16. april 2021
(opdateret 27. april 2021)

TI's svar på Justitsministeriets spørgsmål på 2. møde om revision af logningsreglerne mv. (14. april 2021) – **tekniske forhold** og procedurer

Målrettet logning:

1. Hvilke typer af lokaliseringsoplysninger registrerer teleudbyderne i dag (er det muligt med en bruttoliste over typer af oplysninger)?

SVAR:
I følgende situationer registrerer teleselskaberne lokaliseringsdata (= hvilke masteceller en mobilterminal/mobilnummer har været registreret på):

1. Lokaliseringsdata, som er trafikdata ifm. telefoni- og sms/mms-kommunikation.
–> Logges p.t. 1 år. 1-2 registreringer pr. opkald/sms/mms.

2. Lokaliseringsdata, som er trafikdata ifm. mobildata-kommunikation (internetforbrug).
–> Registreres i kort tid til brug for fejlretning. Fx 1000* registreringer pr. døgn pr. kunde.

3. Lokaliseringsdata, som ikke er trafikdata (dvs tændte telefoner, der ikke anvendes aktivt).
–> Registreres i kort tid til brug for fejlretning. Fx 100* registreringer pr. døgn pr. kunde.

* Antallet af registreringer af lokaliseringsdata i fejlretningssystemerne (prober) afhænger af antal aktive apps på telefonen samt telefonens geografiske bevægelse, og kan variere fra ca. 100 til over 1000 registreringer af celle-ID pr. telefonnummer pr. døgn afhængig af aktivitet og bevægelsesmønster.

Det bemærkes, at der i alle tre situationer er tale om samme type lokaliseringsdata, og registreringen af lokaliseringsdata omfatter i alle tre situationer registrering af celle-ID, tidspunkt for registreringen af celle-ID samt identiteten på det benyttede abonnement (mobilnummeret/MSISDN og sim-kortnummeret/IMSI) og det benyttede kommunikationsudstyr (IMEI-nummer).

Opsamlingen og registreringen af lokaliseringsdata sker i alle de 3 nævnte situationer via analysesystemer til brug for fejlretning og drift af mobilnettet (ofte benævnt prober). Derudover opsamles parallelt via CDR-data (call detail record – "taksttelegrammer") de lokaliseringsdata, som er omfattet af de gældende logningsregler (situation 1).

For detaljeret teknisk beskrivelse: Se side 9-11 i TI's notat om teledata, sendt til Justitsministeriet og Rigspolitiet i februar 2020 (vedhæftet og på https://www.teleindu.dk/brancheholdninger/logning-og-teledata/). Bemærk TI's anbefaling i notatet side 11:

"For at undgå, at eventuelle kommende nye logningsregler bliver afgrænset utilsigtet – lige som de gældende – anbefaler TI, at eventuelle nye regler om logning af lokaliseringsdata udformes fuldstændig teknologineutralt og blot fastslår, at lokaliseringsdata, som teleudbydere opsamler og registrerer til egne formål, skal logges eller hastesikres og således opbevares i en længere periode end teleudbyderen selv har brug for (data retention, pkt. 3.1 i dette notat). For at sikre teknologineutrale regler, bør eventuelle nye regler derimod hverken forholde sig til opsamlingsmetoder (probe-systemer, CDR-systemer osv.) eller nævne specifikke tjenestetyper (telefoni, sms, mms, data), ligesom bestemmelsen ikke bør forholde sig til, om lokaliseringsdata opsamles ifm aktiv kommunikation eller ej. Pga. den omfattende mængde af data i probe-systemerne, samt teleselskabernes omkostninger til opbevaring af data, ønsker TI som nævnt i pkt. 3 en opbevaringsperiode så kort som overhovedet mulig."

2. Kan oplysningerne evt. skilles ad, og hvordan og hvor længe opbevares de i dag?

SVAR:
Lokaliseringsdata fra analysesystemerne (prober) kan kun leveres samlet til politiet. Det vil kræve betydelige omkostninger til systemudvikling, hvis de samlede oplysninger om lokaliseringsdata skal skilles

ad. Telebranchen ønsker en uddybning af baggrunden for spørgsmålet, herunder hvorfor der skulle være behov for at adskillelse.

De p.t. logningspligtige lokaliseringsdata (situation 1) kan leveres separat, idet lokaliseringsdata ifm telefoni og sms kan opsamles parallelt via CDR-data. Teleselskaberne logger disse lokaliseringsdata i 1 år efter de gældende regler om logning.

