastrukturen er i undersøgelsen belyst indirekte fra to vinkler. Dels er infrastrukturen belyst via interviews med teleudbydere og eksperter i telekommunikation med henblik på at beskrive teledataværdikæden og karakteren af det genererede historiske teledata. Hertil afspejles infrastrukturen indirekte som et element i analysen af rådata og konverteret data, idet bl.a. mastepositioner og celle-id fremgår af det analyserede data.

Undersøgelsen har ikke belyst den faktiske kvalitet i teleudbydernes infrastruktur, herunder eksempelvis den faktiske placering af master. Endvidere er der f.eks. ikke foretaget selvstændige målinger af mobile enheders forbindelse til teleinfrastrukturen med hensyn på at validere det fra teleudbyderne modtagne rådata.

#### 4.4 Metode til dataanalyse

Dataanalysen fokuserer på konverteringen af historiske teledata og foretager en sammenligning af alle de rådatasæt og konverterede datasæt, der er til rådighed for analysen. I et værdikædeperspektiv er fokus i denne delanalyse alene det modtagne rådata fra teleudbyderne, konvertering og sammenstilling heraf i Rigspolitiets Telecenter. Denne afgrænsning fremgår med blå i figuren nedenfor. Formålet med undersøgelsen er at afgøre, om der er uoverensstemmelser mellem de to datasæt, herunder ift. om alle aktiviteter og lokaliseringsoplysninger i rådata er medtaget korrekt i konverterede data.



##### 4.4.1 Opsumming af metode til dataanalyse

Beskrivelsen af metoden er opsummeret i dette afsnit, mens de enkelte punkter gennemgås mere detaljeret i efterfølgende underafsnit.

Der er indledningsvis etableret et sikkert og afskærmet miljø til analysen af historiske teledata. Miljøet har været placeret fysisk hos Rigspolitiet og har været fuldstændigt afskærmet fra andre netværk af hensyn til datas følsomhed og sikring af uvildighed i forhold til Rigspolitiets egne data og analyser. På det afskærmede miljø er installeret en række avancerede standardsoftware-produkter, der har været anvendt til analysen. Deloitte har på dette miljø indlæst de rådatafiler og konverterede datafiler, som har været identificerede og tilgængelige i Rigspolitiets Telecenter den 27. august på det tidspunkt, hvor data blev trukket og efterfølgende overleveret til Deloitte.

Data er overdraget til Deloitte i form af rådata, som modtaget fra teleudbydere, og de fundne konverterede data, som Rigspolitiet efterfølgende har udsendt til politikredse mv., der har rekvireret data. Konverteret data er hos Rigspolitiet indsamlet til undersøgelsens formål ved en søgning på mailservere, netværksdrev mv., som er blevet afsøgt for data, idet Rigspolitiets Telecenter ikke opbevarer en kopi af de data, der konkret er sendt til kredsen. Efter Telecenterets forretningsregler – der er fastsat ud fra rent kapacitetsmæssige overvejelser – opbevares dog en databaseversion af den konverteret data i 24 måneder, med mindre den rekvirerende politikreds mv. anmoder om at data ikke slettes ved udløbet af denne frist. Data gemt i databasen har ikke nødvendigvis været berørt af de samme problemer, som konverteret data fremsendt til politikredse, og kan derfor ikke entydigt benyttes som validering.

Deloitte har sammenlignet de modtagne rådata og de afsendte konverterede data 1:1 og identificeret i hvilket omfang de to dataset er identiske. Herefter er gennemført en statistisk analyse af de modtagne rådata (en dataprofil) for at vurdere datakvaliteten af de modtagne data. I forhold til at perspektivere, fortolke og konkludere på resultaterne af såvel den direkte 1:1 sammenligning af data og dataprofileringerne, er der gennemført en række interviews med it-udviklere og driftsmedarbejdere i Rigspolitiets Telecenter, teleudbydere samt nationale og internationale eksperter på teledataområdet.

#### **4.4.1.1 Etablering af et sikkert afskærmet miljø**

Der er etableret et sikkert afskærmet miljø til udvikling og test af Rigspolitiets datakonvertering af de modtagne rådata. Miljøet har ikke været forbundet til andre interne eller eksterne netværk og har således været helt afsondret fra Rigspolitiets Telecenter og omverdenen.

#### **4.4.1.2 Anvendt software**

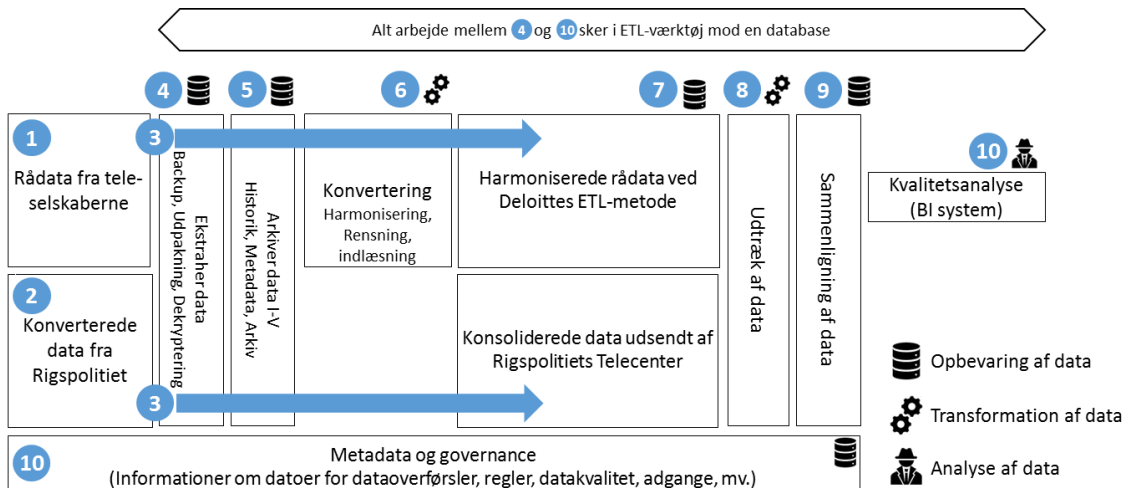
På det afskærmede miljø er installeret en række avancerede standardsoftware-produkter. Deloitte har anvendt en type software, der er kendt fra datavarehuses behandling af massive datamængder som 'Extract, Transform, Load' (ETL). Formålet med denne type software er på en ensartet, entydig og sporbar måde at transformere data fra mange forskellige kildesystemer til ét fælles format. Metoden baseret på denne type software er beskrevet i litteraturen og har været anvendt i over 25 år på tværs af brancher og lande, når data skal konsolideres.

#### **4.4.2 Udvikling af rapporteringsarkitektur**

Deloitte har som en del af analysen etableret en rapporteringsarkitektur, der har sikret integriteten af data i hver enkelt lag i arkitekturen. Derudover sikrer arkitekturen, at alle datatransformationer er klart definerede og

sporbare. Målet er at datas ejerskab og sporbarhed er entydig fra start til slut (dataprovien).

Data analyseres ved at gennemføre en række transformationer og harmoniseringer, som understøttes af en arkitektur, der er illustreret nedenfor og efterfølgende detaljeres.

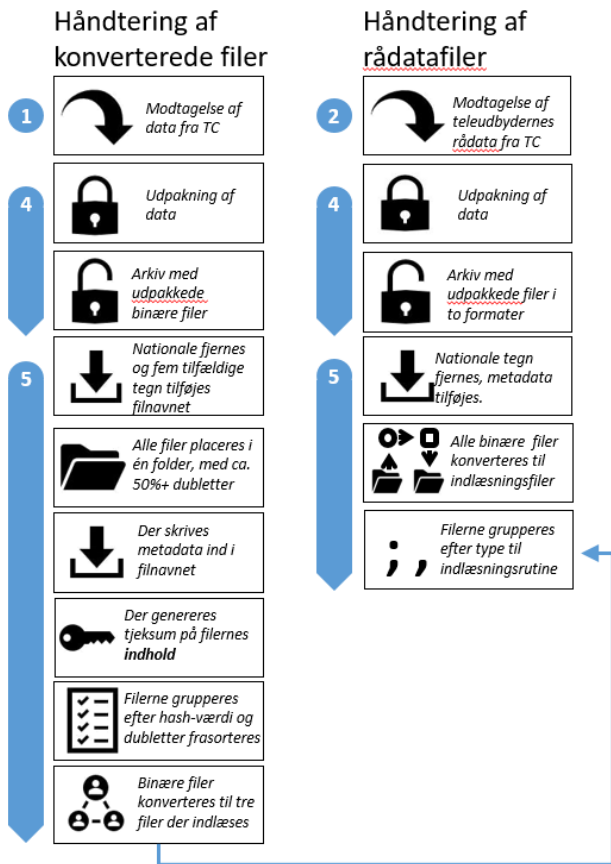


Rigspolitiets Telecenter har overleveret de oprindelige rådata til Deloitte, som er modtaget fra teleudbyderne i perioden 3. januar 2011 til 27. august 2019 på trækningstidspunktet (trin 1). Rådata er overdraget i de to oprindelige ikke-konverterede formater. Rigspolitiets Telecenter har hertil leveret kopier af de fundne konverterede data, der er udsendt fra Rigspolitiets Telecenter til politikredsene mv. i perioden 23. november 2011 til 27. august 2019 (trin 2). Det konverterede data fra Rigspolitiets Telecenter består af tre separate rapporter, hhv. en sessionsrapport, en samlerapport og en summeringsrapport. Sessionsrapporten og samlerapporten er udtryk for separate konverteringer, mens summeringsrapporten er afledt af sessionsrapporten. Det er samme rådata, der ligger til grund for de tre rapporter. Der er en lille forskel i måden de tre rapporter er lavet på, hvilket historisk er set have påvirket sessions- og samlerapporten, så der ikke har været overensstemmelse mellem disse. Derfor gennemføres analysen på disse to rapporter.

Data er herefter kopieret fra Rigspolitiets medie til analyseplatformens 'data staging area' (DSA) (trin 3), som er et lag i arkitekturen, hvor data modtages og forberedes til indlæsning. Al videre behandling af de modtagne data foregår i dette lag (trin 4). DSA-laget i arkitekturen fungerer samtidig som et arkiv, hvorfra data kan genindlæses, hvis det viser sig, at der er fejl i en efterfølgende konvertering.

For både rådata og konverterede filer gælder, at der først foretages en udpakning af data, hvorefter filerne placeres i et arkiv med udpakkede filer. Processen for indlæsning og arkivering af rådata og konverteret data er herefter af forskellig kompleksitet (trin 5). De enkelte trin i indlæsningen af hhv. rådata og konverteret data fremgår i figuren nedenfor og uddybes i det efterfølgende.

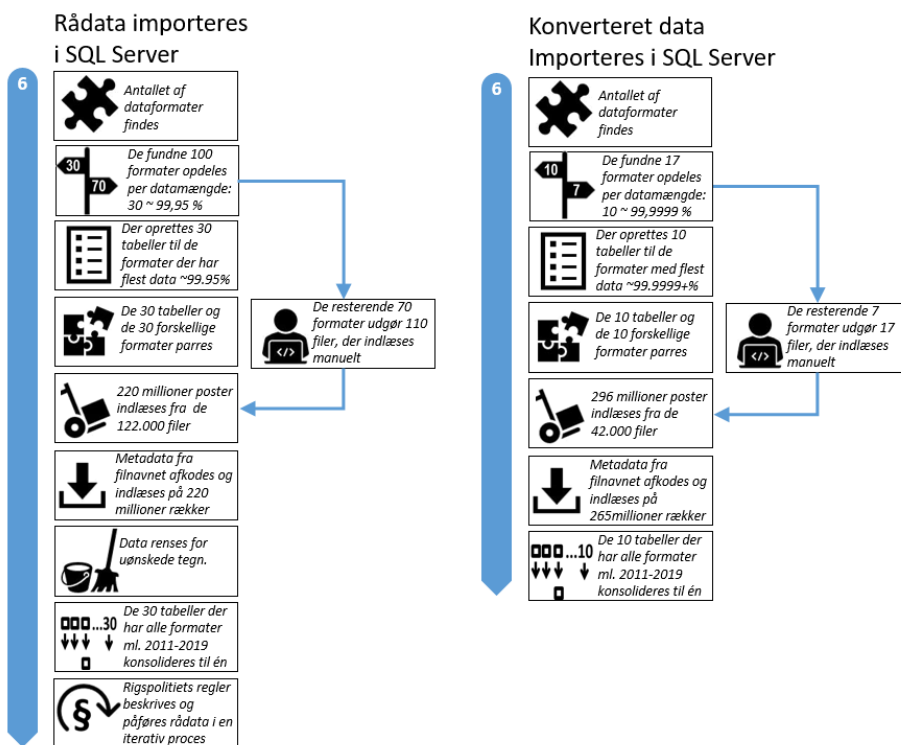




Indledningsvis dekomprimeres filerne og nationale specialtegn fjernes fra filnavnene.

Der er identificeret en betydelig mængde dubletter i de modtagne konverterede filer, som fjernes ved at identificere, om indholdet af filen er unikt (trin 5 i figurens venstre søjle). Dubleringen af filer skyldes den af Rigspolitiet anvendte indsamlingsmetode for konverteret data, hvor konverteret data via forskellige søgninger kan være modtaget flere gange. Dubletter håndteres ved at generere en såkaldt 'hash-kode'. Hash-koder er unikke koder, der tilføjes den enkelte fil som metadata på baggrund af en algoritmisk hash-funktion. De genererede koder er i praksis unikke, og hvis indholdet af to filer er ens, vil filerne få samme kode (selvom filerne har forskellige tidsstempeller eller forskelle i andre metadata). Baseret på disse koder elimineres filer med dubleret indhold inden data behandles videre. Samtlige filer konverteres til et format, der indeholder præcis samme data, men er lettere at importere i databasen. jf. ovenstående illustration. Forskellen skyldes, at det konverterede data har en anden struktur og sammensætning end rådata.

Efter arkivering af rådata gennemføres en harmonisering (konvertering) af rådata ved Deloittes ETL-metode (trin 6, uddybes i figuren nedenfor). Harmoniseringen af rådata muliggør en efterfølgende sammenligning af rådata og konverteret data. Dermed skabes et grundlag for at vurdere, om Rigspolitiets konvertering er foretaget korrekt. Harmoniseringen håndterer en række forhold, der ellers ville hindre en sammenligning af rådata og konverteret data. Herunder transformeres rådata til et ensartet format. Disse transformationer uddybes i de efterfølgende afsnit.



Transformeringen af formater gennemføres for at kunne sammenligne de modtagne rådata, der foreligger i 100 forskellige formater, ved at ensarte dem til så få formater som muligt. Hvert af de 100 dataformater afviger fra de øvrige 100 formater på mindst én af følgende måder:

- Rækkefølgen af kolonnerne varierer
- Navngivningen af kolonnerne varierer
- Antallet af kolonner varierer

Forskelle i antallet af kolonner afspejler dels teleudbydernes forskellige opfattelse af, hvilke data der skal inkluderes i datatræk, men også en variation over tid, hvor Rigspolitiets ønsker til data varierer. Dertil kommer, at forskellige typer af rekvisitioner resulterer i forskellige datakolonner. Forskelle i navngivningen af kolonnerne skyldes forskelle i teleselskabernes IT-systemer. Ved at reducere antallet af formater mest muligt lettes sammenligningen med de formater, som Rigspolitiet har tilstræbt i sine konverteringer. Dette betegnes 'dataharmonisering'.

Dertil kommer, at der er mange eksempler på kendte fejlkilder i rådata, der håndteres af Rigspolitiets Telecenter. Disse fejlkilder skal rettes før en sammenligning af indholdet giver mening og er mulig. Eksempler på fejlkilder i de modtagne rådata kan være dataposter, der kun indeholder tomme felter, dataposter med uvedkommende data (f.eks. taksten for SMS'er), eller dataposter hvor danske tegn er erstattet med tegn som ⚡ og Ÿ. Sådanne simple og systematiske fejlkilder skal korrigeres under indlæsningen. Dette betegnes som 'datarensning' og er nødvendig for at kunne sammenligne indholdet mellem poster.

Endelig repliceres en række datatransformationer, som gennemføres som del af Rigspolitiets Telecenters konvertering af historiske teledata. Indarbejdelsen af transformationerne bidrager til at gøre sammenligningen mellem Deloitte's konvertering og den konvertering, som Rigspolitiets Telecenter historisk har foretaget, så valid som mulig. Konkret inkluderes og implementeres de konverteringsregler, som Rigspolitiets Telecenter kan dokumentere over for Deloitte. Afdækningen af den dokumenterede

konvertering er sket ved interviews med Rigspolitiets Telecenter, der forestår konverteringen.

Der kan her skelnes mellem enkle og komplekse konverteringsregler. En enkel konverteringsregel kan f.eks. være, at de øverste rækker i en rådatafil fra en teleudbyder i en periode er blevet fjernet, fordi denne udbyder har inkluderet takseringsinformation i de øverste rækker i rådatafilerne (denne information er irrelevant for politiets formål). Et eksempel på en kompleks konverteringsregel er den transformation af mastekoordinater, som gennemføres fordi teleudbyderne anvender forskellige koordinatsystemer i de rådata, der leveres til Rigspolitiets Telecenter.

Langt de fleste af de identificerede konverteringsregler kan kategoriseres som simple. Konverteringsreglerne og -intentionerne repliceres og afspejles i ETL-metoden. Det er ikke den faktiske konverteringskode, der kopieres. Det sikrer, at eventuelle konverteringsfejl grundet koden ikke overtages. Datatransformationerne resulterer i data, der kan sammenlignes linje for linje med de data, som Rigspolitiet har udsendt og med en klar sporbarhed til de originale rådata. Efter gennemført dataharmonisering og datarensning indlæses Deloitte's harmoniserede data i databasen (trin 7).

Rigspolitiets konverterede data læses direkte ind i databasen uden at dataindholdet bliver modificeret. Der tilføjes enkelte nye felter til hver post, der sikrer at hver enkelt linje i databasen kan henføres til den oprindelige sag, rekvisition til teleudbyderne, fil fra Rigspolitiets Telecenter, teleudbyder der har sendt data og indlæsningstidspunktet. Disse metadata tilføjes det oprindelige indhold, men ændrer det ikke.

De harmoniserede, kvalitetssikrede og rensede data gemmes og ligger til grund for al senere analyse (trin 7). De to sæt konverterede data fra hhv. Rigspolitiet og Deloitte ligger i forskellige dele af databasen, men kan sammenlignes direkte og analyseres sammen eller hver for sig.

Der foretages herefter et udtræk af data (trin 8), og det defineres hvilke tests, der skal gennemføres. For hver rekvisition af data, hvor der er identificeret rådata og tilhørende konverteret data fra Rigspolitiets Telecenter, foretages en sammenligning af data, der er konverteret af Deloitte og Rigspolitiet (trin 9). Der gennemføres tests af:

- 1) **Antallet af rekvisitioner**, hvor der forefindes både rådata og konverterede data. Dette er med til at definere, hvor dækkende dataanalysen er
- 2) **Indeholder konverterede data alle de forventede rådata**, eller er der rådata, der er blevet overset i konverteringen. Testen belyser række for række og felt for felt, om der er sket et datatab i konverteringen
- 3) **Har alle konverterede datasæt tilsvarende rådata**, eller forekommer der indhold i de konverterede data, der er sendt til politikredsen mv., hvor rådata har tomme felter. Dette testes særligt med fokus på felter, der angiver retning for celler
- 4) **Antal af dublerede linjer**. Testen belyser, om konverteringen har resulteret i direkte dublerede linjer i de konverterede data
- 5) **Direkte sammenligning af dataindhold** i poster, hvor dataindhold kan sammenlignes direkte. Testen belyser for alle dataposter, om der er fejl i de kolonner, hvor dataindhold i rådata og konverteret data kan sammenlignes direkte, f.eks. vedrørende opkaldstype, startdato og tid, IMEI-nummer etc.

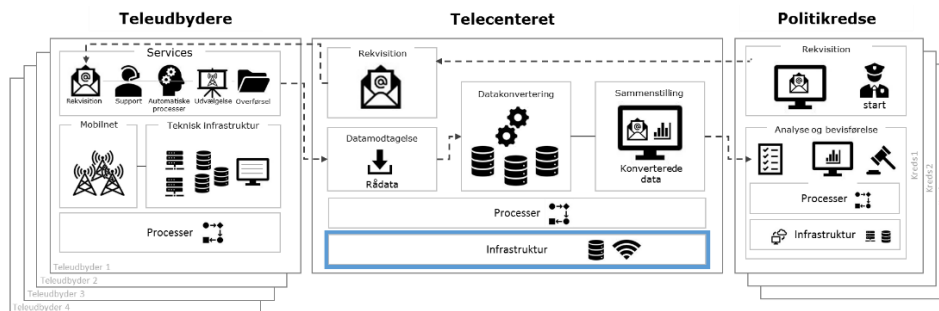
6) **Sammenligning af konverterede masteoplysninger.** Testen belyser, om der er fejl i de kolonner, hvor der er foretaget en konvertering af mastepositioner

I forlængelse af sammenligningen af rådata og konverteret data præsenteres sammenligningerne (trin 10).

I metadatalaget er data om systembehandling af de modtagne data registreret for trin 1-10 (trin 11). Herunder registreres datoer, brugerroller, filnavne, kilder, forretningsregler, der anvendes, og alt anden dokumentation vedrørende databehandlingen.

**4.5 Metode til afdækning af systemer og infrastruktur**

Undersøgelsen belyser funktionalitet, teknisk integritet og driftsstabilitet for de IT-systemer, der anvendes til opbevaring og behandling af historiske teleoplysninger i Rigspolitiets Telecenter, samt processer og dokumentation for IT-kontroller i Rigspolitiets Telecenter og Koncern IT. Dette fokus for undersøgelsen er i et værdikædeperspektiv markeret med blå nedefor. Undersøgelsen belyser således ikke teleudbydernes systemer og infrastruktur til modtagelse, sammenstilling og behandling af historiske teledata.



Afdækningen af Rigspolitiets systemer og infrastruktur er foretaget med afsæt i et metodisk rammeværk, som tager udgangspunkt i kvalitetsstandarden ISO 27001:2013 (Information Security Management) samt ITIL (Information Technology Infrastructure Library)-rammeværktøjerne for sikker drift. ISO 27001 blev ligeledes et krav i 2014 for statslige myndigheder at følge. Undersøgelsen er fokuseret på de generelle IT-kontroller, der er væsentlige i forhold til de systemer og tilhørende tekniske platforme, der behandler og opbevarer historiske teledata. Udvælgelsen af de generelle IT-kontroller er således baseret på det overordnede formål at afdække IT-systemernes funktionalitet, tekniske integritet og driftsstabilitet. Inden for disse områder belyser rammeværket en række underdimensioner:

- **Systemernes funktionalitet**, herunder overordnet funktionalitet ift. håndtering og opbevaring af historiske teledata. F.eks. områder som versionsstyring, revisionsspor, kvalitetskontroller mv.
- **Teknisk integritet**, herunder systemers indretning ift. at sikre dataintegritet, herunder sikring mod teknisk forvanskning.
- **Driftsstabilitet**, herunder i forhold til sikring mod systemnedbrud ved f.eks. backup, fail-over, systemreetablering ved backup, og ydelse (eksekverings hastighed) i daglig brug

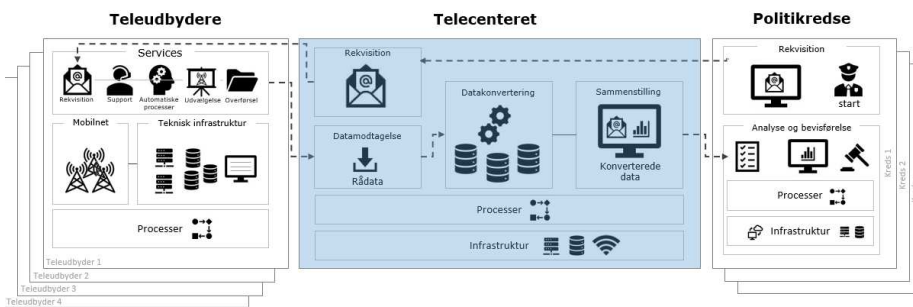
Med afsæt i rammeværket er der indledende foretaget en gennemgang af systemlandskabet med henblik på at foretage en afgrænsning af systemer i

scope, således at der foretages en gennemgang af *alle* systemer, der anvendes i forbindelse med konvertering af historiske teledata. Med afsæt i denne afgrænsning og systemforståelse er der foretaget en gennemgang af de ledelsesgodkendte procedurer for informationssikkerhed og administration af IT-systemer og infrastruktur.

Analysen har taget udgangspunkt i tilgængelig dokumentation, herunder systemoptegnelser og en 'vugge til grav' gennemgang af dataflow. Der er yderligere gennemført interviews med nøglemedarbejdere i Telecenteret samt medarbejdere i Koncern IT, der arbejder med driftsunderstøttelsen af Rigspolitiets Telecenter.

#### 4.6 Metode til afdækning af governance, roller og processer, herunder kvalitetskontrol

Som et sidste lag i undersøgelsen er governance, roller og processer afdækket med et primært fokus på kvalitetskontrol af historiske teledata. I et værdikædeperspektiv har undersøgelsen således belyst governance, roller og processer på tværs af teleudbydere, Rigspolitiets Telecenter og kredsene, hvilket fremgår med blå af figuren nedenfor.



Det er væsentligt at bemærke, at det primære fokus for afdækningen af governance, roller og processer, herunder kvalitetskontrol, er Rigspolitiets Telecenters processer fra historiske teledata modtages, opbevares og behandles til de afleveres til politikredsene mv. Analysen af teleudbydere og politikredsene mv. har været overordnet og begrænset til enkelte interviews.

Som afsæt for analysen har Deloitte haft adgang til et omfattende kildemateriale, som er stillet til rådighed af Rigspolitiet. Materialet dækker bl.a. tidligere udarbejdede rapporter og interne notater vedrørende anvendelse af historiske teledata, historik omkring Rigspolitiets Telecenter og dets rolle, kommunikation og dokumentation om identificerede fejkilder i rådata og i konverteringen af historiske teledata, resultater af Rigspolitiets interne undersøgelser af håndtering og konvertering af historiske teledata, kontrakter med teleudbydere, vejledninger og øvrigt materiale fra politikredsene mv. vedrørende håndtering og kvalitetssikring af historiske teledata. Materialet er anvendt til at identificere iboende usikkerheder ved anvendelse af historiske teledata, give et overordnet indblik i teledataværdikæden samt at belyse governance, roller og processer på tværs af televærdikæden. Deloitte har løbende gennem undersøgelsens forløb modtaget yderligere kildemateriale fra Rigspolitiet, herunder hvor der fra konsulentteamet er efterspurgt yderligere dokumentation.

Afdækningen af governance, roller og processer tager herudover i vidt omfang udgangspunkt i interviews. Der er foretaget interviews internt i Rigspolitiet, med eksterne interessenter, samt relevante teleeksperter og

teleudbydere. Formålet med de gennemførte interviews har dels været at belyse processer, arbejdsgange og roller på tværs af teledataværdikæden, herunder ift. kvalitetskontrol, samt at belyse potentielle fejkilder og usikkerheder i dette perspektiv. Interview-tilgangen har været central, da særligt processer for kvalitetskontrol i meget begrænset omfang har været dokumenteret.

Der er gennemført interviews med følgende aktører:

- **Interviews med Rigspolitiets Telecenter.** Rigspolitiets Telecenters roller, processer, systemer og samarbejde med telebranchen er belyst gennem interviews. Herunder både ift. overordnede arbejdsgange samt vedrørende mere tekniske forhold. I forbindelse med dataanalysen (afsnit 4.4) har der været en tæt løbende dialog med Rigspolitiets Telecenter omkring data, dataindlæsning, forretningsregler mv.
- **Interview med Koncern IT i Rigspolitiet.** Interviews har belyst roller, processer og governance mellem Rigspolitiets Telecenter og Koncern IT samt driftsunderstøttelsen af Rigspolitiets Telecenter.
- **Interview med Rigspolitiets databeskyttelsesrådgiver og sektionsleder inden for sikkerhed i Koncern IT.** Interviews har belyst Rigspolitiets arbejde med IT-sikkerhedspolitikker og dataklassifikation.
- **Interviews med Rigsadvokaten.** Interview vedrørende anvendelse af historiske teledata i straffesager.
- **Interviews med PET.** Interviews vedrørende systemunderstøttelse mv.
- **Interviews med politikredse.** Interviews med efterforskere vedrørende politikredsenes anvendelse af historiske teledata. Foruden efterforskere og teleanalytikere er der gennemført interviews med den lokale anklagemyndighed.
- **Interviews med de 4 teleudbydere og Teleindustrien.** Interviews vedrørende proces for håndtering af rekvisitioner samt forståelse af tekniske aspekter af televærdikæden og historiske teledatas iboende karakteristika. Dette med særligt henblik på indsamling af information til udarbejdelse af notat om anvendelse af historiske teledata i straffesager.
- **Interviews med udenlandske politimyndigheder.** Der er gennemført interview med en politimyndighed i USA (gennemført af Rigspolitiet på baggrund af spørgeguide fra konsulentteamet). Interviewet har bidraget med perspektiver på en fremadrettet styrket kvalitetskontrol og governance teleudbydere og politiet imellem.
- **Interviews med Deloitte-eksperter i USA og England.** Interviews har belyst perspektiver på kvalitetskontrol og governance teleudbydere og politiet imellem.
- **Interview og ekspertbidrag fra teleekspert fra DTU Telecommunications.** Ekspertbidrag vedrørende processer, teleinfrastruktur og -netværk mv. hos teleudbyderne samt bidrag vedrørende fejkilder og usikkerheder vedrørende historiske teledata.
- **Ekspertbidrag fra Analyses Mason.** Ekspertbidrag om processer, teleinfrastruktur og -netværk mv. hos teleudbyderne samt bidrag vedrørende fejkilder og usikkerheder vedrørende historiske teledata.
- **Ekspertbidrag fra strafferetseksperter.** Ekspertbidrag vedrørende vedrørende opmærksomhedspunkter ved anvendelse af historiske teledata i straffesager.

- **Ekspertbidrag fra forsvarsadvokat.** Ekspertbidrag vedrørende vedrørende opmærksomhedspunkter ved anvendelse af historiske teledata i straffesager.

# 5 Sammenligning af rådata og konverterede data

## 5.1 Formål og afgrænsning af sammenligning af rådata og konverterede data

Undersøgelsen har til formål at sammenligne alle de rådatasæt og konverterede datasæt, der har været til rådighed for analysen med henblik på at afgøre, om der er uoverensstemmelser mellem de to datasæt. Undersøgelsen dækker både uoverensstemmelser på række- og feltniveau, herunder om alle aktiviteter og lokaliseringsoplysninger i rådata er medtaget korrekt i konverterede data.

Dataanalysen fokuserer på historiske teledata (herunder udvidede teleoplysninger også kaldet mastesug), dvs. beskrivelser af hændelser, der har fundet sted (ikke hændelser der finder sted) samt data, der er transporteret via mindst én mobilantenne. Ud over samtaler vedrører undersøgelsen også historiske data om de tre øvrige tjenestetyper (sms, mms og datatransmissioner) til og fra mobile enheder. Uagtet tjenestetype omhandler undersøgelsen ikke det faktiske indhold af kommunikationen mellem enheder. De historiske data – og derfor dataundersøgelsen – omhandler alene tidspunktet, tjenestetypen, anvendt mast(er), første og sidste celle i transmissionen og involverede mobile enheder.

Sektionen er struktureret i fire hovedsektioner:

- **Datakvalitet i rådata modtaget fra teleudbydere.** Afsnittet belyser datakvaliteten i det rådata, som er modtaget fra teleudbyderne, og som udgør grundlaget for den videre sammenligning af rådata og konverterede data.
- **Analyse af antal rækker i rådata og konverteret data.** Analysen belyser, hvorvidt der i forbindelse med konverteringen af rådata modtaget fra teleudbyderne er sket et tab af rækker i det konverterede data (herefter rækketab).
- **Sammenligning af indhold i felter i rådata og konverteret data.** Analysen sammenligner dataindholdet i de rekvisitioner, hvor der både findes rådata og konverteret data. Sammenligningen er foretaget på niveau af det enkelte felt i den enkelte række, som sammenholdes på tværs af rådata og konverteret data.
- **Analyse af konvertering af mastepositioner.** Analysen belyser for alle rekvisitioner, hvor der findes både rådata og konverteret data, om der er fejl i konverterede mastepositioner.

Rigspolitiet har ligeledes gennemført en række interne undersøgelser og stikprøvekontrol af konvertering af historiske teledata. Herunder bl.a. en stikprøvekontrol på konvertering af 365 rekvisitioner dækkende perioden 2012-2019, ligesom der er foretaget en intern undersøgelse af konvertering af mastekoordinater. Deloitte har i forbindelse med undersøgelsen af Rigspolitiets håndtering af historiske teledata fået overdraget Rigspolitiets egne analyser med henblik på videre kvalificering. I gennemgangen af



analysens resultater nedenfor perspektiveres resultaterne af den uvildige analyse til Rigspolitiets egne fund vedrørende konverteringsfejl mv.

## 5.2 Sammenfatning af sammenligningen af rådata og konverteret data

Den indledningsvise analyse af rådata modtaget fra teleudbyderne viser, at teleudbydernes leverancer til Rigspolitiet er karakteriseret ved en lav grad af standardisering. Der er samtidig identificeret en række eksempler på manglende eller ikke-retvisende indhold vedrørende centrale oplysninger i rådata. Samlet set indikerer disse fund, særligt vedrørende mastepositioner, at der fremadrettet med fordel kan iværksættes tiltag for at øge datakvaliteten.

Analysen af Rigspolitiets konvertering af historiske teledata på rækkeniveau viser, at der er uoverensstemmelse i antal rækker mellem konverterede data og rådata i 6,9 pct. af de undersøgte rekvisitioner. Heraf er der samlet set et rækketab i ca. 5,8 pct. af de undersøgte rekvisitioner, hvilket er en lavere andel end Rigspolitiet har identificeret i sin interne screening. Rækketabet er overvejende koncentreret i 2016. Betydningen af rækketab afhænger af den konkrete anvendelsessituation.

Analysen af Rigspolitiets konvertering af historiske teledata på rækkeniveau identificerer en række konverteringsfejl på feltniveau, hvor der i perioden 2011-2019 er sket en række meget forskelligartede konverteringsfejl, som optræder i varierende omfang. Der er i al væsentlighed tale om resultater, der flugter med de fund, som Rigspolitiets Telecenter har identificeret i interne undersøgelser og en stikprøvekontrol for perioden 2012-2019. Betydningen af en konverteringsfejl varierer afhængig af feltets indhold og fejls karakter. Nogle konverteringsfejl er helt uden praktisk betydning, andre kan have betydning i specifikke situationer, mens endnu andre generelt kan have betydning. I forhold til mastepositioner kan fremhæves, at de fundne konverteringsfejl i de fleste tilfælde ikke vil have betydning i lyset af de generelle usikkerheder, der er forbundet med geografisk lokalisering ved brug af teledata. Navnlig i tættere bymæssig bebyggelse, hvor celler generelt dækker et mindre område, kan selv mindre forskydninger dog i specifikke situationer potentielt have betydning.

Endelig viser analysen af konvertering af mastekoordinater, at der i perioden 2011-2019 er sket forskydninger af mastekoordinater i forbindelse med i Rigspolitiets Telecenters konvertering af mastepositioner. Den langt overvejende del af disse forskydninger udgøres af en konverteringsfejl, hvor mastekoordinater er forskudt med ca. 222 meter. Hertil er der identificeret et mindre antal rekvisitioner med forskydninger af mastekoordinater på ca. 100 meter. Endelig er der identificeret et meget begrænset antal rekvisitioner med meget betydelige forskydninger af mastepositioner.

Sammenfattende bekræfter Deloitte's undersøgelse i al væsentlighed de resultater, som Rigspolitiets interne undersøgelser og stikprøvekontroller har afdækket. Det er gældende for alle identificerede afvigelser mellem rådata og konverteret data, at det på baggrund af undersøgelsens metode er muligt at spore uoverensstemmelser i konverteringen ned på niveau af den enkelte rekvisition og journalnummer (den enkelte sag). Disse oplysninger stilles til rådighed for politi og anklagemyndighed i forlængelse af undersøgelsen og vil kunne anvendes fremadrettet af politikredse mv. i forhold til at belyse hvorvidt og i hvilket omfang konkrete sager er berørt af konverteringsfejl, herunder hvilke specifikke fejl, der er tale om.

### 5.3 Datakvalitet i rådata modtaget fra teleudbydere

Der er indledningsvist gennemført en analyse af datakvaliteten for rådata leveret af teleudbyderne. Analysen af datakvalitet indebærer ikke en sammenligning op mod konverteret data, men har karakter af deskriptiv statistik for det rådata, som Rigspolitiet har modtaget fra teleudbyderne.

Samlet set viser gennemgangen af datakvalitet for rådata, at teleudbydernes leverancer til Rigspolitiet er karakteriseret ved en lav grad af standardisering. Det bemærkes, at en lav grad af standardisering af formater ikke er ensbetydende med, at datakvaliteten nødvendigvis er lav. De mange formater stiller imidlertid store krav til den efterfølgende konvertering af det indkomne rådata hos Rigspolitiets Telecenter.

Der er samtidig identificeret en række eksempler på manglende indhold vedrørende centrale oplysninger i rådata. Der er ligeledes identificeret eksempler på master, som er registreret med koordinater, der ligger uden for Danmarks grænser, ligesom der er eksempler på mastepositioner, der flytter sig over tid. Samlet set indikerer disse fund, særligt vedrørende mastepositioner, at der fremadrettet med fordel kan iværksættes tiltag for at øge datakvaliteten.

#### 5.3.1 Rekvisitioner af rådata

Der er i perioden 3. januar 2011 - 27. august 2019 modtaget 41.842 rekvisitioner fra teleudbyderne, hvoraf 39.622 indeholder data. Årsagen til tomme rekvisitioner vurderes af Rigspolitiets Telecenter til, at der historisk set har været sendt rekvisitioner til samtlige teleudbydere, og teleudbyderne har returneret tomme filer i tilfælde, hvor udbyderen ikke har haft registreringer på det forespurgte nummer. Rekvisitioner med indhold udgør grundlaget for det følgende.

Rekvisitioner	Antal
Rekvisitioner med rådatafiler med og uden indhold	41.842
Rekvisitioner med rådatafiler med indhold	39.622

Herunder vurderes datakvaliteten i form af statistiske oversigter, vurderingen af datakvaliteten er fordelt på:

- Formater, herunder antal formater, antal kolonner per format, antal formater per teleudbyder og år
- Datakvalitet for indhold, dvs. hvorvidt centrale feltoplysninger fremgår af rådata
- Datakvalitet for mastepositioner, herunder ændringer over tid

#### 5.3.2 Dataformater for rådata fra teleudbyderne

Teleudbyderne leverer rådata til Rigspolitiets Telecenter i forskellige formater. Formaterne har varieret fra teleudbyder til teleudbyder og fire af fem teleudbydere har varieret formatet over tid (der er i dag kun fire teleudbydere).

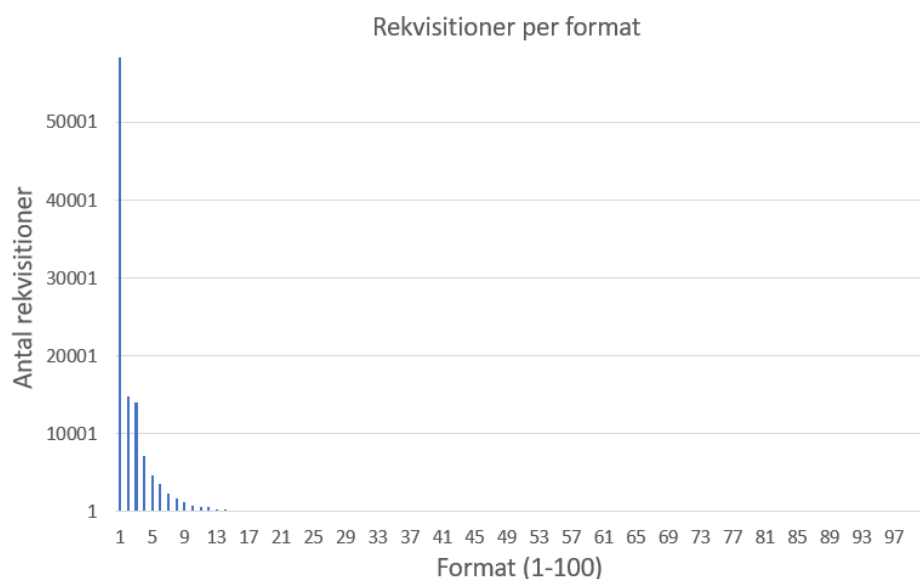
Der er lavet en statistisk sammenligning af de formater, der er afleveret data i. Sammenligningen har identificeret 100 forskellige formater i perioden 2011-2019. En mere detaljeret analyse af formaterne har efterfølgende vist at 95 formater af de 100 indeholder relevant data. Det store antal formater kan forklares med, at en del af de fremsendte filer har været fejlbehæftede udtræk, at systemerne hos leverandørerne til generering af rådata er ændret og endelig har en del udtræk ikke været automatiseret, hvorfor den manuelle håndtering hos teleudbyderne har introduceret forskelle i formaterne.

Hvert af de 100 dataformater afviger fra de øvrige 99 formater på mindst én af følgende måder:

- Rækkefølgen af kolonnerne varierer
- Navngivningen af kolonnerne varierer
- Antallet af kolonner varierer

Et format kan således anses som et unikt mønster (pattern), som rådata er struktureret efter. Optællingen af formater afspejler således ikke formatforskelle i *indholdet af kolonner* (f.eks. forskellige datoformater, adresseformater etc.). Antal formater opgjort på format af indholdet i kolonner vil være langt højere. Der er for eksempel identificeret 30 forskellige datoformater inden for én kolonne.

Nedenfor fremgår en oversigt over antallet af filer for hvert af de 100 identificerede formater (der kan være adskillige filer for hver rekvisition). De 30 mest hyppigt anvendte formater dækker 99,9 pct. af de fra teleudbyderne afsendte filer. De 30 formater er indlæst automatisk i forbindelse med undersøgelsen, mens øvrige formater er indlæst manuelt. De tre mest anvendte formater dækker ca. 78 pct. af de samlede filer der er modtaget, mens 53 formater kun er anvendt én gang. De 100 formater dækker således over en koncentration af filer på 30 formater og en meget lang 'hale' af formater, der bedst kan karakteriseres som meget sjældne undtagelser.



Ses der på antallet af anvendte formater for rådata per år, fremgår det af nedenstående tabel, at der i 2019 har været otte formater i anvendelse og tilsvarende i 2018. Der er over tid sket en reduktion i antallet af anvendte

formater per år, siden antallet af formater nåede sit højdepunkt i 2013 med 17 forskellige formater.