3. Hvilket format vil de kunne leveres i?

SVAR:
Se svar nedenfor under "tværgående emner"

4. Er der kapacitetsmæssige udfordringer, som vi skal være opmærksomme på?

SVAR:
Pga. den omfattende mængde af data i analysesystemerne (prober), samt teleselskabernes omkostninger til opbevaring af data, ønskes en opbevaringsperiode så kort som overhovedet mulig. Ved drøftelserne mellem telebranchen, Justitsministeriet og Rigspolitiet i 'den tekniske arbejdsgruppe' i 2018, blev opbevaringsperioder på 3 måneder eller 6 måneder drøftet og teleselskabernes byrde forbundet hermed blev undersøgt. Telebranchen finder det på den baggrund beklageligt, at der nu lægges op til en opbevaringsperiode på 1 år.

I forhold til spørgsmålet om, at registrering af lokaliseringsdata fra fejlretningssystemer sker efter "best effort" – som blev drøftet på vores møde den 14. april – bemærkes, at dette skal ses som en faktum-oplysning og ikke som kapacitetsmæssig udfordring. Teleselskaberne driver således kommunikationssystemer og ikke overvågningssystemer, og mængden af data, som opsamles, er således baseret på en forretningsmæssig beslutning om, hvad der er nødvendigt og tilstrækkeligt for driften af mobilnettet. Telebranchen vil således under ingen omstændigheder kunne acceptere eventuelle krav om etablering af yderligere kapacitet i probe-systemerne af hensyn til politiets efterforskningsmuligheder og overvågning.

For en nærmere beskrivelse af registreringen af lokaliseringsdata i netudbydernes probe-systemer efter "best effort" henvises til side 10 i TI's notat om teledata, februar 2020:

"*Særligt i forhold til registrering af lokaliseringsdata i probe-systemerne skal det bemærkes, at registrering kun kan ske efter "best effort", idet alle data kun opsamles, hvis kapaciteten i teleudbydernes opsamlingssystemer er tilstrækkelig. Teleudbyderne har selv interesse i at opsamle flest mulige trafikdata og lokaliseringsdata i probe-systemerne til brug for fejlretning, og teleudbyderne tilpasser derfor løbende kapaciteten i probe-systemerne. I sjældne tilfælde – fx ifm uforudset øget trafik i mobilnettene – kan der dog forekomme mangel på kapacitet i probe-systemerne, og i så fald vil den opsamlede mængde af lokaliseringsdata blive reduceret. Selv i disse sjældne situationer, opsamles der dog typisk stadig langt flere registreringer af lokaliseringsdata pr. mobilterminal i probe-data end i CDR-data. Dertil kommer, at probe-systemet primært er beregnet til støtte for driften af mobilnettet, og probe-systemerne understøttes derfor ikke med back-up og fuldt service-level 24/7, …*"

5. Hvordan defineres slutbrugeren af en enhed mest hensigtsmæssigt, og hvordan overgives denne mest hensigtsmæssigt mellem udbyderne og politiet? Hvis ikke CPR-nr. er det mest hensigtsmæssige, hvordan sikrer vi så, at personer entydigt logges?

SVAR:
Telebranchen henstiller, at personbestemt målrettet logning af trafik- og lokaliseringsdata iværksættes ved angivelse af personens telefonnumre i politiet pålæg – på samme måde som kendelser om udlevering af trafik- og lokaliseringsdata skal indeholde oplysning om telefonnummer, jf. RPL § 783.

Det er telefonnummeret (MSISDN) der entydigt identificerer både mobil- og fastnetabonnementer, og det er denne identitet, som netværksudbyderen bruger til fremføringen af trafik i telenetværket. Telefonnummeret for et abonnement er også registreret i tjenesteudbyderens administrative systemer sammen med kundens navn og adresse (kundedata). Telefonnummeret er derfor "nøglen" til at sammenholde trafik- og lokaliseringsdata fra netværksudbyderens net ("trafikmaskinen") med kundedata i tjenesteudbyderens administrative systemer. Det bemærkes, at netværksudbyderen og tjenesteudbyderen ofte er forskellige selskaber. På mobilområdet findes der således over 100 tjenesteudbydere i Danmark, der udbyder mobilabonnementer, herunder såkaldte gensælgere. Der findes derimod kun 4 mobilnetværksudbydere. Nogle netværksudbydere er også tjenesteudbydere, og udbyder abonnementer i forskellige brands på eget netværk. Men der findes også rene netværks-udbydere, der ikke udbyder abonnement på tjenester til slutbrugere – fx er TDC-koncernen netop i gang med en opsplitning i et netselskab (TDC NET (A/S), der kun udbyder netværksadgang engros til tjenesteudbydere, og et tjenesteselskab (Nuuday A/S), der kun udbyder abonnementer til slutbrugere.