År	Antal formater for rådata i anvendelse
2019	8
2018	8
2017	9
2016	13
2015	9
2014	10
2013	17
2012	14
2011	14

Antallet af formater kompliceres yderligere da ændringer i dataformaterne historisk er forekommet uden varsel. Det medfører, at Rigspolitiets udviklere, der skal assistere en meget operativ organisation, bliver stillet i en yderst vanskelig situation. I de fleste sager anvendes teledata ikke i skarpe operative situationer, men der vil særligt i visse sager være behov for at levere data hurtigt. Dette indebærer at datakonverteringen skal være automatiseret i videst muligt omfang.

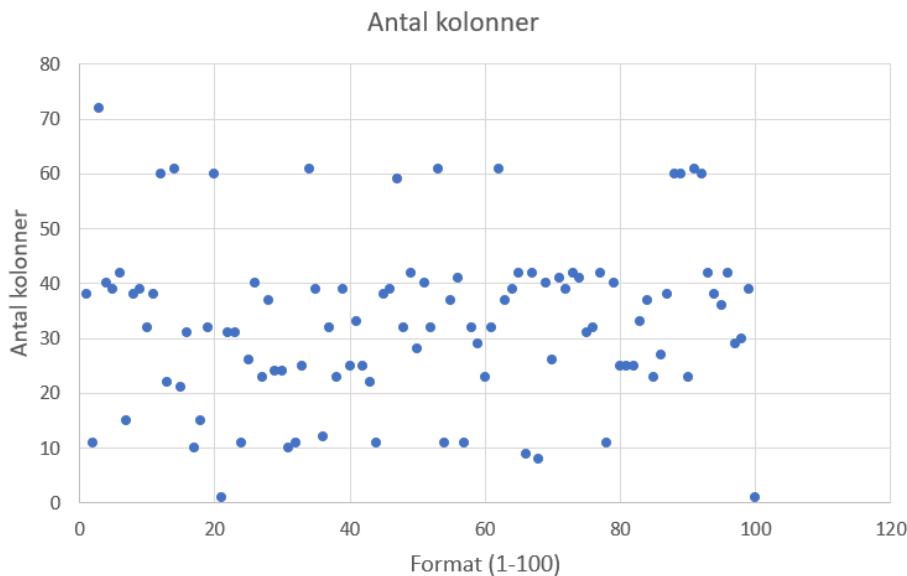
Rigspolitiets Telecenter skal vælge, om man vil acceptere ukurante dataformater med risiko for fejlfortolkning, om man (eventuelt manuelt) skal konvertere data, eller om der skal udvikles endnu en 'knopskydning' på et kompliceret IT-system.

De 30 mest anvendte formater er ligeledes opgjort per udbyder, jf. tabellen nedenfor. Én udbyder (A) har anvendt ti formater gennem hele perioden, én (B) har anvendt 17 forskellige formater, én har anvendt tre formater (C) og endelig har den sidste udbyder (D) anvendt et og samme format i perioden 2011-2019. Tabellen summer til 31, da to udbydere i en periode har anvendt samme format.

Formater	Antal formater per udbyder
Udbyder A	10
Udbyder B	17
Udbyder C	3
Udbyder D	1

Figuren nedenfor viser antallet af kolonner per format. Det fremgår, at der er en meget betydelig variation i antallet af kolonner per format, der svinger fra knap 10 til 70+ kolonner (ekskl. to formater, der hver har én

kolonne, hvilket imidlertid beror på en fejl i formatets formatering så kolonnerne ikke adskilles korrekt). Variationen i antallet af kolonner dækker over en række 'formatkategorier', som har lignende indhold og ca. samme antal kolonner. Inden for hver formatkategori er der typisk ét til to hovedformater, hvorpå langt de fleste rekvisitioner er koncentreret, og en række formatvariationer, som kun har været i anvendelse ganske få eller en enkelt gang.



Antallet af kolonner i det modtagne rådata skal ses i lyset af, at Rigspolitiets datamodel for modtagelse af rådata indeholder et specifikt antal kolonner, som dog ikke er repræsenteret i de modtagne formater. Rekvisitioner med et højere antal kolonner end forudsat i skabelonen kan være udtryk for, at Rigspolitiets Telecenter modtager mere data fra teleudbyderne end forespurgt, at der er indsat kolonneoverskrifter uden øvrig indhold, at forespurgte datakolonner er dubleret eller at der anvendes dataformat der tjener andre formål end at levere data vedrørende mastesug eller historiske teledata.

De mange afvigende datamønstre introducerer en betydelig risiko, da Rigspolitiets Telecenter programmatisk skal håndtere en stor variation af dataformater. Rigspolitiet har løbende rettet op på den programkode der har fortolket data ved modtagelsen fra teleudbyderne i takt med at dataformater og indhold har ændret sig. Variationer, der skal håndteres, kan kategoriseres i følgende hovedtemaer:

- **Forskelle i kolonnenavne**, der betyder, at konverteringen skal bruge uens betegnelser for samme kolonne, f.eks. 'tidspunkt'.
- **Forskelle i kolonnerækkefølge**, der betyder, at modtagelse og sammenligning af data på tværs af teleudbyderne kompliceres, da data skal flyttes og indplaceres på fem forskellige måder.
- **Forskelle i begreber**, der beskriver samme information, så der er behov for at programmere regler, der skal tolke indhold i kolonner, i fem variationer.
- **Manglende oplysninger om de data der sendes**, hvilket kræver programmering af regler der identificerer, hvorledes data skal fortolkes så betydningen er klar og data kan behandles korrekt.

- **Manglende kolonner**, hvilket betyder behov for programmering af regler, der fortolker indhold, for at beregne data som kunne være medsendt.
- **Manglende opdeling af data i egne kolonner**, idet der afleveres flere informationer i hver række, så der skal udvikles regler, der identificerer og opdeler data i relevante delmængder.

Grundlæggende komplicerer ovenstående forhold ved de modtagne data opgaven for Rigspolitiet og introducerer en betydelig kompleksitet og dermed potentielle risici for fejl. Håndteringen af denne kompleksitet skal ses i lyset af Rigspolitiets Telecenters omskiftelige tilværelse og et begrænset ledelsesfokus over en årrække. Rigspolitiets Telecenters nuværende medarbejdere har med begrænsede ressourcer, en omskiftelig organisation og en udfordret teknisk platform i udstrakt grad formået at håndtere kompleksiteten.

### 5.3.3 Datakvalitet for indhold

Der er foretaget en simpel analyse af, om rådata indeholder de ventede informationer for en række konkrete indholdsfelter. Analysen påviser et misforhold mellem den statistiske variation i data og den faktiske betydning af afvigelserne. En simpel statistisk analyse kan sammenlignes med et meget finmasket net, som vil finde alle afvigelser. En stor del af disse afvigelser er uden betydning for forståelsen af data. Eksempler på sådanne forskelle kan være anvendelse af '.' i stedet for ',' som tusindtals separator, ekstra mellemrum, og identifikation af fokusnummeret på hver række (efterforskerne ved godt hvilket fokusnummer de har begæret indgreb for) osv. Den kvalitative datakvalitet, dvs. datas generelle anvendelighed til formålet, er god.

Datagrundlaget består grundlæggende af to typer rekvisitioner, udvidede teleoplysninger (kaldet mastesug) og indgreb mod specifikke numre (historiske teleoplysninger). Disse to typer rekvisitioner resulterer i meget forskellige datasæt, både hvad angår indhold og mængde. Mastesug er en generel forespørgsel, der identificerer al teletrafik i et område og derfor indeholder informationer fra flere teleudbydere (der jf. ovenstående kommer i meget varierende formater) og i langt større volumen end den langt mere hyppige indsats rettet mod et enkelt nummer.

Mastesug resulterer i langt flere og mere varierede data end indgreb mod telefon eller IMEI-numre. Mastesug resulterer i massive datamængder der varierer i format pga. forskellene i teleudbydernes dataformater. Eftersom statistisk variation (herunder variation pga. forskelle i format) tolkes som lav datakvalitet, giver det et forvansket billede af datakvaliteten. Datakvaliteten fra mastesug vil alene pga. variationen i formater, blive vurderet lavere end den reelt set er. Når disse data bliver sat i forbindelse med en sag, trækker de (statistisk set) unødigt meget ned i det samlede billede af datakvaliteten på sagen.

Det giver derfor et mere reelt billede af rådatas kvalitet og betydning for sagers oplysning at vurdere kvaliteten på indgreb, der er rettet mod specifikke telefoner, idet en samlet statistik af datakvaliteten på tværs af historiske teleoplysninger og mastesug ikke vil give et retvisende billede.

Rigspolitiet har tidligere i undersøgelser og en stikprøvekontrol på et mindre antal rekvisitioner identificeret en række historiske fejl, hvor indhold mangler i rådata. Resultaterne af stikprøvekontrollen er udleveret af

Rigspolitiet til Deloitte og har indgået som del af undersøgelsens datagrundlag. Deloitte's fund vedrørende manglende indhold i rådata flugter resultater af en stikprøvekontrol foretaget af Rigspolitiet, om end frekvenser for manglende data i Deloitte's undersøgelse overvejende er lavere end de af Rigspolitiet identificerede frekvenser.

#### 5.3.4 Mastepositioner i rådata

Rigspolitiet har oprindeligt lagt data fra teleudbyderne om infrastruktur, herunder mastepositioner, celle-identifikation, celleretning og placering til grund for sagers oplysning. Det fremstår dog, at der i perioder har været systematiske fejl i de indrapporterede data for samtlige af de ovenstående parametre.

Fejlene er imidlertid i vidt omfang håndterbare og giver ikke umiddelbart grund til generel mistillid til kvaliteten af de teledata, der anvendes. En kort opsummering af fejlene og deres konsekvenser er givet nedenfor:

**Forkerte koordinatsæt.** Der findes en række forskellige standarder for angivelse af koordinater til stedfæstelse af mastens placering. Tre af de danske udbydere anvender én type koordinatsæt, mens den fjerde anvender et andet, men lignende koordinatsæt. Ingen af udbyderne skriver eksplicit i data, hvilket koordinatsæt der anvendes. Rigspolitiet anvender et tredje koordinatsæt, som anvendes i politiets øvrige systemer. Resultatet er, at de to modtagne koordinatsystemer fra teleudbyderne skal konverteres til et tredje, der anvendes af Rigspolitiet. Forskellene i de to er dog så lille, at en konvertering med den forkerte algoritme kun vil 'flytte' en mast cirka 40-100 meter. Det er en begrænset afvigelse set i lyset af, at en mast ofte har et dækningsområde på flere km<sup>2</sup> og en rækkevidde på mange km. Afvigelser i denne størrelsesorden vil i de fleste tilfælde ikke have betydning i lyset af de generelle usikkerheder, der er forbundet med lokalisering baseret på historiske teledata.

**Ombyttede koordinater.** Effekten af ombyttede koordinater er meget let at fastslå idet det vil 'flytte' masten til en position adskillige tusind km mod syd (se afsnit 5.2.4.1). Dette betyder i værste fald at oplysningerne ikke umiddelbart kan anvendes til stedfæstelse, men vil kræve at fejlen rettes inden data fortolkes. Det åbenlyse ved fejlen vil imidlertid gøre, at data ikke fejlfortolkes ved et uheld.

**Forkerte celle-koordinater og eller adresser.** Fejlen opstår oftest hvis en celle er afmonteret og genmonteret på en anden mast, uden at cellens koordinater eller adresse samtidig er blevet opdateret. Det afsløres ved at samtalen bliver registreret på celler der ligger meget geografisk adskilt. Dette er forekommet, men er ikke selvstændigt analyseret af Deloitte i forbindelse med undersøgelsen. Denne type fejl er let at gennemskue som en adressefejl på en celle. Der er en lille risiko for, at fejlen i sjældne tilfælde ville kunne have en betydning, hvis en celle er genmonteret på en nærliggende mast, således at et falsk 'mastespring' kunne have været sandsynligt.

**Forkert celle-retning.** En celle er enten omni-directional eller dækker en begrænset vinkel (langt de fleste dækker 120 grader). Hvis vinklen og dermed dækningsområdet registreres forkert af teleudbyderen, f.eks. ved ombytning af kabler, ved af- og genmontering eller lignende, kan en enhed, der kommunikerer med masten blive rapporteret i et andet område, end hvad der har været tilfældet.

#### 5.3.4.1 Ombyttede mastekoordinater i rådata

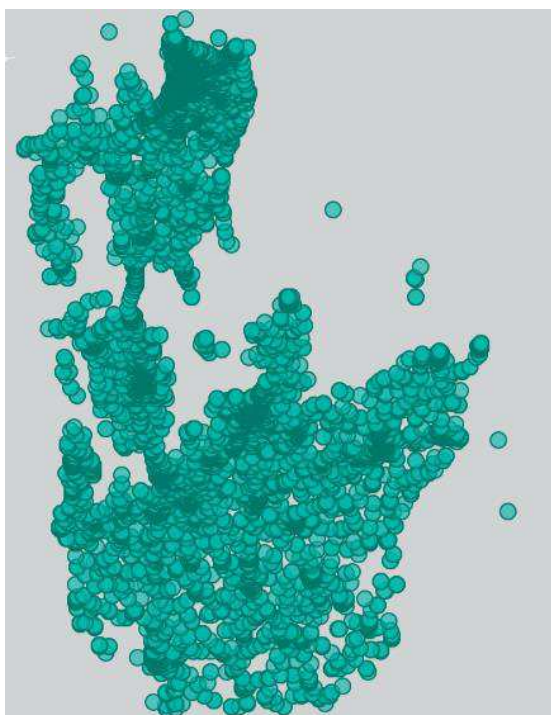
Der er foretaget en analyse af mastepositioner i rådata med henblik på at belyse datakvaliteten. Indledningsvist er de i rådata registrerede mastekoordinater omregnet fra koordinater til geografisk placering.

Koncentrationen af grønne prikker på kortet nedenfor viser mastekoordinater, hvoraf hovedparten ligger inden for Danmarks geografiske placering samt i det sydlige Sverige. Der er hertil identificeret en betydelig population af mastekoordinater mod sydøst samt en mindre population stik syd.



Populationen mod sydøst er herefter analyseret nærmere. Figuren nedenfor belyser i nærmere detaljer de koordinater, som udgør den sydøstlige population.





Der er anlagt en hypotese om, at populationen i sydøst kan være udtryk for, at der er sket en ombytning af koordinater.

For at teste dette er koordinaterne byttet om, så der foretages en spejling fra sydvest til nordøst. Denne spejling fremgår af figuren nedenfor (*transposed values*). Det fremgår, at spejlingen resulterer i en udstrækning af koordinat-datapunkter, der har en betydelig lighed med Danmarks kontur. Det bestyrker hypotesen om, at disse koordinatfejl i rådata er udtryk for, at der i forbindelse med registrering af koordinater hos teleudbydere, er sket en ombytning af koordinaterne.



#### 5.3.4.2 Mastekoordinater over tid i rådata

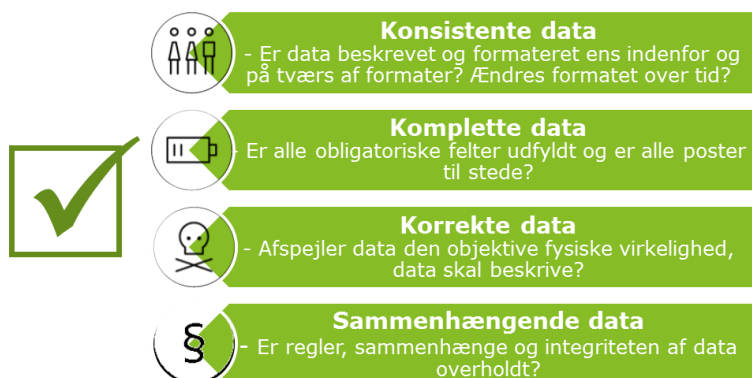
Det er fra et datakvalitetsperspektiv ligeledes belyst, om registreringer vedrørende mastepositioner er konsistente i rådata over tid. Konkret er der foretaget en stikprøvetest af konsistens i rådata for mastekoordinater i en større provinsby i perioden. Der er i stikprøven identificeret afvigelser i mastepositioner over tid på op til 200 meter.

Afvigelser i denne størrelsesorden vil i de fleste tilfælde ikke have betydning i lyset af de generelle usikkerheder, der er forbundet med geografisk lokalisering ved brug af teledata. Navnlig i tættere bymæssig bebyggelse, hvor celler generelt dækker et mindre område, kan selv mindre forskydninger dog i specifikke situationer potentielt have betydning.

#### 5.4 Introduktion til dimensioner i sammenligning af rådata og konverteret data

Undersøgelsen belyser herefter, hvorvidt konverteringen af de rådata, der tilsendes Rigspolitiets Telecenter fra teleudbyderne, introducerer fejl i datakvaliteten. I det følgende gennemgås de kriterier, der vurderes i undersøgelsen.

Nedenstående figur beskriver de dimensioner, der indgår i begrebet datakvalitet. Deloitte anvender en sammensat definition af datakvalitet, eftersom det i praksis, er muligt for data at indeholde flere typer af fejl. Disse forskellige typer fejl identificeres ved hjælp af forskellige teknikker, ligesom det ofte kræver forskellige tiltag at afhjælpe eller forhindre fejl i data. Typerne af fejl, appliceret på historiske teledata, er gennemgået i det følgende.



##### 5.4.1 Konsistente data

Undersøger om data er formateret konsistent på tværs af tid, teleudbyder og konvertering. Som det beskrives i afsnit 5.2.2, introducerer manglende konsistens i data væsentlige risici i konverteringen og fortolkningen af data.

For konformitet testes konkret, hvor mange forskellige formater data optræder i over dataværdikæden.

##### 5.4.2 Komplette data

Undersøgelsen tester for det første, om data er komplette. Med komplette menes, at alle obligatoriske felter skal være udfyldt, og alle poster skal være til stede. Hvis der mangler aktiviteter (rækker) i et datasæt, uanset om det er i rådata eller udsendte data, er data ikke komplette. For kompletthed testes konkret:

- **Antallet af rækker i modtagne og konverterede datasæt.** Testen belyser, om der er sket et datatab i konverteringen.

##### 5.4.3 Korrekte data

Undersøgelsen tester for, om de data der er modtaget fra teleudbyderne, er transformeret i overensstemmelse med Rigspolitiets dokumenterede

standard. Dermed testes, om de reelle data stemmer overens med de forventede data.

- **Direkte sammenligning af dataindhold i poster.** Testen belyser for alle dataposter, om der er fejl i de kolonner, hvor dataindhold i rådata og konverteret data forventes at være konformt, f.eks. vedrørende opkaldstype, startdato og tid, IMEI-nummer, telefonnummer etc.

#### 5.4.4 Sammenhængende data

Sammenhængen handler om, at data i ét felt er betinget af data i et andet felt. Er det tilfældet, skal disse afhængigheder overholdes. Visse datafelters 'lovlige' værdi er direkte afhængige af værdien af et andet felt. Eksempelvis er der 'krav' om, at en samtale har en udstrækning i tid, mens en sms ikke spænder over en periode. Der kan også være regler for, hvordan data fra forskellige tabeller bindes sammen, f.eks. skal en celle have en adressekoordinat og en retning.

Hvis disse logikker ikke er overholdt skades datas sammenhæng. Konkret testes følgende:

- **Direkte sammenligning af dataindhold i poster med opslag.** Testen belyser for alle dataposter, om der er fejl i de kolonner, hvor dataindholdet afspejler et automatiseret opslag. F.eks. hvor fokusnummeret hentes fra filnavnet i filen med rådata.
- **Direkte sammenligning af dataindhold i felter med konverteret data.** Testen belyser for alle dataposter, om der er fejl i de kolonner, hvor der er foretaget datatransformationer, f.eks. om der er fejl i konverterede mastepositioner.
- **Sammenligning af afledte værdier.** Her sammenlignes f.eks. om typen af teletjeneste (Voice, SMS, MMS, SMS Kvittering, osv.) er korrekt udledt af de modtagne rådata.

### 5.5 Resultat af dataanalyse af rådata sammenholdt med konverterede data

Der er gennemført en sammenligning af rådata, Rigspolitiets konvertering af rådata og Deloitte's uvildige konvertering af rådata, med henblik på at identificere fejkilder i konverteringen. Undersøgelsen er gennemført i henhold til metoden beskrevet i afsnit 4.4.

Det bemærkes, at konverteret data består af tre separate rapporter, hhv. en sessionsrapport, en samlerapport og en sumrapport. Det er samme data, der ligger til grund for de tre rapporter. Der er en lille forskel i måden, de tre rapporter laves på, hvilket i få tilfælde i en kortere periode har påvirket samlerapporten, så der ikke har været overensstemmelse med sessionsrapporten. Derfor gennemføres tests på disse to rapporter.

#### 5.5.1 Antal rekvisitioner

Afsættet for sammenligningen er de rekvisitioner, hvor der findes både rådata og konverteret data. I de tilfælde, hvor der alene foreligger rådata, og det ikke har været muligt at identificere det samme data i konverteret udgave, er det ikke muligt at belyse, om konverteringen er foretaget korrekt, og dermed om der er fejkilder i konverteringen.

Det fremgår af tabellen nedenfor, at afsættet for sammenligningen er de 24.028 rekvisitioner, hvor der er identificeret både rådata og konverteret data. Det udgør knap 58 pct. af de tilgængelige rekvisitioner for rådata. Af disse er der 19.386, hvor der er reelt teledataindhold i filerne, svarende til 46 pct. Disse rekvisitioner vedrører 5.551 sager hvor der er anvendt teledata, opgjort på baggrund af unikke journalnumre.

Rekvisitioner	Antal	Procent hvor både rådata og konverteret data kan forefindes
Rådata	41.842	-
Konverteret data	24.245	57,9 pct.
- Heraf hvor der findes både rådata og konverteret data	24.028	57,4 pct.
- Heraf hvor der findes både rådata og konverteret data, og er indhold	19.386	46,3 pct.

Det er vurderingen i Rigspolitiets Telecenter, at filer uden indhold skyldes, at man tidligere har sendt rekvisitioner til samtlige teleudbydere, og at disse returnerede tomme filer, såfremt de ikke havde registreringer på det forespurgte nummer. Disse rådata og konverteret data er frasortet i de efterfølgende sammenligninger, der således tager afsæt i de 19.386 rekvisitioner, hvor der er både rådata og konverteret data og er indhold.

## 5.6 Overensstemmelse mellem antal rækker i rådata og konverteret data

Det er belyst, om der på rækkeniveau er overensstemmelse mellem antal rækker i Rigspolitiets konverterede data og Deloittes uvildige konvertering. Dvs. hvorvidt der mangler rækker i det konverterede data, som er tilsendt politikredsene mv., eller om der omvendt er flere rækker i konverteret data end rådata. Analysen dækker de rådata og konverterede data, hvor der er muligt at identificere hver række på en entydig måde (se 5.6.1.1). I sammenligningen af antal rækker fokuseres der på den såkaldte sessionsrapport i det konverterede data, da det er denne konvertering, der skal indeholde det samlede rådata i konverteret format.

Sammenfattende kan det på baggrund af analysen af antal rækker i rådata sammenholdt med konverterede data for sager, konkluderes, at Deloittes undersøgelsen i væsentlighed bekræfter de resultater, som Rigspolitiets interne undersøgelser og stikprøvekontroller har afdækket. Der er identificeret rækketab i ca. 5,8 pct. af de undersøgte rekvisitioner, hvilket er en lavere andel end Rigspolitiet har identificeret i deres interne screening. Rækketabet påvirker 1.131 rekvisitioner i undersøgelsesperioden.

### 5.6.1.1 Metode til analyse af antal rækker i rådata og konverteret data

For at sammenligne to rækker i en tabel er det nødvendigt at kunne identificere hver række på en entydig måde. Det gøres ved hjælp af en såkaldt nøgle, der skal være unik for hver række. Vi anvender nøgler til at

identificere objekter hver eneste dag ofte uden at reflektere over det: nummerplader, CPR-numre og telefonnumre er alle eksempler på nøgler, der har til formål at adskille objekter, som ellers ville være umulige umiddelbart at skelne, f.eks. flere tilsyneladende ens biler (af samme mærke, farve, årgang og model).

Hvis der ikke findes en naturlig nøgle må man, for at sammenligne data konstruere en sammensat nøgle. Det vil sige, at kombinationen af flere felter tilsammen kan anvendes til at identificere en række som unik. I tilfældet med historiske teledata anvendes en sammensat nøgle til at identificere og koble en række i rådata med en række i de konverterede data. Det er nødvendigt, fordi der historisk ikke er blevet medsendt en nøgle for hver række historisk teledata fra teleudbyderne, ligesom Rigspolitiets Telecenter ikke har defineret en nøgle ved modtagelse af rådata.

Betingelsen for at et felt kan bruges i en sammensat nøgle er, at feltet altid indeholder data og aldrig ændrer indhold. Hvis det ikke er tilfældet, kan nøglerne ikke sammenlignes. I forhold til teledata begrænser det antallet af kandidater sig til fire felter: DatoTid, Liid<sup>1</sup>, rekvisitionsnummer og teleudbyder. 'DatoTid' identificerer dato og tidspunktet for anvendelsen af en telecelle med en præcision på et sekund. Imidlertid er teleudbyderen, rekvisitionen og Liid konstant for hver fil. Det betyder, at for hver række, der er modtaget fra en given teleudbyder, er det reelt set kun dato og tidspunktet, der kan anvendes til at differentiere mellem rækkerne.

Oftest er det tilstrækkeligt, men i to tilfælde er det ikke:

- Hvis en bruger anvender sin mobil til to forskellige tjenester samtidig, kan dato og tidspunkt for de to aktiviteter overlapse, hvorfor den sammensatte nøgle ikke længere er unik.
- Hvis der foretages et mastesug, hvor potentielt hundreder af brugere anvender en teleudbyders mast samtidig, vil der ofte forekomme flere aktiviteter inden for samme sekund.

I begge disse tilfælde er det ikke muligt entydigt at sammenligne rådata og konverterede data række for række. En maskinel sammenligning vil resultere i, at alle kombinationer af unikke nøgler sammenlignes, hvilket vil resultere i en eksponentiel mængde af 'falske' fejl. Derfor er undersøgelsen begrænset til de 48.713.348 (48,7 mio.) rækker, der kan identificeres ved hjælp af den sammensatte nøgle. Dette er ud af et antal på cirka 297 millioner rækker. De rækker, hvor det ikke er muligt at identificere en unik nøgle, er langt overvejende rækker fra mastesug, hvilket skal ses i lyset af forklaringen ovenfor.

#### 5.6.1.2 Resultater af analyse af rækketab

Der er i sammenligningen af rådata og konverterede data identificeret 18.047 unikke rekvisitioner, hvor der er overensstemmelse i antallet af rækker og 1.339 unikke rekvisitioner, hvor der ikke er overensstemmelse, jf. nedenstående tabel. De 1.131 rekvisitioner, hvor der er identificeret rækketab, udgør ca. 5,8 pct. af det samlede antal rekvisitioner med match mellem rådata og konverteret data.

---

<sup>1</sup> Lawful Interception Identifier, svarende til indgrebs kendelse.

<b>Antal rækker (records)</b>	<b>Antal unikke rekvisitioner med overensstemmelse</b>	<b>Antal unikke rekvisitioner uden overensstemmelse</b>
Total antal	18.047	1.339
Heraf flere rækker i rådata end konverteret data (sessionsrapport)	N/A	1.131
Heraf færre rækker i rådata end konverteret data (sessionsrapport)	N/A	208

Det ses, at rekvisitioner med uoverensstemmelse i antallet af rækker fordeler sig over 1.131 rekvisitioner, hvor der er identificeret manglende rækker i konverteret data, og 208 rekvisitioner hvor der er identificeret flere rækker i konverteret data i forhold til rådata. Færre rækker i konverteret data end rådata er et udtryk for et datatab, mens et højere antal rækker i konverteret data sandsynligvis vil være et udtryk for en dublering i forbindelse med konverteringen. Det er datatabet, som kan have betydning for straffesagen, hvorfor datatab belyses yderligere.

Af figuren nedenfor fremgår antallet af rekvisitioner per år, hvor der er flere rækker i rådata end i konverteret data (sessionsrapport), og hvor der altså er sket et rækketab i forbindelse med konverteringen af rådata. Det fremgår, at divergensen er koncentreret i særligt 2016, hvor der er identificeret 361 rekvisitioner med rækketab. Herudover er der særligt identificeret rækketab i 2012-2013 samt i 2015 og 2017. Sættes antallet af rekvisitioner med rækketab i forhold til det samlede antal rekvisitioner per år fremgår det, at der procentuelt har været størst rækketab i 2012, og der generelt over tid er sket en reduktion i procentandelen af rekvisitioner, der er påvirket af rækketab.

<b>År</b>	<b>Antal rekvisitioner med flere rækker i rådata end konverteret data (sessionsrapport)</b>	<b>Total antal rekvisitioner per år</b>	<b>Procent rekvisitioner <u>uden</u> rækketab per år</b>
2019	8	2.668	99,2
2018	99	4.678	97,5
2017	131	4.122	96,7
2016	361	2.550	84,4
2015	108	1.707	93,6
2014	45	1.385	87,9
2013	143	961	85,0
2012	169	823	79,3
2011	67	492	85,6
Total	1.131	19.386	94,2

Rækketabet påvirker samlet set 1.131 rekvisitioner i undersøgelsesperioden svarende 4,5 mio. tabte rækker. Rækketabet påvirker overvejende rekvisitioner vedrørende historiske masteoplysninger (858 rekvisitioner), mens der i mindre omfang er tale om rekvisitioner vedrørende mastesug (273 rekvisitioner). Opgøres rækketabet på antal tabte rækker kan de 1,5 mio. rækker henføres til mastesug, mens de 3 mio. rækker kan henføres til historiske teleoplysninger. Mastesug anvendes overvejende i forbindelse med efterforskning af sager, mens teleoplysninger i højere grad også anvendes i forbindelse med anklagemyndighedens forelæggelse af sager for retten.

Det øgede rækketab i 2016 skyldes bl.a. en af Rigspolitiet identificeret fejl i et delsystem, hvor en timerfunktion betød at den konverterede fil blev afsendt uden fuldstændighedskontrol. Hvis konverteringen tog mere end 60 minutter, hvilket kan forekomme ved mastesug, blev filen afsendt inden den var fuldt indlæst. Timerfunktionen er per 8. marts 2019 ikke længere i drift. Der er i 2019 identificeret 8 rekvisitioner med rækketab, hvoraf 7 rekvisitioner har et rækketab på over 100 rækker. Af disse rekvisitioner ligger 6 før 8. marts 2019, mens de to resterende ligger i hhv. april og juni 2019. De to berørte rekvisitioner efter 8. marts 2019 blev identificeret i politikredsenes interne manuelle kvalitetskontrol. For de 8 rekvisitioner er gældende, at 7 angår historiske teleoplysninger, mens én angår mastesug.

Rekvisitioner med flere rækker i rådata end i konverteret data er nedbrudt yderligere ift. rækketabets størrelse, jf. nedenstående tabel. Analysen tager udgangspunkt i rækker, hvor der er en gyldig dato på rækken. Det skyldes, at visse af de 30 dataformater inkluderer et antal tomme linjer under kolonneoverskrifterne. Disse rækker har ikke betydning og indgår derfor ikke i oversigten.

Det ses, at der i 142 tilfælde, svarende til 13 pct., er tale om en divergens på én række, i 261 tilfælde mangler 2-10 rækker (23 pct.), i 275 tilfælde mangler 11-100 rækker (24 pct.), mens der i 453 tilfælde er identificeret konverterede datasæt, der mangler mere end 100 rækker ift. konverteret data (40 pct.). Omfanget af rækketab skal ses i lyset af antallet af rækker i en rekvisition. Det gennemsnitlige antal rækker er til sammenligning ca. 3.900 rækker, mens medianen er ca. 400 rækker (høje rækkeantal i mastesug trækker gennemsnittet op). Der ses samtidig en meget betydelig variation i antallet af rækker i en rekvisition.

Omfang af rækketab (records)	Antal unikke rekvisitioner med flere rækker i rådata end konverteret data	Procent af rekvisitioner med flere rækker i rådata end konverteret data
Total antal	1.131	100
Rækketab på 1 række	142	13
Rækketab på 2-10 rækker	261	23
Rækketab på 11-100 rækker	275	24
Rækketab på >100 rækker	453	40

Telecenteret har tidligere gennemført en screening af sager fra 2018 for at belyse tab af rækker i konverteringen. Denne undersøgelse har identificeret knap 9 pct. sager med en uoverensstemmelse mellem antal rækker i rådata

og konverteret data. Det udgør en højere andel af afvigelser end de 5,8 pct. rekvisitioner med rækketab, der identificeres af Deloitte for perioden 2011-2019.

I tabellen nedenfor er nedbrydningen af rækketabenes størrelse ligeledes fordelt per år i undersøgelsens periode. Det fremgår, at rækketab overvejende er koncentreret i 2016 (361 rekvisitioner med rækketab). De største rækketab (rækketab >100 rækker) er koncentreret i perioden 2016-2018 med hhv. 109, 70 og 77 rekvisitioner med rækketab over 100 rækker.

	2011	2012	2013	2014	2015	2016	2017	2018	2019
<b>Total antal</b>	67	169	143	45	108	361	131	99	8
<b>Rækketab på 1 række</b>	5	18	23	7	12	61	9	7	0
<b>Rækketab på 2-10 rækker</b>	17	34	49	6	16	105	28	5	1
<b>Rækketab på 11-100 rækker</b>	25	52	39	11	28	86	24	10	0
<b>Rækketab på &gt;100 rækker</b>	20	65	32	21	52	109	70	77	7

Fejlkilden vedrørende manglende rækker i konverteret data er tidligere identificeret af Rigspolitiet, jf. ovenstående, herunder på baggrund af henvendelse fra udvalgte politikredse i november 2018 og februar 2019. Rigspolitiet vurderer, at en række forhold kan have bidraget hertil:

- Manglende konvertering af data vedrørende såkaldte 'særlige tjenester', herunder bl.a. viderestilling af opkald. Dette er en datatype, som udelukkende leveres af en enkelt teleudbyder. I en periode fra 2016-2018 oplyser Rigspolitiets Telecenter, at konverteringen ikke har taget højde for denne datatype, hvorfor der er opstået rækketab i forbindelse hermed. Ovenstående analyse understøtter denne årsagsforklaring, idet rækketab forekommer hyppigst netop hos denne udbyder.
- En sammensat it-systemfejl, som vurderes at bestå i en kombination af en timer-funktion til udsendelse af filer (omtalt ovenfor), som kan have medført udsendelse af ukomplette filer, samt en opdatering i it-systemet, der har medført at sektioner af filer er blevet sprunget over i konverteringen.

Det bemærkes, at den af Rigspolitiet identificerede fejl, hvor konverteret data er blevet afsendt til politikredse mv. inden alle rækker har været konverteret, på grund af en timer-funktion for afsendelse, ikke kan belyses fuldstændigt på baggrund af den anvendte analysemetode. Såfremt kredse mv. efterfølgende er blevet tilsendt den fuldt konverterede fil, vil denne være indgået i analysens datagrundlag og efterfølgende sammenligning desuagtet, at kreds mv. ikke nødvendigvis faktisk har anvendt den fuldt konverterede fil i efterforskningen.



## 5.7 Sammenligning af *dataindhold* i rådata og konverteret data i sager med brug af historiske teleoplysninger

Dette afsnit sammenligner *dataindholdet* i de rekvisitioner, hvor der både findes rådata og konverteret data. Sammenligningen er foretaget på niveau af det enkelte felt i den enkelte række, som sammenholdes på tværs af rådata og konverteret data. Dermed er analysen baseret på de rækker, som der kan matches på tværs af de to datasæt, hvilket udgør ca. 48,7 mio. rækker.

I afsnittet er behandlet en datamængde svarende til 5.551 journalnumre (sager). Det er gældende for alle identificerede afvigelser mellem rådata og konverteret data, at det på baggrund af undersøgelsens metode er muligt at spore uoverensstemmelser i konverteringen ned på niveau af den enkelte rekvisition og sag. Disse oplysninger stilles til rådighed for politiet i forlængelse af undersøgelsen og vil kunne anvendes fremadrettet af politikredse mv.

Samlet set identificerer undersøgelsen en række konverteringsfejl på feltniveau, hvor der i perioden 2011-2019 er sket en række forskelligartede konverteringsfejl, som optræder i varierende omfang. Der er identificeret et meget begrænset antal konverteringsfejl vedrørende f.eks. celleretning samt A- og B-numre, mens der f.eks. er identificeret et højere antal uoverensstemmelser for bl.a. tjenestetype. Ses der på antallet af rækker med uoverensstemmelse mellem rådata og konverteret data som andel af det totale antal rækker, fremgår det, at der overvejende er tale om meget små andele, mens det alene er for varighed og IMEI-numre at konverteringsfejl påvirker en større andel af de analyserede rækker. Der er i al væsentlighed tale om resultater, der flugter med de fund, som Rigspolitiets Telecenter har identificeret i interne undersøgelser og stikprøvekontrollen og generelt i lavere frekvenser for perioden 2011-2019 end foreløbigt identificeret af Rigspolitiet for en kortere periode (2018).

### 5.7.1 Sammenligning af *dataindhold*

Sammenligningen af *dataindhold* belyser overensstemmelsen mellem indholdet på feltniveau i matchende rækker. Nedenfor fremgår resultatet af en felt-til-felt sammenligningen mellem konverteret data og rådata i form af antal rekvisitioner *uden* overensstemmelse for centrale felter. Hertil fremgår antallet af rækker uden overensstemmelse som en andel af det totale antal rækker i feltsammenligningen.

Det fremgår, at der i varierende grad er identificeret uoverensstemmelser på feltniveau, og disse gennemgås per felt nedenfor. Det ses, at der er betydelig forskel på forekomsten af konverteringsfejl målt som antal rækker påvirket af en given fejl i lyset af det totale antal analyserede rækker (48,7 mio. rækker i alt i de i alt 19.386 rekvisitioner med både rådata og konverterede data med indhold). Forekomsten varierer fra at påvirke opkaldets varighed i 33 pct. af rækkerne til betydeligt lavere procentsatser for f.eks. mastekoordinater. Tilsvarende varierer betydningen af en konverteringsfejl afhængig af feltets indhold og fejlens karakter. En meget betydelig andel af de identificerede konverteringsfejl vurderes uden praktisk betydning, mens andre kan have betydning afhængig af situationen. Oversigten over konverteringsfejl i tabellen herunder, skal derfor ikke læses alene, men ses i kontekst af forklaringerne i de efterfølgende afsnit.

I gennemgangen nedenfor er konverteringsfejlenes potentielle betydning kommenteret baseret på et analytisk perspektiv. Deloitte har ikke belyst betydningen af de identificerede konverteringsfejl i et strafferetligt perspektiv. Undersøgelsens fund, herunder koblingen af specifikke konverteringsfejl til rekvisitionsnumre og dermed sager (opgjort som journalnumre), stilles til rådighed for politiet i forlængelse af undersøgelsen og vil kunne anvendes fremadrettet af politi og anklagemyndighed.

<b>Feltindhold</b>	<b>Rækker uden overensstemmelse som pct. af total række i feltsammenligning</b>
Tjenestetype	2,0
Varighed	33,3
A-nummer	0,0
B-nummer	0,0
C-nummer	0,0
Startmast	1,5
- Heraf koordinat	1,2
- Heraf celleretning	0,3
Slutmast	0,7
- Heraf koordinat	0,7
- Heraf celleretning	0,0
IMEI	19,4
Fokus ABC	6,9

I det følgende gennemgås afvigelser i forhold til de enkelte felters indhold. Det skal bemærkes, at flere af afvigelserne på de enkelte felter kan optræde på samme rekvisition. Derfor er det ikke muligt at addere de nedenfor nævnte afvigelser i forhold til at afgøre hvor mange rekvisitioner som er påvirket af konverteringsfejl.

#### **5.7.1.1 Sammenligning af dataindhold – tjenestetype**

Tjenestetypen er et felt der angiver, om en række indeholder aktivitet vedrørende tale, sms eller internettjenester. Der er identificeret 8.037 rekvisitioner, hvor der er en afvigelse mellem opkaldstype af en aktivitet i rådata og konverteret data. Samlet set er der tale om 2 pct. af de i cirka 48,7 millioner rækker, der er sammenlignet række for række.

Flere af konverteringsfejlene har mere karakter af simplificeringer og opsummeringer end af meningsforstyrende fejl. Teleudbyderne differentierer deres tjenestetyper i langt højere grad end en efterforskning typisk vil behøve, hvorfor 'SMS Kvittering' typisk vil blive oversat til 'SMS', hvilket vil fremstå som en fejl ved en direkte sammenligning. Dette er

dokumenteret og er gjort med overlæg. Dertil kommer, at flere af teleudbyderne ikke eksplicit oplyser, hvilken tjenestetype en given aktivitet hører under. Det er information der skal afledes ved hjælp af en forretningsregel, der skal fortolke teleudbydernes interne produktkode. Denne afkodning er uhyre følsom for ændringer i produktkoder, tegntabeller og generel formatering af de felter, der eksporteres til Rigspolitiet.

Specielt er der en diskrepans mellem observationerne af antallet af rækker med tjenestetypen opkald (voice) og tjenestetypen viderestilling på 3.890 rekvisitioner. Af disse afvigelser mellem rådata og konverteret data udgøres størstedelen – 1.354 rekvisitioner – af en konverteringsfejl, hvor droppet kald bliver til opkald (droppet kald er en betegnelse for når et opkald tabes af netværket). I tillæg er der identificeret en række andre konverteringsfejl, hvor der ligeledes sker en ændring af en tjenestetype til en beslægtet tjenestetype. Hertil er der identificeret et mindre antal rekvisitioner, hvor rådata ikke har indhold i feltet tjenestetype, men hvor der i konverteret data fremgår en tjenestetype.

Rigspolitiet har ligeledes identificeret en række konverteringsfejl af denne type, herunder at opkaldsforsøg ændres til opkald, alarmopkald ændres til opkald, sms ændres til opkald, hvis aktivitet er foregået i udlandet, droppede opkald eller anden aktivitet ændres til opkald, sms kvittering ændres til sms, droppet sms ændres til sms og viderestilling ændret til opkald. Deloitte's undersøgelse bekræfter således i al væsentlighed de fund, som er gjort i Rigspolitiets egne foreløbige undersøgelser, samt identificerer yderligere variationer af ændringer i tjenestetype.

Fælles for disse fejl omkring skrift i tjenestetype er, at de ofte vil være af mindre eller ingen betydning, herunder fordi de øvrige oplysninger typisk fremgår korrekt af den enkelte række. Hvor opkaldsforsøg eller droppet kald ændres til opkald, vil det fremstå som om, at en enhed har været i kontakt med en anden enhed, selvom dette forsøg på kommunikation mislykkedes. I disse tilfælde vil det imidlertid kunne udledes af feltet varighed, at der ikke har fundet et faktisk opkald sted, da et opkaldsforsøg vil have en varighed på nul. Denne fejl vurderes derfor ikke umiddelbart at have praktisk betydning.

#### **5.7.1.2 Sammenligning af dataindhold – varighed**

Varighed angiver, hvor lang tid kommunikation mellem to enheder har været ved. Ikke alle tjenestetyper har en varighed, herunder sms, ligesom varighed ved internettjenester er behæftet med usikkerhed.

Der er for varighed identificeret 4.869 rekvisitioner, hvor der er en afvigelse mellem varigheden af en aktivitet i rådata og konverteret data. Det er en hyppigt forekommende fejl, som er identificeret i 33 pct. af rækkerne i feltsammenligningen. Generelt er der langt overvejende – i 96 pct. af tilfældene – tale om konverteringsfejl på rekvisitioner af tjenestetypen internet, konkret 4.698 rekvisitioner med afvigelser. Dette er en kendt afvigelse, der skyldes at der siden 2016 fejlagtigt ikke er registreret tid på tjenestetypen internet. Hertil er der identificeret 157 afvigelser i varighed på opkald, samt et meget begrænset antal afvigelser på en række andre tjenestetyper.

Rigspolitiet har ligeledes identificeret konverteringsfejlen vedrørende varighed for internet, ligesom der er set eksempler på, at varighed er forskellig på timeniveau, så der er lagt en eller flere hele timer til en aktivitet's varighed.

Man skal generelt være varsom med at tillægge varigheden på internetsessioner værdi. Det skyldes, at en internetsession kan fortsætte selv om enheden ikke aktivt benyttes af brugeren. At der for en enhed er registreret en internetsession på f.eks. 3.600 sekunder behøver derfor ikke betyde, at enheden har været på internettet i alle 3.600 sekunder. Det kan også være et udtryk for en internetsession der er startet op, anvendt kortvarigt og ikke lukket ned igen.

Er der tale om fejlkonvertering af varigheden af en telefonsamtale, kan det ikke udelukkes, at det kan have betydning. Fejlkonverteringen ændrer dog ikke ved de øvrige felters rigtighed, herunder at to enheder har kommunikeret med hinanden. Derfor vil konverteringsfejlen alene have betydning, såfremt selve længden af en kontakt mellem to enheder tillægges betydning.

#### **5.7.1.3 Sammenligning af dataindhold – A-nummer**

A-nummeret er en betegnelse for det telefonnummer, der har foretaget et opkald, sendt en besked eller tilgået internettet. Der er identificeret 213 rekvisitioner, hvor der er en uoverensstemmelse mellem et numerisk A-nummer i rådata og konverteret data. I lyset af antallet af analyserede rækker er der tale om en type fejlkonvertering med en ekstremt sjælden forekomst (under 0,0 pct. af de analyserede rækker).

Konverteringsfejl vedrørende A-nummer består i en række forskelle, der umiddelbart er svært kategoriserbare. Herunder er der identificeret en konverteringsfejl, hvor A-numre bliver afrundet, hvis det har mange cifre. Afrundingen af A-numre er ligeledes identificeret af Rigspolitiet. Der er tale om numre bestående af mere end 15 cifre. Et telefonnummer kan imidlertid ikke være mere end 15 cifre. Såfremt det er tilfældet, vil der altså ikke være tale om et gyldigt telefonnummer. I de få tilfælde, hvor konverteringen har resulteret i et manglende A-nummer vil det være åbenlyst, at der mangler data, idet kommunikation forudsætter en initierende part. Det vil i disse tilfælde være muligt at finde det manglende A-nummer i rådata.

#### **5.7.1.4 Sammenligning af dataindhold – B-nummer**

B-nummeret er en betegnelse for det telefonnummer, der har modtaget et opkald, modtaget en besked eller tilgået internettet. Der er her identificeret 451 rekvisitioner, hvor der er en uoverensstemmelse mellem B-nummer i rådata og konverteret data.

Herunder er der identificeret en konverteringsfejl, hvor B-nummeret har fået fjernet foranstillede nuller eller hvis nummeret er blevet skrevet i videnskabelig notation. Denne konverteringsfejl i B-nummeret medfører, at der har været angivet et ukorrekt nummer på den ene part i kommunikation mellem to enheder.

Hertil er der identificeret 49 tilfælde, hvor B-nummeret er tabt i forbindelse med konverteringen. I disse tilfælde vil det ligeledes være åbenlyst, at der mangler data, idet kommunikation forudsætter en modtagende part. Det vil i disse tilfælde være muligt at finde det manglende B-nummer i rådata.

#### **5.7.1.5 Sammenligning af dataindhold – C-nummer**

C-nummeret er en betegnelse for det telefonnummer, der eventuelt er viderestillet til. Der er her identificeret 510 rekvisitioner, hvor der er en uoverensstemmelse mellem C-nummer i rådata og konverteret data.

Konverteringsfejl vedrørende C-nummer består i en række forskelle, der umiddelbart er svært kategoriserbare. Der er identificeret tre tilfælde, hvor C-nummeret er tabt i forbindelse med konverteringen.

Hvor et C-nummer i konverteringen er forvansket, vil det, afhængig af at der af konverteret data fremgår et meningsfuldt nummer, kunne fremstå som om, at en given enhed har viderestillet til en anden enhed, end det faktisk har været tilfældet. I de tre tilfælde, hvor C-nummeret er tabt, vil der være en enhed, som ikke er blevet sat i forbindelse med kommunikation, som den reelt har taget del i.

#### **5.7.1.6 Sammenligning af dataindhold – startmast**

Startmasten angiver den mast, som en given enhed opnår forbindelse til ved initiering af kommunikation. Hver mast er identificeret med en koordinat, angivet i et koordinatsystem. En enhed kommunikerer med mobilnetværket via celler, jf. rapportens sektion 3. En celle har typisk en dækningsvinkel på 120 grader og peger i en bestemt retning. Ved initiering af kommunikation registreres koordinaterne på den anvendte mast og cellens retning.

Der er identificeret 586 rekvisitioner, hvor der *enten* er sket en fejl i konverteringen af koordinater eller celleretning på startmasten. Heraf er der identificeret 461 fejlkonverteringer af koordinat på startmasten og 156 rekvisitioner med fejl i konverteringen af celleretning. Et mindre antal rekvisitioner indeholder fejl af begge typer, hvorfor summen af de to fejltyper summerer til mere end 586.

Fejl i koordinater og celleretning ændrer ikke ved, at en enhed er blevet registreret på en given celle, hvilket inden for de usikkerheder, der er beskrevet i sektion 6, giver en indikation af enhedens lokalisering. En fejl i celleretning kan dog potentielt have medført, at enhedens placering i cellens dækningsområde er blevet fejlfortolket, hvilket kan have en betydning. Størrelsen på cellers dækningsområde kan variere betydeligt. Hvor en enhed opnår forbindelse til en celle med et stort dækningsområde (f.eks. på landet, hvor der er længere mellem master), kan fejlen potentielt have større betydning, end i byer, hvor afstanden mellem masterne er kortere.

Afsnit 5.7.2 indeholder en detaljeret gennemgang af konverteringsfejl vedrørende mastekoordinater, der ligeledes er en af Rigspolitiet kendt fejl.

#### **5.7.1.7 Sammenligning af dataindhold – slutmast**

Slutmasten angiver den mast, som en given enhed har forbindelse til ved afslutning af kommunikation. Det er ikke alle tjenestetyper, der genererer en registrering af en slutmast, herunder sms. Der er identificeret 412 rekvisitioner, hvor der enten er sket en fejl i konverteringen af koordinater eller celleretning på slutmasten. Af disse er 385 rekvisitioner omfattet af en konverteringsfejl vedrørende mastekoordinat, mens 26 er omfattet af en konverteringsfejl vedrørende celleretning. Et mindre antal rekvisitioner indeholder fejl af begge typer, hvorfor summen af de to fejltyper summerer til mere end 412.

Afsnit 5.7.2 indeholder jf. ovenstående en detaljeret gennemgang af konverteringsfejl vedrørende mastekoordinater, mens fejl i konvertering af celleretning behandles i foregående afsnit.

#### **5.7.1.8 Sammenligning af dataindhold – IMEI-nummer**

En mobilenhed har en unik identifikationskode, der kaldes IMEI. Der er her identificeret 2.043 rekvisitioner, hvor der er en uoverensstemmelse mellem IMEI-nummer i rådata og konverteret data. Der er tale om en fejlkonvertering, der er forekommende i ca. 19,4 pct. af det samlede antal analyserede rækker.

Der er identificeret en række fejl vedrørende IMEI-numre, herunder tab af IMEI-numre i konverteringen, visning af IMEI-numre i forskelligt format og en fejl, hvor de sidste to tal i IMEI-nummeret afrundes til hele nærmeste tier, uden at der dog tabes cifre. Der er herunder identificeret et antal rekvisitioner med tab af IMEI-nummer og 1.792 rekvisitioner hvor IMEI-nummeret afrundes. Tab af IMEI ses typisk i forbindelse med tjenestetypen internet.

Fejlformatering og tab af IMEI-numre betyder, at nummeret ikke er umiddelbart tilgængeligt for efterforskeren i en given sag. I disse tilfælde vil IMEI-nummeret dog kunne findes ved at konsultere rådata. Disse konverteringsfejl vurderes derfor ikke umiddelbart at have praktisk betydning.

Afrunding af IMEI-numre er som nævnt forekommende i 1.792 rekvisitioner. Denne konverteringsfejl kan have betydning, idet IMEI-numre anvendes til at identificere enheder ved indhentning af historiske teleoplysninger. Fejlen kan derfor betyde, at en anden enhed end den faktiske involverede inddrages i en given sag. Nærmere analyse viser dog, at ca. 99 pct. af de berørte IMEI-numre på rækkeniveau har 16 cifre, hvorfor afrundingen berører ciffer nummer 15 og 16. Det vil sige, at ca. 1 pct. vedrører det 14. ciffer, dvs. anslået 18 rekvisitioner. I det begrænsede antal rekvisitioner, hvor afrundingen kan have påvirket de 14 anvendte cifre, kan fejlen have medført, at en anden enhed end den faktisk involverede inddrages i en sag, f.eks. i forlængelse af et mastesug.

Det bemærkes, at Rigspoliet ligeledes har identificeret fejl vedrørende afrunding og tab af IMEI-numre i interne stikprøvekontroller.

#### **5.7.1.9 Sammenligning af indhold - FokusABC**

FokusABC angiver, hvorvidt det er A-, B- eller C-nummer, der udgør fokus for et indgreb i meddelelshemmeligheden (kaldet fokusnummer). Der er identificeret 1.411 rekvisitioner, hvor der er fejl i Fokus ABC. Der er tale om en fejlkonvertering, der er forekommende i ca. 6,9 pct. af det samlede antal analyserede rækker.

Fejlkonverteringer vedrørende FokusABC ses hyppigst forekommende ved tjenestetypen internet (855 rekvisitioner). Generelt er der tale om en konverteringsfejl, der vurderes at være af mindre betydning. Det skyldes, at efterforskeren, der rekvirerer historiske teledata, selv vil være bekendt med, hvilken enhed, der udgør fokus for et indgreb i meddelelshemmeligheden. I den forstand kan FokusABC ansues som en ekstra 'service' til brugeren af det historiske teledata.

#### **5.7.2 Analyse af konvertering af mastepositioner**

Analysen belyser for alle rekvisitioner, hvor der er et match mellem rækker i rådata og konverteret data, om der er fejl i de kolonner, hvor der er foretaget en indholdsmæssig konvertering af data (jf. trin 6 i afsnit 4.4.), konkret om der er fejl i konverterede mastepositioner. Data konverteres af Rigspolitiets Telecenter for at sikre, at teleoplysningerne fremstår ensartede

og genkendelige under efterforskningen og i forbindelse med en eventuel efterfølgende fremlæggelse af teleoplysningerne i retten. Behovet for konvertering og ensretning af data skyldes, at politiet modtager data fra teleudbydere i forskellige formater.

Analysen viser jf. ovenstående afsnit, at der i perioden 2011-2019 er sket forskydninger af mastekoordinater i forbindelse med i Rigspolitiets Telecenters konvertering af mastepositioner. Konkret er der identificeret 461 rekvisitioner med fejlkonvertering af koordinater på startmast og 385 rekvisitioner med fejlkonvertering af slutmast. Den langt overvejende del af disse forskydninger udgøres af en konverteringsfejl, hvor mastekoordinater er forskudt med ca. 222 meter. Hertil er der identificeret et mindre antal rekvisitioner med forskydninger af mastekoordinater på ca. 100 meter.

Afvielser i denne størrelsesorden vil i de fleste tilfælde ikke have betydning i lyset af de generelle usikkerheder, der er forbundet med geografisk lokalisering ved brug af teledata. Navnlig i tættere bymæssig bebyggelse, hvor celler generelt dækker et mindre område, kan selv mindre forskydninger dog i specifikke situationer potentielt have betydning.

Hertil er der identificeret et begrænset antal rekvisitioner med meget store afvielser. Disse afvielser vurderes at have et omfang, hvor det vil være helt åbenlyst for brugerne af historiske teledata i politikredse mv., at der er tale om en fejl.

#### 5.7.2.1 Forskydning af mastepositioner

Rigspolitiets konvertering af historiske teledata indebærer, at mastepositioner fra teleudbydere konverteres til et ensartet format. Teleudbydere anvender to forskellige koordinatsystemer, og politiet konverterer mastekoordinater til et tredje system. Da rådata og konverteret data derfor *forventes* at være forskelligt (da det afspejler forskellige koordinatsystemer), sammenlignes i stedet Rigspolitiets Telecenters og Deloitte's konvertering af mastekoordinater. Det gør det muligt at identificere, om der er sket fejlkonverteringer af mastekoordinator.

Det fremgår af tabellen nedenfor, at der er identificeret 461 og 385 rekvisitioner med uoverensstemmelse i konverteringen af mastekoordinaterne for hhv. start- og slutmast. Det ses, at der er færre fejlkonverteringer på slutmaster end startmaster. Det skal ses i lyset af at visse tjenestetyper (mms og internet) kun registreres på startmast, hvorfor der generelt er flere koordinater på startmaster end slutmaster i de analyserede rekvisitioner.

<b>Mastekoordinater</b>	<b>Antal unikke rekvisitioner uden overensstemmelse</b>
Koordinat startmast	461
Koordinat slutmast	385

De 461 og 385 rekvisitioner med konverteringsfejl på hhv. start- og slutmast dækker over et antal fejlbehæftede rækker. Det fremgår af tabellen nedenfor, at der er identificeret 589.705 og 345.517 unikke rækker med uoverensstemmelser i mastekoordinaterne for hhv. start- og slutmast mellem Rigspolitiets Telecenters og Deloitte's konvertering. Dette udgør hhv. 1,2 pct. og 0,7 pct. af det totale antal rækker i feltsammenligningen.

<b>Mastekoordinater</b>	<b>Antal unikke rækker uden overensstemmelse</b>
Koordinat start mast	589.705*)
Koordinat slut mast	345.517*)

\*) En umiddelbar analyse af disse tal viser, at de reelle forskelle sandsynligvis er betydeligt lavere. Tallene oven for er et konservativt estimat, der afspejler et forsigtighedsprincip. Forventeligt ligger de reelle forskelle på under 10 pct. af tallene i tabellen ovenfor. Det vil sige, at tallene forventes at ligge under 85.000 af de 48,7 millioner rækker, der indeholder over 225 millioner positioner svarende til under 0,04 pct. uoverensstemmelser.

Tallene i tabellerne nedenfor er afledt af disse højt satte værdier.

Rekvitioner med en fejl eller forskydning af mastekoordinater på hhv. start- og slutmast i forbindelse med konverteringen, er nedbrudt på størrelsen af afvigelsen i nedenstående tabel. Denne fremstilling indebærer en omregning fra koordinater til geografisk placering. Konkret fremgår det af tabellen, hvor mange unikke rækker, der er identificeret med en given forskydning, målt i antal meter.

Tabellen nedenfor viser et yderligere nedbrud af de 461 rekvisitioner med forskydninger af startmastens position som følge af konverteringsfejl. Det fremgår af tabellen at de identificerede konverteringsfejl langt overvejende leder til en forskydning af mastepositioner på ca. 100 eller ca. 220 meter. Den enkelte rekvisition kan indeholde flere fejlkonverterede rækker (da den indeholder flere rækker), hvorfor tabellen summer til mere end 461 fejlbehæftede rekvisitioner. Set i lyset af det samlede antal rækker, der indgår i analysen, er der samlet set identificeret fejlkonvertering af startmasten på 1,2 pct. af de analyserede rækker.

<b>Antal meters forskydning af startmast</b>	<b>Antal rekvisitioner, der indeholder forskydning i den pågældende størrelsesorden *)</b>	<b>Antal rækker med forskydning *)</b>
1 meter	14	95
80-89 meter	1	19
90-99 meter	147	194.876
100-109 meter	194	178.907
220-223 meter	112	170.683
13.514 meter	1	4
>1.000.000 meter	114	45.121

\*) Jævnfør ovenstående er tallene i tabellen et konservativt estimat der med meget stor sandsynlighed er væsentlig lavere. Tallet afspejler et



*forsigtighedsprincip. Forventeligt ligger de reelle forskelle på væsentligt under værdierne i tabellen ovenfor.*

Tabellen nedenfor viser et lignende nedbrud af de 412 rekvisitioner, hvor der er identificeret forskydninger af mastkoordinater for slutmasten. Den enkelte rekvisition kan indeholde flere fejlkonverterede rækker (da den indeholder flere rækker), hvorfor tabellen summer til mere end 412 fejlbehæftede rekvisitioner. Det fremgår igen, at konverteringsfejl primært har resulteret i en forskydning af mastepositioner på ca. 100 eller ca. 222 meter. Ses der på de berørte rækker i lyset af det samlede antal rækker, der indgår i analysen, er der samlet set identificeret fejlkonvertering af slutmasten på 0,7 pct. af de analyserede rækker.

<b>Antal meters forskydning</b>	<b>Antal rekvisitioner, der indeholder forskydning i den pågældende størrelsesorden *)</b>	<b>Antal rækker (i rekvisitioner) med forskydning *)</b>
1 meter	10	81
80-89 meter	1	13
90-99 meter	129	121.006
100-109 meter	176	106.019
220-223 meter	98	92.881
1000-19.999 meter	1	5
90.000-99.999 meter	5	9
>1.000.000 meter	76	25.503

*\*) Jævnfør ovenstående er tallene i tabellen et konservativt estimat der med meget stor sandsynlighed er væsentlig lavere. Tallet afspejler et forsigtighedsprincip. Forventeligt ligger de reelle forskelle på væsentligt under værdierne i tabellen ovenfor.*

På tværs af de to tabeller fremgår det, at forskydninger som følge af konverteringsfejl langt overvejende er koncentreret omkring en forskydning på ca. 222 meter, hvilket er en konverteringsfejl, som Rigspolitiet selv har identificeret i forbindelse med teledatasagen. Fejlen skyldes ifølge Rigspolitiets undersøgelser, at et koordinatsystem i en kort periode i 2016 er dobbeltkonverteret til et andet koordinatsystem, som anvendes i dansk politi. Fejlen berører langt overvejende data fra én udbyder. Det har i denne periode betydet, at samtlige mastekoordinater er forskudt ca. 82 meter mod vest, og ca. 206 meter mod syd - i alt ca. 222 meter i syd-sydvestlig retning. Hertil er der identificeret et antal rækker, hvor der er sket en forskydning på ca. 100 meter. Dette er ligeledes en konverteringsfejl, som tidligere er identificeret af Rigspolitiet.

Deloitte's undersøgelse bekræfter således, det billede, som Rigspolitiets interne undersøgelser har afdækket.

Der er ligeledes identificeret et antal rækker, der angår et lavt antal rekvisitioner, med større afvigelser. Forskydningerne af en størrelse, som

betyder at de med overvejende sandsynlighed vil kunne identificeres som helt åbenlyse fejl af brugeren af historiske teledata i politikredse mv. Disse fejl kan ikke umiddelbart forklares med forkert anvendt koordinatsystem eller en ombytning af koordinater.

Der er ligeledes foretaget en nedbrydning af konverteringsfejl på rækkenniveau per år, jf. de to nedenstående tabeller. Det fremgår, at forskydninger i mastepositioner langt overvejende er koncentreret i 2016, hvilket ligeledes stemmer overens med Rigspolitiets fund, jf. ovenstående. Det fremgår ligeledes, at der ikke er identificeret konverteringsfejl vedrørende mastkoordinater i 2019.

For startmasten fremgår det, at konverteringsfejl langt overvejende er identificeret i årene 2015-2016, mens der i meget begrænset omfang er identificeret konverteringsfejl i de andre år i undersøgelsens periode.

År	Antal rekvisitioner med forskydning på startmast	Antal unikke rækker med forskydning af mastekoordinater
2019	0	0
2018	6	9
2017	7	74
2016	274	317.167
2015	162	272.371
2014	3	3
2013	0	0
2012	4	76
2011	5	5

Det fremgår tilsvarende for slutmasten, at konverteringsfejl langt overvejende er identificeret i årene 2015-2016, mens der i meget begrænset omfang er identificeret konverteringsfejl i de andre år i undersøgelsens periode.

År	Antal rekvisitioner med forskydning på slutmast	Antal unikke rækker med forskydning af mastekoordinater
2019	0	0
2018	2	4
2017	7	67
2016	216	183.601
2015	149	161.774
2014	2	2

Undersøgelse af Rigspolitiets håndtering af historiske teledata

2013	0	0
2012	5	59
2011	4	10

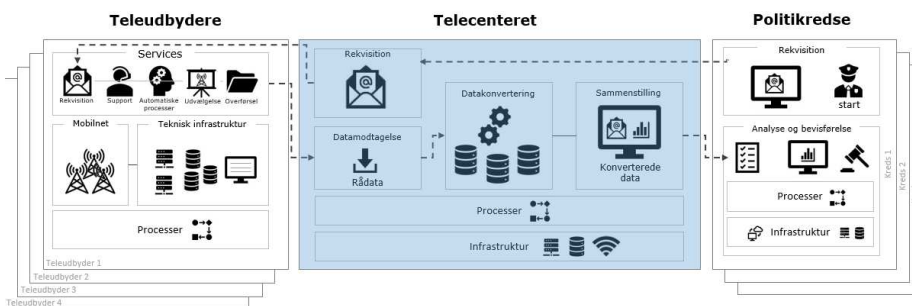
# 6 Potentielle fejlkilder og usikkerheder ved anvendelse af historiske teledata

## 6.1 Formål og afgrænsning af undersøgelse

Undersøgelsen har belyst potentielle fejlkilder og usikkerheder ved anvendelse af historiske teledata. Formålet er at etablere et helhedsbillede over de opmærksomhedspunkter, som skal iagttages ved anvendelse af historiske teledata i forbindelse med straffesager.

Afsnittet er struktureret med afsæt i teledataværdikæden, jf. afsnit 3. Således gennemgås først usikkerheder og fejlkilder forbundet med tekniske forhold ved teleudbydere (mobilnet og infrastruktur) og processer omkring konsolidering af historiske teledata, herefter gennemgås usikkerheder og fejlkilder i Rigspolitiets håndtering af historiske teledata, herunder konvertering, processer og systeminfrastruktur. Endelig belyses fejlkilder og usikkerheder vedrørende den efterfølgende anvendelse af historiske teledata i politi og anklagemyndighed.

Undersøgelsen har taget udgangspunkt i metoden angivet i afsnit 4. Det er væsentligt at bemærke, at det primære fokus for afdækningen af governance, roller og processer, herunder kvalitetskontrol, er Rigspolitiets Telecenters processer fra historiske teledata modtages, opbevares og behandles til de afleveres til politikredsene mv. Analysen af teleudbydere og politikredsene mv. har været overordnet og begrænset til enkelte interviews.



## 6.2 Sammenfatning af potentielle usikkerheder og fejlkilder ved anvendelse af historiske teledata

Denne sektion opsummerer de usikkerheder og fejlkilder, som bør iagttages ved anvendelse af historiske teledata i forbindelse med straffesager.

Ved anvendelse af historiske teledata er det grundlæggende centralt at bemærke, at der er tale om data, der er karakteriseret ved en række iboende usikkerheder af teknisk karakter, herunder justering af antenne samt hvordan terrænet påvirker signalers rejse gennem landskabet. Hertil medfører tekniske forhold såvel som processer og arbejdsgange hos teleudbyderne en række kilder til fejl og usikkerheder.

Konverteringen af historiske teledata hos Rigspolitiets Telecenter indebærer, jf. sektion 5, ligeledes en række fejlkilder af varierende karakter. Nogle fejlkilder vil have medført manglende data i konverteret data. Heraf vil nogle mangler være åbenlyse, mens andre ikke er mulige at identificere med mindre konverteret data sammenlignes med rådata. Hertil er der identificeret en række eksempler på fejlkonverteringer, som afhængig af det konkrete indhold, kan have haft betydning eller ej. Der henvises til sektion 5 for en detaljeret gennemgang af de identificerede konverteringsfejl.

Endelig er der en række usikkerheder forbundet med arbejdsgange og kompetencer vedrørende håndtering af historiske teledata i politikredse mv.

På baggrund af undersøgelsen har Deloitte udarbejdet et uvildigt notat om anvendelsen af historiske teledata, der redegør for de særlige opmærksomhedspunkter, man bør have, når historiske teledata anvendes til efterforskning og som strafferetligt bevis (Notat om anvendelse af historiske teledata i straffesager). Notatet henvender sig til politi, anklagere, dommere og forsvarere og kan fremadrettet blive fremlagt af anklagemyndigheden i straffesager, således at det sikres, at alle straffesagens aktører er bekendt med de potentielle fejlkilder og usikkerheder, der er ved anvendelsen af historiske teledata som bevismiddel.

### **6.3 Generelle usikkerheder givet historiske teledatas beskaffenhed**

Teleudbydere indsamler historiske teledata i forretningsøjemed, bl.a. med henblik på taksering af ydelser og fakturering af kunder samt optimering af netværket. Historiske teledata er således genereret med andet formål for øje end anvendelse i forbindelse med straffesager.

Generelt er gældende, at telekommunikationens rejse mellem mobilenhed og antenne, som er placeret på en given mast, påvirkes af tekniske forhold, herunder justering af antennen, højden på antennens placering og den anvendte transmissionsteknologi, samt en række eksterne forhold, bl.a. vejrlig, landskab, vegetation, bygningsmasse mv. Derfor kan det over tid variere hvilken mast og antenne en enhed knyttes til, uanset at kommunikation gennemføres fra den samme geografiske position. Historiske teledata har således langt fra samme præcision som f.eks. GPS. Det er en iboende usikkerhed ved historiske teledata, som bør iagttages ved anvendelse af historiske teledata i forbindelse med straffesager.

#### **6.3.1 Usikkerheder grundet mobilnet og infrastruktur**

Telekommunikationen påvirkes af tekniske forhold, herunder antennens justering, højdemæssige placering og den anvendte transmissionsteknologi. Hertil vil belastningen på telenetværket påvirke hvilken antenne en mobil enhed knyttes til. Det kan betyde, at mobile enheder på et givent tidspunkt

opnå forbindelse til andre master, end hvad der ville være forventet i en situation med mindre belastning på netværket.

Der er typisk færre master i landområder til dækning af et givent areal, hvilket indebærer, at 'mastespring' kan ske over en større geografi. Præcisionen ved lokalitetsangivelser spænder således fra ned til få hundrede m<sup>2</sup> i tættere bymæssig bebyggelse til adskillige km<sup>2</sup> i landområder. Ofte vil den lokalitetsmæssige usikkerhed i landområder dermed være betydeligt større end i byområder.

Hertil er der forskel i præcisionen i historiske teledatas lokalitetsangivelser afhængig af, om mobilenheden har en aktiv forbindelse (*connected mode*) eller ej (*idle mode*). En mobilenheds placering i *idle mode* registreres kun på cellegruppeniveau, ikke på niveau af den enkelte celle, som det er tilfældet når enheden har en aktiv forbindelse. En enhed kan i *idle mode* derfor skifte celle internt i en cellegruppe, uden at det registreres, selvom enheden har bevæget sig over en distance, der ville have medført registrering af et celleskift, hvis enheden havde været i aktiv anvendelse.

Disse tekniske forhold medfører, at lokalitetsangivelser ved historiske teledata bør betragtes som indikative.

### **6.3.2 Usikkerheder grundet terræn mv.**

Forhold som landskab, vejr og årstid kan påvirke, hvilken mast en given enhed, på et givet tidspunkt, får forbindelse med. En enhed vil eksempelvis typisk kunne opnå forbindelse med en mast over større afstande over vandområder, end det er tilfældet over land, grundet færre hindringer i terrænet (og dermed mindre dæmpning af signalet), eller hvis enheden er placeret højt i landskabet. Tilsvarende kan årstiden påvirke en enheds forbindelse til en given mast, idet f.eks. blade på træerne i sommerhalvåret dæmper signalet i højere grad, end det vil være tilfældet i vinterhalvåret.

Således påvirker en række forhold omkring terræn mv. en mobilenheds forbindelse til telenetværket, hvilket medfører en generel usikkerhed, som bør iagttages ved anvendelse af historiske teledata.

## **6.4 Usikkerheder og fejlkilder givet forhold hos teleudbydere**

Afsnittet beskriver usikkerheder og fejlkilder givet forhold hos teleudbydere, herunder både af teknisk og processuel karakter.

### **6.4.1 Systemudtræk i forbindelse med rekvisitioner af historiske teledata hos teleudbydere**

Konsolideringen af teledata hos den enkelte udbyder er forbundet med en betydelig kompleksitet, idet data trækkes fra et stort antal platforme og systemer, som er leveret af et stort antal underleverandører. Alle platforme og systemer konfigureres med et stort antal parametre. Disse processer er underlagt almindelige forretningsmæssige processer og procedurer hos teleudbydere. Udtræk fra systemer i forbindelse med rekvisitioner fra politiet omfatter hos teleudbydere i varierende grad manuelle og automatiserede processer. Særligt i forbindelse med manuelle processer kan der opstå menneskelige fejl.

#### **6.4.2 Udvalgelse af master ved mastesug**

Ved lokalisering af enheder i en afgrænset geografi (mastesug) baseres dataudtræk på data fra de master og celler, som i teleselskabernes modeller for dækningskort forventes at dække den angivne geografi. Dækningskort er teleudbydernes opgørelser over den geografiske netværksdækning givet teleinfrastruktur og netværksdesign og giver en indikation om signalstyrken på et givet sted. Disse modeller varierer fra manuelle til automatiserede modeller. Modellerne indebærer antagelser, som kan variere mellem selskaberne, og som kan være kilde til usikkerheder. Det er hertil et opmærksomhedspunkt, at dækningskort typisk tager afsæt i en højde på 1,5 meter for brugeren af den mobile enhed. Afvigelser i højde, f.eks. ved fysisk placering af en enhed i et højhus, kan medføre forbindelse til master inden for et større geografisk område.

Udvælgelsen af master hos den enkelte teleudbyder udgør en potentiel fejlkilde i forbindelse med mastesug, idet kan være aktivitet, som ikke registreres, hvis en given enhed har været forbundet til mast, der ikke var omfattet af teleudbyderens geografiske udvælgelsesmodel.

#### **6.4.3 Usikkerheder forbundet med ikke-logningspligtige historiske teledata**

Logningsbekendtgørelsen definerer de teleoplysninger, som teleselskaberne er forpligtet til at registrere og opbevare. Hertil registreres i varierende omfang yderligere oplysninger, som kan finde anvendelse i forbindelse med straffesager. Det gælder f.eks. signaleringsdata for mobile enheder, som ikke aktivt har været i anvendelse (idle mode).

Såfremt der anvendes ikke-logningspligtige historiske teledata, er det et generelt opmærksomhedspunkt, at disse data kan være ufuldstændige, da teleudbyderne ikke er forpligtiget til at registrere dem, hvorfor data kun registreres af nogle udbydere med henblik på fejlretning i netværket. Hertil kan driftsforhold medføre udfald. Signaleringsdata er hertil forbundet med større usikkerhed end de logningspligtige historiske teledata, da en mobil enheds placering i idle mode kun registreres på cellegruppeniveau, jf. afsnit 6.3.1.

#### **6.4.4 Manglende oplysninger vedrørende nye dataservices**

Kommunikation faciliteres i stigende grad via nye data- og samtalservices. Herunder kan både opkald og SMS-beskeder gennemføres med anvendelse af nye teknologier benævnt VoLTE (Voice over Long Term Evolution) og VoWiFi (Voice over WiFi). Rigspolitiets undersøgelser har identificeret, at der i en række tilfælde er leveret ufuldstændigt data vedrørende disse nye dataservices fra en teleudbyder, samt at kommunikation ved disse teknologier i en række tilfælde ikke har fremgået korrekt af rådata. Tilsvarende er der identificeret et tilfælde med en anden teleudbyder, der i en periode har leveret ufuldstændige data vedrørende kommunikation foretaget ved VoLTE og VoWiFi.

#### **6.4.5 Fejl i mastelister og mastepositioner**

Teleudbydernes netværk opgraderes og vedligeholdes løbende med henblik på at levere så god netværksdækning som muligt. Opgraderingen af telenetværket er særligt betydende ift. kobling med mastelister, idet

opdateringer til mastelister (adresser, koordinater og retning på celler), kan indebære en risiko for registreringsfejl.

Der er i dataanalysen identificeret en række eksempler på fejl af denne karakter, herunder hvor masterpositioner angiver en lokalisering langt uden for Danmarks grænser. Der er i dataanalysen identificeret koordinater i rådata, der placerer den mobile enhed langt uden for Danmarks grænser. I nogle tilfælde vurderes det, at fejlen skyldes ombytning af koordinater, mens det i andre tilfælde ikke er muligt at vurdere, hvordan datatræk kan resultere i de angivne koordinater. Fejl af denne type er imidlertid nemme at identificere, da de angivne lokaliteter er uden for landets grænser og i øvrigt ikke stemmer overens med de adresser, der ligeledes fremgår af data.

Tilsvarende er der identificeret historiske tilfælde, hvor adresser og koordinater på master ikke har været i overensstemmelse.

#### **6.4.6 Manglende data i rådatafiler**

Der er i dataanalysen såvel som Rigspolitiets egne undersøgelser identificeret en række eksempler på, at centrale oplysninger mangler i de rådatafiler, som er modtaget fra teleudbyderne. Der er her tale om mangler, der er til stede i rådata inden det er konverteret. Der er både identificeret eksempler på relevante rækker i data, der ikke er medtaget i dataudtræk, såvel som manglende indhold i konkrete felter.

I de fleste tilfælde vil fejl af denne type være nemme at identificere, idet centrale oplysninger hverken vil fremgå af rådata eller konverteret data. Det gør det muligt for politikredse mv. at efterspørge nyt rådata hos teleudbyder.

#### **6.4.7 Øvrige fejlkilder i rådatafiler**

Der er af Rigspolitiet identificeret en række eksempler på fejl i rådata af forskellig karakter, herunder ombytning af A- og B-nummer ved VoLTE-opkald og forkert landekode ved udenlandske opkald og ombyttede mastekoordinater.

### **6.5 Fejlkilder og usikkerheder i Rigspolitiets håndtering af historiske teledata**

Historiske teledata modtages hos Rigspolitiet i form af rådata fra teleudbyderne og konverteres herefter. Behovet for konvertering og ensretning af data skyldes, at politiet modtager data fra teleselskaberne i forskellige formater, og at sammenstilling af oplysninger og egentlig analyse på tværs af teleudbydere er svær at gennemføre på baggrund af rådata i oprindelige formater. Der er i konverteringen identificeret en række fejlkilder, jf. sektion 5, og som opsummeres i dette afsnit.

#### **6.5.1 Manglende rækker eller for mange rækker i konverterede data**

Dataanalysen har jf. sektion 5 identificeret, at der i en række tilfælde er sket fejl i konverteringen af rådata, som har resulteret i, at rækker, der fremgår af rådata ikke er afspejlet i det konverterede data – og omvendt at der optræder flere rækker i konverteret data end i rådata.



Fejl vedrørende manglende rækker er ligeledes identificeret af Rigspolitiet, som har peget på en række årsagsforklaringer, herunder peger Rigspolitiet på en it-systemfejl og en fejl i håndteringen af oplysninger om 'særlige tjenester' (f.eks. viderestilling af opkald).

Fejl i antallet af rækker vil have medført, at oplysninger ikke er tilgået politikredse mv., men kan kontrolleres ved en sammenligning af antal rækker i hhv. rådata og konverteret data. Fejlen vedrørende manglende rækker i konverteret data optræder stadig i begrænset omfang og er derfor et relevant opmærksomhedspunkt i forbindelse med konvertering af data.

### **6.5.2 Manglende indhold i felter i konverteret data**

Der er ligeledes identificeret en fejlkilde, hvor der i konverteret data mangler indhold på niveau af det enkelte felt. Fejlkilden er identificeret for celleindhold vedrørende celle-id, celle-kordinater, manglende IMEI-nummer, herunder særligt ved rækker vedrørende internet, manglende landekode mv.

Fejl af denne type vil typisk være umiddelbart identificerbare, og det vil være muligt at konsultere rådata med henblik på at konstatere, om der er tale om en konverteringsfejl, såfremt informationen fremgår af rådata.

### **6.5.3 Fejlkonvertering af tomme celler i rådata**

Der er identificeret en fejlkilde, hvor tomme felter i rådata i konverteringen udfyldes med den numeriske værdi 0. I langt de fleste tilfælde vil denne fejl være åbenlys at identificere, idet der vil være angivet 0 i felter, hvor 0 ikke er en meningsfuld værdi (f.eks. A-nummer eller B-nummer). Fejlen kan imidlertid have haft betydning i celler vedrørende celleretning, idet 0 her angiver nordlig retning.

### **6.5.4 Fejlkonvertering af indhold i felter**

Der er i dataanalysen identificeret en række eksempler, hvor oplysninger vedrørende celler ikke er konverteret korrekt. Der er tale om en bred vifte af forskellige konverteringsfejl, og der henvises til sektion 5 for en detaljeret gennemgang heraf.

Rigspolitiet har ligeledes identificeret en række fejl vedrørende konvertering af celleoplysninger, herunder eksempler hvor celle-id har været erstattet af angivelse af land; tilfælde, hvor et land ikke har fremgået, men blot 'udland' selvom rådata har indeholdt en angivelse af det konkrete land; samt tilfælde hvor celle-id ikke er blevet konverteret i fuldt format. Hertil er der identificeret fejl vedrørende trunkering af koordinater i udlandet (fra syv til seks cifre), trunkering af IMEI-numre og A-numre over 15 cifre. Hertil er der identificeret fejl, hvor numre der starter med 0 er rensat. Dette er set både i IMEI samt A-, B-, og C-nummer kolonnerne.

Nogle konverteringsfejl er helt uden praktisk betydning, andre kan have betydning i specifikke anvendelsessituationer, mens endnu andre potentielt kan have betydning.

### 6.5.5 Forskydning af mastepositioner

Der er i dataanalysen, såvel som i Rigspolitiets egne undersøgelser, identificeret en fejlkilde vedrørende forskydning af mastepositioner. Forskydninger af mastepositioner er, som følge af konverteringsfejl, langt overvejende koncentreret omkring en forskydning på ca. 222 meter. Fejlen skyldes ifølge Rigspolitiets undersøgelser, at et koordinatsystem i en kort periode i 2016 er dobbeltkonverteret til et andet koordinatsystem, som anvendes i dansk politi. Hertil er der identificeret en anden historisk konverteringsfejl, som resulterer i en forskydning på ca. 100 meter. Dette er ligeledes en konverteringsfejl, som tidligere er identificeret af Rigspolitiet. I lyset af de usikkerheder, der generelt er forbundet med lokaliseringangivelser baseret på teledata, og at de konstaterede fejl ikke har betydning i forhold til en aktivitetes rigtighed (enhed A har kommunikeret med enhed B etc.), vurderes konverteringsfejl af denne størrelsesorden umiddelbart – dog afhængig af den konkrete anvendelse i forbindelse med en sag – overvejende sandsynligt at være af mindre betydning.

Der er ligeledes identificeret eksempler på konverteringsfejl, som har resulteret i meget betydelige forskydninger af mastepositioner. Forskydningerne er af en størrelse, som betyder, at de umiddelbart vil kunne identificeres som helt åbenlyse fejl af brugeren af historiske teledata i politikredse mv. Disse fejl kan ikke umiddelbart forklares med forkert anvendt koordinatsystem eller en ombytning af koordinater.

### 6.6 Usikkerheder og fejlkilder i kredsenes håndtering af historiske teledata

Undersøgelsen har taget udgangspunkt i metoden angivet i afsnit 4. Det primære fokus for afdækningen af governance, roller og processer har været Telecenterets processer fra historiske teledata modtages, opbevares og behandles til de afleveres til politikredsene mv. Analysen af politikredsene mv. har været overordnet og begrænset til enkelte interviews.

Generelt har de enkelte politikredse mv. i nogen grad etableret egne uformelle processer for håndtering af historiske teledata, blandt andet i forhold til uddannelse af efterforskere, hvornår specialister involveres, hvilke værktøjer og teknologier, der anvendes til behandling af historiske teledata, hvordan der videndeles og kommunikeres med andre aktører i teledataværdikæden uden for kredsen. Der er generelt set ikke en etableret praksis omkring kvalitetssikring af de modtagne historiske teledata.

I nedenstående afsnit er der fortaget en mere udførlig beskrivelse af usikkerheder og fejlkilder i politikredse mv.

#### 6.6.1.1 Kompetencer

Kompetencer inden for anvendelse af historiske teledata er forskellige i politikredsene.

Generelt oplæres efterforskere i anvendelse af historiske teledata ved sidemandsoplæring af mere erfarne efterforskere, men der ses ikke en egentlig uddannelsesplan eller -forløb til nye efterforskere. Der er i nogle politikredse tidligere blevet udbudt kurser i anvendelse af historiske teledata, men kurserne afholdes ikke konsistent og har varierende indhold. Der udbydes ikke kurser og kun i begrænset omfang vejledning fra

Rigspolitiets Telecenter. Det betyder, at der er risiko for at efterforskere ikke er bekendt med de usikkerheder, der er ved anvendelse af historiske teledata og dermed fejltolker data.

Siden 2016 er en ny gruppe af teledataspecialister blevet ansat i Særlig Efterforskning Øst og Særlig Efterforskning Vest (SEØ og SEV), som typisk har en akademisk baggrund med speciale i behandling af data. Denne gruppe behandler og analyserer alene historiske teledata og tager ikke del i selve efterforskningen. SEØ og SEV supporterer efterforskerne i henholdsvis øst og vest. Teledataanalytikergruppen har deltaget i telespecialistkursus 1. Dataanalytiker/specialister inddrages i sager alene på opfordring af den enkelte efterforsker.

#### **6.6.1.2 Kvalitetssikring i politikredse mv.**

Før december 2018 har der generelt ikke været foretaget kvalitetssikring af modtaget historiske teledata fra Rigspolitiets Telecenter. Der har i politikredsene mv. været en formodning om, at modtaget historiske teledata fra Rigspolitiets Telecenter har været korrekt og fuldstændigt, og derfor har det ikke været praksis at foretage en afstemning af fuldstændighed i den konverterede fil. På den baggrund er der usikkerhed om, hvorvidt denne afstemning er blevet foretaget.

Den efterbehandling, analyse, tilpasning og berigelse af andre datalister, som teledataanalytikere og efterforskere foretager, bliver generelt ikke logget eller nedskrevet, hvorfor det er vanskeligt at følge transaktionssporet. Her er det dog væsentligt at fremhæve, efterforskerne som hovedregel vedlægger den konverterede fil til anklager, og at anklageren i forbindelse med forberedelse til retten vil kontrollere, at data anført i analyserapport kan findes i underliggende konverterede filer. Som indledningsvist anført er der generelt en uens praksis for kvalitetssikring, hvilket bl.a. gør sig gældende i forhold til involvering af teledataspecialister, anvendelse af værktøjer til efterbehandling af historiske teledata samt arkivering af historiske teledata.

Der er dog enkelte politikredse, som lokalt har etableret (hovedsagligt uformelle) retningslinjer for håndtering af historiske teledata.

#### **6.6.1.3 Kommunikation og opsamling af fejkilder**

Politikredsene mv. har ikke etableret entydige kommunikationsveje, såfremt der opstår behov for support eller til indberetning af identificerede fejl vedrørende anvendelse af historiske teledata. Bortset fra et årligt ERFA-gruppemøde, med deltagelse af teledataanalytikere og andre udpegede videnspersoner, er der ikke etableret fora for løbende vidensdeling. Der er i 2018 oprettet et fora for teledataanalytikere til vidensdeling, men der er begrænset kendskab til dette fora i kredsene.

Såfremt der er behov for support, vil den lokale teledatabehandler i politikredsen mv. kontakte de videnspersoner, som er kendte i deres personlige netværk, det være sig andre telespecialister, Rigspolitiets Telecenter eller direkte til teleudbyderen. Ved fundne fejl, vil det ofte være afhængig af fejltypen, hvorvidt Rigspolitiets Telecenter eller teleudbyderen kontaktes. I forhold til løbende vidensdeling, sker dette uformelt og uens på tværs af politikredsene mv. Dog er der hos Rigspolitiets Telecenter i sommeren 2019 etableret et fælles fora for indberetning af fejl.

Der henvises i øvrigt til Deloitte's anbefalinger vedrørende politikredsene mv. i sektion 8 om kvalitetskontrol af historiske teledataoplysninger.

Anbefalingerne kan i det væsentligste opsamles til kommunikation om indholdet i *Notat om anvendelse af historiske teledata i straffesager*, processer for revisionsspor og opbevaring af historiske teledata, fuldstændighedskontrol af data samt kompetenceløft og overvejelser om etablering af videnscentre.

# 7 Gennemgang af Rigspolitiets systemer til opbevaring og behandling af historiske teledata

## 7.1 Formål og afgrænsning af undersøgelse

Formålet med gennemgangen af Rigspolitiets systemer til opbevaring og behandling af historiske teledata er at vurdere funktionalitet, teknisk integritet og driftsstabilitet for de IT-systemer, der anvendes til opbevaring og behandling af historiske teleoplysninger, samt processer og dokumentation for IT-kontroller. Gennemgangen har taget udgangspunkt i ISO 27001:2013 (Information Security Management) samt ITIL (Information Technology Infrastructure Library) rammeværktøjerne for sikker drift.

Systemgennemgangen dækker applikationer og tilhørende infrastruktur (netværk, servere, operativsystemer og databaser), der håndterer eller opbevarer historiske teleoplysninger. Systemernes funktionalitet vurderes ift. systemernes overordnede formål, herunder mod standard og forventelig funktionalitet for f.eks. ETL (Extract Transform Load)/datakonvertering og data processing.

Undersøgelsen har fokuseret på den del af de generelle IT-kontroller, som er væsentlige i forhold til de systemer og tilhørende tekniske platforme, der behandler og opbevarer historiske teledata. Udvælgelsen af de generelle IT-kontroller er således baseret på det overordnede formål at afdække:

- **Systemernes funktionalitet**, herunder overordnet funktionalitet ift. håndtering og opbevaring af historiske teledata. F.eks. områder som versionsstyring, revisionsspor, kvalitetskontroller mv.
- **Teknisk integritet**, herunder systemers indretning ift. at sikre dataintegritet, herunder sikring mod teknisk forvanskning.
- **Driftsstabilitet**, herunder i forhold til sikring mod systemnedbrud ved f.eks. backup, fail-over, systemreetablering ved backup, og ydelse (eksekverings hastighed) i daglig brug

Gennemgangen munder ud i konkrete anbefalinger til hvordan de identificerede udfordringer kan imødegås på kort og længere sigt.

## 7.2 Resultater af systemgennemgang

Undersøgelsen har taget udgangspunkt i en analyse af den samlede tekniske platform, hvor der er etableret et overblik over systeminfrastrukturen, som den ser ud i dag, men også i et historisk perspektiv inden for tidshorizonten for denne analyse. Analysen har taget udgangspunkt i tilgængelig dokumentation, herunder systemoptegnelser, og en 'vugge til grav' gennemgang af dataflow. Der er yderligere gennemført interviews med nøglemedarbejdere i Rigspolitiets Telecenter samt udvalgte medarbejdere fra Koncern IT, der er allokeret til Rigspolitiets Telecenter.

Systemerne og den tilhørende infrastruktur kan kort beskrives som utidssvarende og kompleks. Systemkomplekset omfatter flere systemer, integrationer og dataoverførsler. IT-miljøet har løbende været udviklet i takt med at nye dataformater, behov mv. er opstået. Udviklingen kan bedst beskrives som 'knopskydning'.

Undersøgelsen viser, at den samlede systemplatform, herunder procedurer for udvikling og drift, er på et helt utilstrækkeligt niveau.

Som følge af knappe ressourcer i Rigspolitiets Telecenter, der specifikt håndterer historiske teledata, har der været begrænset tid til sædvanlige drift af applikationerne samt løbende fokus på forbedring.

Infrastrukturen til håndtering af historiske teledata har over tid oparbejdet en meget stor teknisk gæld, der på den korte bane ikke vil kunne adresseres. Der er således betydelige risici forbundet med den fremadrettede driftsstabilitet, det vil sige sikkerheden for, at der fortsat kan leveres konverteret teledata. En u hensigtsmæssig arkitektur, utilstrækkelig governance mellem Telecenteret og Koncern IT, samt knappe ressourcer fra Koncern IT, der er allokeret til Rigspolitiets Telecenter, medvirker samtidig til en yderligere oparbejdelse af teknisk gæld. Dette som følge af begrænset tid til sikkert at kunne drifte og vedligeholde systemerne efter leverandørernes anbefalinger.

Endelig er der identificeret en mangelfuld governance mellem Rigspolitiets Telecenter, Koncern IT og brugere af systemerne til opbevaring og håndtering af historiske teledata.

Detaljerede observationer samt anbefalinger kan af hensyn til sikkerhedsniveauet ikke deles offentligt, men er meddelt Rigspolitiet.

## 7.3 Anbefalinger på baggrund af systemgennemgang

Der er i anbefalingerne skelnet mellem kortsigtede og langsigtede anbefalinger.

Kortsigtede anbefalinger bør af hensyn til karakteren af de observerede risici og hvad der teknisk og processuelt er muligt, gennemføres hurtigst muligt. Det er anbefalinger, der vil kunne adressere helt fundamentale IT-mæssige forhold og derved i noget omfang kunne adressere systemrisikoen og operationelle fejl. De kortsigtede anbefalinger omfatter blandt andet forbedringer i visse processer samt IT-mæssige forhold, der i noget omfang vil kunne reducere risikoen for fejl i selve konverteringsprocessen.

Adressering af de kortsigtede anbefalinger kombineret med selv betydelige investeringer i den nuværende infrastruktur, vil ikke kunne fjerne den tekniske gæld, endsiige reducere den væsentligt.

Som det fremgår nedenfor under langsigtede anbefalinger, vil der skulle investeres i ny infrastruktur. De langsigtede anbefalinger har fokus på at adressere relevante IT-mæssige forhold og den tekniske gæld. Adresseringen af den tekniske gæld vil strække sig over en længere periode og vil kræve betydelige investeringer i nye systemer mv.

Samlet set vil der være behov for en betydelig investering i ny infrastruktur og systemer, samt et ikke ubetydeligt ressourcetræk, til at kunne adressere både de kortsigtede og langsigtede anbefalinger.

### **7.3.1 Kortsigtede anbefalinger vedrørende systemer til opbevaring og behandling af historiske teledata**

Kortsigtede anbefalinger omhandler i det væsentligste nedenstående temaer.

#### **7.3.1.1 Stabilisering af nuværende infrastruktur og applikationer for historiske teledata**

Overordnet bør der iværksættes en detaljeret risikoanalyse og prioritering af de kernesystemer og infrastrukturkomponenter, som er særlige kritiske i forhold til driftsstabiliteten af systemerne, der opbevarer og håndterer historiske teleoplysninger, samt kan sikre den nødvendige tekniske integritet.

På baggrund af infrastrukturens nuværende tilstand anbefales det, at der fokuseres på at iværksætte tiltag, der skal sikre den nuværende platforms stabilitet. Dermed reduceres risikoen for driftsforstyrrelser og at systemer, der opbevarer og behandler historiske teledata, potentielt ikke kan reetableres. Det anbefales, at ovenstående tiltag udføres og implementeres hurtigst muligt.

Investeringerne i infrastrukturen vil være nødvendige for at sikre driftsstabiliteten på den korte bane, men vil have begrænset anvendelse i forhold til de langsigtede anbefalinger.

#### **7.3.1.2 Etablering af processer, procedurer og kontroller**

På kort sigt anbefales det, at Rigspolitiets Telecenter sikrer sig, at minimumskrav til politikker, processer, dokumentation samt kontroller etableres til sikring af den nødvendige stabilitet af infrastruktur og systemer samt sikrer mod teknisk forvanskning af data.

I forlængelse af ovenstående, anbefales det ligeledes, at der implementeres et minimum af kontroller, som sammen med ovenstående skal sikre stabiliteten og integriteten af systemer. Rigspolitiets it-sikkerhedspolitik tager udgangspunkt i bl.a. ISO 27001 rammeværket, og vi anbefaler at ovenstående tager udgangspunkt i dette.

Foruden ovenstående kortsigtede anbefalinger, henviser vi endvidere til etableringen af 3. parts løsningen, til validering af telecenterets konvertering jf. afsnit 8.

### **7.3.2 Langsigtede anbefalinger systemer til opbevaring og behandling af historiske teledata**

Langsigtede anbefalinger omhandler i det væsentligste nedenstående temaer. Der vil i nedenstående anbefalinger være tale om større udviklings- og implementeringsprojekter, som givet kompleksiteten vil betyde et højt ressource behov samt væsentlige investeringer.

#### **7.3.2.1 Ny og tidsvarende infrastruktur til håndtering af historiske teledata**

Til adressering af den tekniske gæld, anbefales overordnet, at der implementeres en ny og mere tidsvarende infrastruktur. Den nuværende infrastruktur har en for stor teknisk gæld til, at det er relevant at tage afsæt i denne. Der er vurderingen, at en ny infrastruktur bør baseres på standard-software, der har til formål at håndtere og konvertere data som ETL-software, der er designet til behandling af store og komplekse datamængder, med bevaring af fuldt revisionsspor.

Foruden infrastrukturen, bør selve arkitekturen nytænkes med henblik på at sikre, at den nuværende kompleksitet ikke videreføres i en ny infrastruktur. Infrastrukturen bør i det væsentligste baseres på allerede tilgængelige systemer og teknologier. Ved en ændring af arkitekturen, vil det være muligt for Koncern IT effektivt at køre drift og vedligehold, ligesom for øvrige systemer hos politiet. Det vil bidrage til at sikre, at der ikke opstår behov for at have specifikke Koncern IT-ressourcer tilknyttet det normale drifts- og vedligeholdelsesansvar for infrastrukturen for systemerne, der håndterer og opbevarer historiske teleoplysninger.

#### **7.3.2.2 Anvendelse af standard-software samt allerede indkøbte systemer og software**

Rigspolitiet har de seneste år indkøbt standard software til implementering i Rigspolitiets Telecenter, som imidlertid ikke er implementeret. Rigspolitiet har ligeledes indkøbt øvrig software, f.eks. POL-INTEL til analyse af data, der med fordel kan anvendes sammen med en ny arkitektur og infrastruktur, så der ikke egenudvikles egentlige systemer og applikationer til analyse af historiske teledata.

Anvendelse af POL-INTEL vil kunne sikre en ensrettet adgang til konverterede historiske teledata, og dermed reducere risikoen for forskellig og uensartet udstilling af data på tværs af Rigspolitiets Telecenter samt politikredsene mv. Foruden dette, vil analyseplatformen endvidere kunne bibringe yderligere og mere avancerede analyser til brug for efterforskningen i et standardiseret format.

Beslutning om en ændring af arkitekturen er en forudsætning for at ovenstående er muligt, og det vil endvidere kræve, at der samtidig etableres løsninger til håndtering af data med højere krav til sikkerhed.

#### **7.3.2.3 Implementering af Rigspolitiets politikker for IT-sikkerhed i Rigspolitiets Telecenters infrastruktur og applikationer**

Rigspolitiet har over de seneste år iværksat en række initiativer, der skal sikre høj kvalitet i administrationen af IT-systemer på tværs af hele politiet. Disse initiativer er ikke blevet implementeret hos Rigspolitiets Telecenter.



Rigspolitiets politikker for IT-sikkerhed og dataklassifikation bør implementeres for Rigspolitiets Telecenter, så centeret følger de overordnede politikker, der er etableret bredt i Rigspolitiet og i henhold til deres rette klassifikationsniveau.

Herunder bør centeret bruge det samme rammeværk for informationssikkerhed (ISO 27001), som anvendes af Rigspolitiet, og som i øvrigt er et krav for statslige myndigheder. Rigspolitiet kan med fordel overveje certificering efter ISO 27001 på sigt for at sikre en høj grad af standardisering og procesunderstøttelse af informationssikkerheden.

# 8 Undersøgelse af kvalitetskontrol af historiske teleoplysninger

Hovedfokus i undersøgelsen af kvalitetskontrol har været at gennemgå kvalitetskontrollen af historiske teleoplysninger, der modtages, opbevares og behandles i Rigspolitiets Telecenter fra data modtages fra teleudbyderne, til de afleveres til politikredsene. Gennemgangen munder ud i anbefalinger til, hvordan denne kvalitetskontrol kan styrkes, således at der er sikkerhed for kvaliteten af de konverterede data, som efterforskeres analyser hviler på, og som fremlægges i retten.

## 8.1 Kvalitetskontrol på tværs af teledataværdikæden

I teledataværdikæden for historiske teledata sendes teledata fra teleudbyder til Telecenteret, som konverterer de modtagne data og videresender dem til den rekvirerende politikreds mv. På baggrund af gennemgangen af kvalitetskontrol er der identificeret risici, som medfører en moderat til høj risiko for usikkerheder og fejl. Disse risici er til stede på tværs af den samlede dataværdikæde fra mast til retssag, herunder iboende usikkerheder givet teledatas beskaffenhed samt manuelle og systemmæssige processer og procedurer i forbindelse med rekvisitioner af historiske teledata, jf. sektion 6 og jf. det udarbejdede uvildige notat om de opmærksomhedspunkter, man bør være opmærksom på, når historiske teledata anvendes i forbindelse med retssager.

Nedenfor gennemgås løsningsforslag til kvalitetskontroller af Telecenterets håndtering af historiske teledata. Desuden er der anbefalinger, der rækker ud over telecenteret og vedrører et styrket samarbejde med teleudbydere og politikredsene om forbedret kvalitetskontrol. Anbefalinger vedrørende Rigspolitiets systemer og infrastruktur er adresseret i sektion 7 om systemgennemgang.

### 8.1.1 Kvalitetskontrol i Telecenteret

Som det fremgik af systemgennemgangen i sektion 7 har processer og kontroller generelt været udokumenterede i Telecenteret. Der eksisterer således ikke et samlet overblik over processer, væsentlige risici i disse processer og en prioriteret kontrolindsats.

#### 8.1.1.1 Observationer om kvalitetskontrol og processer i Telecenteret

Generelt har Telecenteret ikke udført kvalitetskontrol ved modtagelse af historiske teledata fra teleudbyderne. Når Telecenteret har modtaget historiske teledata fra teleudbyderne, bliver filerne indlæst til det automatiske konverteringsprogram, såfremt at navnestandard og filtype er i overensstemmelse med foruddefinerede krav. Der bliver ikke udført

yderligere kvalitetskontrol af den modtagne fil, da der i mange rekvisitioner er tidsmæssige hensyn givet de efterforskninger, historiske teledata understøtter. Filerne, der er indeholdt i rekvisitionerne, er kun blevet kontrolleret, såfremt konverteringen slet ikke er kørt og der derfor åbenlyst har været fejl, eller såfremt politikredse mv. har gjort opmærksom på, at de modtagne filer fra Telecenteret ikke er blevet konverteret korrekt. Eventuelle ændringer i formater, der er foretaget af teleudbyderne identificeres ikke, såfremt ændringer ikke afbryder det automatiske konverteringsprogram.

Telecenteret har endvidere ikke udført konsistent kvalitetskontrol af historiske teledata i forbindelse med afsendelse af konverterede teledata til politikredse mv. Der har været opsat en kvalitetskontrol til sikring af, at den afsendte konverterede fil var i overensstemmelse med rådatafilen, men denne kontrol har været uhensigtsmæssigt konfigureret. Kontrollen er således blevet tilsidesat af den i afsnit 5.6 nævnte timer-funktion.

#### **8.1.1.2 Anbefaling til fremadrettet kvalitetskontrol og processer i Telecenteret**

Overgang til en ny infrastruktur i Telecenteret, som er nærmere beskrevet i kapitel 7, vil på sigt adressere mange af de identificerede risici, herunder vil usikkerheder i forbindelse med håndtering af teledata til politikredsene blive væsentligt reduceret ved aflevering og bearbejdning af teledata i den infrastruktur, som politiet også anvender til andre formål.

Det anbefales hertil overordnet, at der implementeres et samlet rammeværk for identifikation af risici, design og implementering af kvalitetskontroller. Som basis for dette rammeværk anbefales det at anvende kvalitetsstandarden ISO 27001 om informationssikkerhed. Standarden benyttes allerede som en del af Rigspolitiets rammeværk for IT-sikkerhed, da Rigspolitiet ligesom andre statslige myndigheder er pålagt at følge denne standard. Standarden tager udgangspunkt i en organisations risikoprofil og lægger op til, at der implementeres netop de sikkerhedsforanstaltninger og kontrolprocedurer, der er passende for Rigspolitiet. Det vil skabe grundlaget for en struktureret tilgang til afhjælpning af Rigspolitiets kontrolsvagheder. Det anbefales, at der på sigt tilstræbes en ekstern certificering med henblik på internt og eksternt at kunne dokumentere kvaliteten og derved skabe tillid omkring den.

Der er nedenfor anvist nogle supplerende og mere specifikke anbefalinger:

Der anbefales helt konkret en ny praksis omkring opdateringer af mastelister. For nuværende opdateres og deles mastelister ugentligt. Ændringer til teleudbydernes netværk og dermed mastelister forekommer dog typisk flere gange dagligt. Alle teleudbydere opdaterer interne mastelister dagligt, men Rigspolitiet har en praksis med at modtage og indlæse disse data ugentligt. Én enkel teleudbyder sender mastelisten til Telecenteret dagligt, men Rigspolitiet anvender kun listen for den dag, hvor mastelister modtages fra de øvrige teleudbydere. Det anbefales, at Telecenteret modtager og anvender opdaterede mastelister fra teleudbyderne på daglig basis.

#### **8.1.1.3 3. parts validering (K4)**

Som følge af observationer og anbefalinger omkring Telecenterets systemer og infrastruktur jf. sektion 7, anbefales det, at der *ikke* udvikles og implementeres ny systemudvikling i nuværende systemer og infrastruktur, ud over det, der skal til for at sikre den fremadrettede driftsstabilitet i en

periode, frem til en fremtidssikret løsning vil kunne være anskaffet og implementeret.

Det anbefales i stedet overordnet, at der hurtigst muligt etableres en uvildig kvalitetskontrol i form af 3. parts validering af alle konverteringer af historiske teledata. Der vil herigennem blive etableret en sideløbende og uvildig kvalitetskontrol af konverteringen af historiske teledata. Kvalitetskontrollen skal systemmæssigt understøtte en paralleliseret proces, som kan validere data uafhængigt af Telecenterets egen konverteringsproces.

Der vil således skulle etableres et automatiseret dataflow, hvor 3. parts validering indgår i flowet på en måde, hvor det påkrævede serviceniveau mod politikredsene holdes intakt, således at hastighed og effektivitet i efterforskningen ikke påvirkes væsentligt. Det bemærkes, at etablering såvel som drift af kontrollen vil indebære et ressourcetræk hos ikke bare tredjepart, men også hos Rigspolitiet.

Når det anbefales at lade en ekstern leverandør varetage valideringsopgaven, er det ud fra hensynet til at etablere den fornødne uvildighed, herunder klare aftaler om konkrete leverancer, eksempelvis i form af automatiserede og manuelle kontroller, og ikke mindst et tilstrækkeligt højt serviceniveau.

Da kvalitetskontrollen tænkes som en automatiseret proces, vil den kunne gennemføres på alle rekvisitioner.

Som input til en 3. parts valideringsplatform, skal rådatafiler (som modtaget fra teleudbyderen inden behandling i Telecenteret) samt konverteringsfiler som resultat af Telecenterets konvertering indlæses på platformen. Kvalitetskontrollen gennemføres som;

1. en validering i form af udvalgte automatiserede kontroller på hver rekvisition, eksempelvis sammenligning af antal linjer i hvert af de to datasæt, sammenligning af indholdet af udvalgte felter mv.,
2. som et supplement til de automatiserede kontroller anbefales det, at der gennemføres stikprøvegennemgang med en vis frekvens, samt
3. iii) løbende kontrol af IT-sikkerhedsmæssige forhold.

Metoden bygger overordnet på følgende grundprincipper:

- Valideringen skal omfatte alle konverterede data
- Valideringen skal gennemføres uden mulighed for påvirkning fra Rigspolitiet
- Validering må ikke reducere politiets muligheder for efterforskningmæssigt at agere hurtigt og effektivt
- Valideringen er midlertidig, men skal have en robusthed til helt eller delvist at kunne fortsætte over en længere periode
- Resultatet af valideringen skal kunne fremvises til politikredsene (politi såvel som anklagemyndighed)
- Valideringen skal være uvildig med højest mulige sikkerhed

Det anbefales tillige, at kvalitetskontrollen metodisk bygger på tre kontrolområder, hhv. dataintegritetskontrol, inddatakontrol samt kvalitetskontrol.

#### *Integritetskontrol*

Kontrollen skal sikre, at både filerne modtaget fra teleudbyderne samt konverteringsfilerne modtaget fra selve Telecenteret er intakte gennem valideringsprocessen. Ligeledes kan filerne samt filernes indhold afstemmes gennem hele valideringen og vil agere som kontrolspor mod output fra valideringen og kvalitetskontrollen i form af eksempelvis kvalitetsrapport. Integritetskontrollen bør benytte solide og anerkendte metoder for sikring af filer samt filers indhold.

#### *Inddatakontrol*

Der vil være behov for at udføre overordnede inddatakontroller, som sikrer at nøgle-felter har det forventede indhold, inden validering af rådata filer mod konverterede filer.

Inddatakontroller sikrer, at data ikke kvalitetskontrolleres, hvis der f.eks. som følge af et nyt format fra en teleudbyder ikke er det rigtige overordnede indhold.

#### *Kvalitetskontrol*

Selve kvalitetskontrollen omfatter de tre punkter nævnt ovenfor: 1) en validering i form af udvalgte automatiserede kontroller på hver rekvisition, 2) manuelle stikprøvegennemgange med en vis frekvens, samt 3) løbende kontrol af it-sikkerhedsmæssige forhold.

Da Telecenterets konvertering bygger på et højt antal forretningsregler, skal disse tilsvarende, dog uafhængigt af Telecenterets tekniske forretningsregler, reflekteres i valideringsplatformen, så sammenligningsgrundlaget er identisk. Kvalitetskontrollen skal således bygge på et antal objektive forretningsregler, der løbende tilpasses i overensstemmelse med aftalte processer mellem Telecenteret og den eksterne valideringspart.

Sammen vil ovenstående tre kontrolområder give sikkerhed for, at Telecenterets konvertering er fuldstændig og korrekt. Valideringen bør foregå parallelt med Telecenterets konverteringsproces, så at der leveres dokumentation for gennemført validering og kvalitetskontrol, når data leveres til politikredsene.

#### *Kvalitetsrapport*

Kvalitetsrapporten skal som udgangspunkt medsendes umiddelbart efter at valideringen er foretaget. Kvalitetsrapporten bør genereres automatisk, og rapporten skal angive resultaterne af konverteringen, samt eventuelle differencer og fejl. Det gør det muligt for politikredsen umiddelbart at kunne identificere de historiske teledata, hvor der reelt er risiko for fejl i datakonverteringen. Politikredsen kan i stedet anvende linjer, hvor fejl ikke som udgangspunkt er identificerede. Det anbefales, at kvalitetsrapporten tillige indeholder oplysninger om:

- Angivelse af filer modtaget og behandlet
- Angivelse af fejl i rådatafiler, såfremt at disse forefindes, som følge af manglende overholdelse af eks. datastandarder
- Angivelse af hvilke kontroller, der er udført, samt resultat heraf
- Angivelse af fejl i datakonverteringen, såfremt at disse forefindes. Dette på linje-niveau, således at politikredse klart kan se hvilke linjer i den af telecenterets konverterede fil, der ikke kan anvendes

Formålet er at angive detaljer om de gennemførte tests til politikredsene, således at de kender kvaliteten af de konverterede historiske teledata, når de anvender dem i efterforskningen.

Foruden etablering af 3. parts valideringsplatformen, bør 3. parts valideringen også sikre formelle processer og behørig kontrol, som i det væsentligste sikrer integriteten på både system- og dataniveau, samt valideringsplatformens driftsstabilitet. Der bør således sikres, at der på valideringsplatformen implementeres de nødvendige processer og procedurer, eksempelvis logisk adgangskontrol, brugeradministration, logning samt udviklings- og ændringskontroller. Processer, kontroller mv. skal være implementerede før idriftsættelsen af kvalitetskontrollen.

### **8.1.2 Observationer om kvalitetskontrol i politikredse mv.**

Fokus for undersøgelsen har været kvalitetskontroller i Rigspolitiets telecenter, men der følger i tillæg hertil en række anbefalinger vedrørende kvalitetskontrol i politikredsene mv.

Generelt har der historisk ikke været foretaget kvalitetssikring af teledata i politikredse mv. ved modtagelse af data, ligesom der ikke på nationalt plan har eksisteret retningslinjer eller vejledninger, som har kunne understøtte en lokal kvalitetssikring. Det er endvidere konstateret, at der eksisterer store forskelle i måden teledata håndteres og anvendes på tværs af politikredsene.

Før årsskiftet 2018/19 er der ikke udført fuldstændighedskontrol af modtagne teledata (sammenligning af rådata og konverterede data). Fra december 2018 er der udstukket retningslinjer for fuldstændighedskontrol ved modtagelse af teledata. Konkret består denne kontrol i, at antallet af rækker i henholdsvis rådata og konverteret data sammenlignes, når kredsene modtager data fra Telecenteret. Såfremt teledataanalytikere eller andre videnspersoner er involveret i anvendelse af teledata i en given sag, udføres kontrol af antal rækker i henhold til retningslinjer fra december 2018. Der udføres typisk ikke yderligere datakontroller såsom kontrol af overensstemmelse mellem rekvirerede og modtagne teledata, som eksempelvis vurdering af mastevalg. Endelig foretages der i politikredse generelt ikke kvalitetssikring af funktionalitet i eventuelt anvendte lokale analyseværktøjer.

Når en anklager ved anklagemyndigheden modtager en sag, vil anklageren oftest sikre, at der er overensstemmelse mellem de angivne teleoplysninger i sagsrapporten og den i bilagene medsendte konverterede datafil. Herudover foretages der typisk ikke yderligere datakontrol ved anklagemyndigheden i forbindelse med anvendelse af teledata i sager, der forelægges for retten. Den enkelte anklager modtager i langt de fleste tilfælde sagsrapporten, inklusiv bilag fra efterforsker, også i de tilfælde hvor teleanalytikere har bistået med behandling af data. Det er sædvanligvis efterforskeren, der afgør hvilke informationer fra analysen af teledata, der indgår i sagsrapporten. Som bilag vedlægges typisk den af Telecenteret konverterede data-fil.

Teleudbyderne har oplyst, at enkelte af deres medarbejdere i visse tilfælde har ydet ekspertbidrag vedrørende fortolkningen af teledata, når sager har været forelagt retten. Baseret på interviews med medarbejdere i teleudbydernes 'politikgrupper', vurderes dette dog at være yderst sjældent forekommende.

Det anbefales på den baggrund, at den viden og indsigt i teledata, som *'Notat om fejlkilder og usikkerheder ved anvendelse af teledata i straffesager'* bidrager med, kommunikeres til politikredse og anklagemyndighed. Der kan i den forbindelse overvejes løbende vidensdeling, undervisning og efteruddannelse eller andre læringsmetoder, som med fordel kan udvides til også at favne indsigt i substansen af de modtagne datafiler.

Hertil kan der med fordel etableres konkrete retningslinjer for behandling og opbevaring af teledata, herunder i lokale analyseværktøjer, således at man sikrer sig, at den analyserapport, der videregives til anklagemyndigheden datamæssigt kan spores tilbage til konverterede teledata modtaget fra telecenteret.

Det kan tillige anbefales at etablere adgang til support fra erfarne kolleger i forbindelse med behandling af komplekse sager, jf. også nedenstående anbefaling omkring etablering af et ekspertmiljø, hvor ansatte på tværs af Telecenteret, ACØ/ACV og politikredsene mv. uddannes på specialniveaueu.

Teleanalytikere og visse efterforskere i kredse mv. har over tid oparbejdet stor viden, nye metoder samt nye værktøjer til analyse af historiske teledata. Denne viden kunne med fordel deles med Telecenteret. Ligeledes har Telecenteret oparbejdet stor viden om historiske teledata, fejlkilder og usikkerheder, som også kan gavne teleanalytikerne i kredsene ift. deres analysearbejde. Det anbefales således at øge samarbejdet mellem Telecenteret og politikredse mv. og i den forbindelse nytænke rollefordelingen. I en fremtidig struktur vil det være naturligt at se på etablering af et stærkt miljø, eksempelvis ved en styrkelse af kompetencerne i Særlig Efterforskning Øst og Vest, i Telecenteret og blandt en eller få udvalgte eksperter i hver politikreds. Det vil betyde, at de ansatte, der indgår i ekspertmiljøet, tilsammen besidder de rette kompetencer, forudsat at de løbende og systematisk modtager relevant kompetenceudvikling. Det skal blandt andet sikres, at de ansatte udover tekniske færdigheder og kontinuerligt opdateret viden om teledata også har - eller får tilført - viden omkring udførsel og dokumentation af kontroller.

Som det fremgår i afsnit 6 og yderligere præciseret i notatet om anvendelse af historiske teledata i straffesager afsnit 3.2.3, er der angivet en række usikkerheder samt fejlkilder ved eksempelvis udvælgelse af master. Der kan bl.a. nævnes en række usikkerheder omkring f.eks. landskab samt omskiftelige forhold som vejr og årstid. Disse forhold kan ligeledes have en indvirkning på udvælgelsen af master og celler ift. udsøgningen af data. For at håndtere usikkerheden om fuldstændige datasæt, eksempelvis ifm. mastesug, kan der være tilfælde hvor politikredse mv., under hensyn til sagens karakter bør foretage yderligere kontrol af, om at der er udvalgt de korrekte master og celler. Baseret på erfaring fra politimyndigheder i udlandet kan de ske ved at anvende teknologier og metoder, der kan måle hvilke master og celler i et givent område, der potentielt kan være relevante for udsøgningen af teledata. Sådanne teknologier kan f.eks. overvejes anvendt i sager, herunder særligt større sager, hvor der kan være større geografiske usikkerheder, og hvor man vil efterkontrollere de leverede data.

### 8.1.3 Rigspolitiets samarbejde med teleudbydere

Teleudbydernes databehandling har ikke været i primært fokus i undersøgelsen, og der har alene været gennemført ét interview med hver af teleudbyderne. Omkring de iboende usikkerheder og fejlkilder der er i forbindelse med anvendelse i straffesager, henvises til *'Notat om fejlkilder og usikkerheder ved anvendelse af teledata i straffesager'*. En generel observation er dog, at der er forskelle ift. hvordan teledata udvælges, generes og leveres i selve rekvisitionsprocessen, herunder graden af automatiserede processer. Rekvisitionsprocessen er her defineret som den proces, hvor teleudbyderne trækker data ud af de almindelige forretningssystemer, til brug for rekvisitioner fra politikredse mv. Særligt i forbindelse med manuelle processer, øges risikoen for fejl.

Resultatet af dataanalysen, jf. sektion 5, viser at der historisk set er forekommet fejl i rådata afleveret til Rigspolitiet. Det ligger uden for Deloitte's opdrag at komme med mere konkrete observationer og anbefalinger i forhold til kvalitetskontrol hos teleudbyderne.

For så vidt angår samarbejdet mellem teleudbyderne og Rigspolitiet, er det anbefalingen, at samarbejdet bør styrkes. Det er vurderingen, at et styrket samarbejde i væsentlig grad vil være til gavn for begge parter og styrke den generelle tillid til anvendelse af historiske teledata i straffesager. Et fremadrettet samarbejde bør både angå et strategisk niveau, men også på et mere dagligdags operationelt niveau. Bortset fra formelle kontraktforhandlinger hvert andet år, er dialogen mellem Rigspolitiet og teleudbyderne i dag begrænset. Rigspolitiet vil på det strategiske niveau have gavn af en bedre forståelse af teledata og den teknologiske udvikling i forhold til fremtidens muligheder og behov. På det operationelle niveau er løbende opdateret viden om eksempelvis ændring af formater nødvendig i forhold til tilretning af applikationer og databaser og dermed korrekt konvertering og korrekt 3. parts validering. Det vurderes ligeledes, at det vil være givtigt for begge parter, såfremt teleudbyderne bibringes en bedre forståelse af Rigspolitiets ønsker og anvendelsesbehov, bl.a. for hensigtsmæssigt at kunne tilrettelægge egne processer, kompetencer og ressourcer.

Det formelle kontraktgrundlag varierer i nogen grad på tværs af teleudbyderne og er primært rettet imod kommercielle områder som ydelser, rekvirering, priser, fakturering, styregruppe, ændringer og effektivisering. Kontrakterne forholder sig således ikke til vidensdeling, dataformater, kvalitet, processer, kontrol, informationssikkerhed og i begrænset omfang til governance og kommunikationsveje. Vi anbefaler, at parterne fremover også inddrager disse områder i samarbejdet.



# 9 Bilag: Introduktion til historiske teledata og teleinfrastruktur

## 9.1 Definition af historiske teledata

Genstandsfeltet for undersøgelsen er historiske teledata (dvs. beskrivelser af hændelser, der har fundet sted, og ikke hændelser der finder sted) samt data, der er transporteret via mindst én mobilantenne. Undersøgelsen behandler anvendelse af historiske teledata i straffesager, jf. retsplejeloven.

Genstandsfeltet er primært logningspligtige data, dvs. afsluttet og registreret teletrafik vedrørende tale, sms, mms og data. Logningen vedrører ikke indholdet af trafikken, herunder f.eks. optagne samtaler, indholdet af sms og mms-beskeder eller data. De historiske data omhandler alene tidspunktet, tjenestetypen, anvendt mast(er), første og sidste celle i transmissionen samt cellernes retning og de involverede mobile enheder. Fokus er således alene en vurdering af det forhold, at aktiviteterne har fundet sted, hvilke enheder der deltog i aktiviteterne og hvilken infrastruktur, der registrerede hændelsen.

## 9.2 Logning af historiske teledata

Historiske teledata fra teleselskaberne reguleres af logningsbekendtgørelsen<sup>2</sup>, der definerer de historiske teledata, som teleudbydere har pligt til at registrere og opbevare. Efter retsplejelovens § 786, stk. 4, påhviler udbydere at foretage registrering og opbevaring af teleoplysninger i ét år. Logningsbekendtgørelsen forpligter teleudbydere til at logge oplysninger, der genereres eller behandles i udbyderens net. Oplysninger om teletrafik, der f.eks. af tekniske grunde ikke genereres eller behandles i udbyderens net, skal derfor ikke logges.

De specifikke oplysninger, som udbydere har pligt til at registrere, specificeres i logningsbekendtgørelsens §§ 4-6. Fælles for de data der registreres er, at der er tale om trafikoplysninger. Udbydere skal derfor ikke registrere og opbevare selve indholdet af kommunikation, hverken i forbindelse med telefonsamtaler mv., brug af internettet eller brug af udbyderens e-mailtjenester. Logningsbekendtgørelsen definerer ikke formatet for de logningspligtige data, hvorfor de leveres til politiet i et format defineret af den enkelte teleudbyder.

Det fremgår af logningsbekendtgørelsens § 4, nr. 1-8, at teleudbydere skal registrere følgende oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation:

<sup>2</sup> BEK nr. 988 af 28/09/2006, BEK nr. 660 af 19/06/2014

- Opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger
- Opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger
- Ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger
- Kvittering for modtagelse af meddelelser
- Identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre)
- Den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen (masteoplysninger)
- Tidspunktet for kommunikationens start og afslutning
- Tidspunktet for første aktivering af anonyme tjenester (taletidskort)

### 9.3 Introduktion til teleinfrastruktur og historiske teledata

Kommunikation til og fra mobiltelefon sker via sendemaster. Mobile enheder 'finder selv' master med afsæt i, hvor dækningen er bedst. En enhed skifter derfor fra mast til mast, når brugeren bevæger sig.

Der er to grundprincipper, der afgør, hvornår der skiftes mast. I *idle mode* (dvs. når enheden ikke har en aktiv forbindelse) vælger mobiltelefonen selv den bedste mast, baseret på instrukser fra mobilnettet. I *idle mode* registreres kun når den mobile enhed skifter mellem en gruppe af celler. I *connected mode* (når den mobile enhed har en aktiv forbindelse til tale eller internet) bestemmer mobilnettet suverænt baseret på målinger fra mobiltelefonen. I *connected mode* styres skift fra celle til celle (hand-over) suverænt af netværket, som derfor registrerer positionen på celleniveau. I begge tilstande samles alle oplysninger om enhederne centralt i udbydernes core net. Enheder skifter mellem de to tilstande. Er en enhed f.eks. i *connected mode*, men har været inaktiv i noget tid, vil den skifte til *idle mode*. Det afhænger af netværkskonfigurationen hvor hurtigt dette sker (typisk efter nogle hundrede millisekunder).

Hver sendemast har et antal transmissionsceller (typisk tre), som hver især dækker omkring 120 grader rundt om sendemasten. Der findes ligeledes omni-direktionelle antenner, der dækker 360 grader rundt om masten. Det præcise dækningsområde for en celle afhænger af en lang række faktorer, blandt andet antennens justering, frekvensbånd og sendestyrke.

Et mobilkommunikationsnet holder styr på hvor telefonerne befinder sig, enten på cellegruppe- eller celleniveau (en cellegruppe udgøres af en række celler, der er grupperet i netværket). Dette er nødvendigt for at kommunikationen på netværket kan fungere korrekt. Der sker en løbende registrering af, hvilke transmissionsceller en enhed har anvendt i forbindelse med start og afslutning på kommunikation, samt registrering af hvilken sendemast kommunikationen anvender. Registreringen konsolideres hos det enkelte teleselskab med henblik på at understøtte forretningsbehov, herunder taksering af ydelser og fakturering af kunder. Den enkelte teleudbyder vedligeholder ligeledes løbende en fortegnelse over master og transmissionsceller (masteliste), der angiver hvor den enkelte mast er placeret (adresse og koordinat), hvilke celler og teknologier der er placeret på den enkelte mast samt cellernes retning.

En bruger er identificeret via sit SIM-kort. På SIM-kortet er brugerens IMSI (International Mobile Subscriber Identification) gemt. Telefonnummeret er dermed ikke gemt på SIM-kortet. Teleudbyderne kobler telefonnummer og IMSI i deres databaser med abonnenter i nettet (Home Subscriber Server (HSS)). IMSI bruges til unikt at identificere brugeren i nettet. Af sikkerhedsmæssige grunde bliver telefonen tildelt en midlertidig identitet så snart den er registreret på nettet. Dette kaldes GUTI i 4G/LTE. I tidligere teknologier anvendtes TMSI. Selve telefonen har tilmed en identifikation, der kaldes IMEI. Denne identifikation er uafhængig af SIM-kortet og kan blandt andet bruges til at spærre stjålne telefoner.

Historiske teledata udgøres således af information om enheders trafik mellem opkaldende enheder, master og modtagende enheder. De registrerede data angår ikke indholdet af den kommunikation, der logges, men kun hvilke master der har være involveret og hvornår. Det bemærkes, at billedet kompliceres, hvis den ene af parterne bruger en mobilenhed hos en anden udbyder eller anvender en anden kommunikationsenhed end en mobil enhed (f.eks. en fastnettelefon eller en app).

# Deloitte.

## Om Deloitte

Deloitte leverer ydelser indenfor revision, consulting, financial advisory, risikostyring, skat og dertil knyttede ydelser til både offentlige og private kunder i en lang række brancher. Deloitte betjener fire ud af fem virksomheder på listen over verdens største selskaber, Fortune Global 500®, gennem et globalt forbundet netværk af medlemsfirmaer i over 150 lande, der leverer kompetencer og viden i verdensklasse og service af høj kvalitet til at håndtere kundernes mest komplekse forretningsmæssige udfordringer. Vil du vide mere om, hvordan Deloitte omkring 286.000 medarbejdere gør en forskel, der betyder noget, så besøg os på Facebook, LinkedIn eller Twitter.

Deloitte er en betegnelse for en eller flere af Deloitte Touche Tohmatsu Limited ("DTTL"), dets netværk af medlemsfirmaer og deres tilknyttede virksomheder. DTTL (der også omtales som "Deloitte Global") og alle dets medlemsfirmaer udgør separate og uafhængige juridiske enheder. DTTL leverer ikke ydelser til kunderne. Vi henviser til [www.deloitte.com/about](http://www.deloitte.com/about) for nærmere oplysninger.