De 4 mobile netværksudbydere, der skal iværksætte logning af trafik- og lokaliseringsdata, har ikke adgang til de mere end 100 tjenesteudbyderes administrative systemer med kundedata, hvor CPR-nummer registreres, hvis tjenesteudbyderen har indhentet oplysning herom. CPR-nummer (eller kundens navn og adresse) er derfor ikke egnet som identifikation ved politiets iværksættelse af målrettet logning. Telebranchen henstiller, at personbestemt målrettet logning af trafik- og lokaliseringsdata i stedet iværksættes ved angivelse af personens telefonnumre i politiet pålæg, jf. princippet i RPL § 783.

Politiets kan via efterforskning, herunder opslag i 118-databasen, afdække, hvilke telefonnumre en fokusperson har adgang til. Via politiets adgang til 118-databasen inkl. hemmelige numre, har politiet adgang til at slå op, hvilke telefonnumre, der er registreret på fokuspersonens folkeregisteradresse, herunder både abonnementer/telefonnumre som fokuspersonen selv er registreret for, og hvilke abonnementer/telefonnumre som i øvrigt er registreret på fokuspersonens folkeregisteradresse (fx fokuspersonens ægtefælles abonnementer/telefonnumre). Rigspolitiet kan til brug for den løbende efterforskning overveje at etablere en it-løsning til adresse-overvågning i politiets adgang til 118-databasen, som automatisk overvåger ændringer mht. oprettelse eller nedtagning af (mobil)telefonabonnementer på fokuspersonens folkeregisteradresse. På baggrund af de telefonnumre, som politiet finder frem til i efterforskningen, kan politiet herefter pålægge en eller flere af de 4 netværksudbydere at iværksætte målrettet logning af trafik- og lokaliseringsdata for de identificerede fokusnumrene. Ved kun at udstede pålægget til de 4 netværksudbydere opnås desuden at viden om fokusnumrene/fokuspersonen ikke spredes til alle over 100 danske tjenesteudbydere [herunder eventuelle fiktive tjensteudbydere, som er kriminelle].

Via politiets adgang til OCH-databasen (operators clearing house) kan politiet slå op, hvilken netværksudbyder (og hvilken tjenesteudbyder), fokusnumrene aktuelt benytter, ligesom OCH-data løbende opdateres, hvis der sker nummerportering til en anden udbyder. På samme måde som for 118-data, kan det overvejes at etablere en it-løsning til overvågning af bevægelser for fokusnumre i politiets adgang til OCH-databasen.

Det bemærkes, at der kun er Politiet (og visse andre myndigheder), der er fuld adgang til 118-databasen inkl. hemmelige numre – de enkelte teleselskaber har ikke adgang.

6. Hvilke muligheder er der for at identificere en bruger hos et CVR-nr.?

SVAR: Politiet kan henvende sig til erhvervskunden og anmode kunden om at oplyse navnet på de ansatte hos erhvervskunden, som benytter erhvervskundens mobilabonnementer.

7. Er det korrekt forstået, at abonnementsoplysninger ikke registreres i samme system som trafikoplysninger hos teleudbyderne – hvilke udfordringer giver det?

SVAR: Ja, det er korrekt.

Kundedata (navn, adresse og abonnementsaftaler, herunder telefonnumre) registreres i administrative systemer hos de teleselskaber, som udbyder teletjenester til slutbrugere (tjenesteudbydere). Der findes i dag ca. 100 teleselskaber/brands, der udbydere mobiltjenester til slutkunder.

Trafik- og lokaliseringsdata registreres i net og centraler (trafikmaskinen) hos de teleselskaber, som udbyder telenet (netudbydere). Der findes i dag 4 netudbydere på mobilområdet (mobiloperatører): Telia, Telenor, Hi3G og TDC NET.

Det er derfor ikke muligt at samkøre kundedata med trafik- og lokaliseringsdata.

Se også beskrivelsen af forskellen på tjenesteudbydere og netudbydere ovenfor under punktet om CPR.

8. Hvordan afgrænses et geografisk område mest hensigtsmæssigt? Hvordan kan et område afgrænses teknisk?

SVAR: Se TI's mail den 19. januar 2021:

*"Det følger af RPL § 783, at kendelser om 'udvidet teleoplysning' skal gå på **'lokalitet'**. TI ønsker en drøftelse til fælles teknisk forståelse af, at målrettet geografisk logning på samme måde skal gå på en afgrænset lokalitet/fokusområde, herunder med henblik på en fælles forståelse af følgende:*

a. *Det er altid teleudbyderens ansvar at udpege, hvilke celler der dækker fokusområdet (**celleudvælgelse**), herunder genberegning af celleudvælgelse ved ændringer i netværket.*
b. *Beslutning om målrettet geografisk logning skal blot angive fokusområdet som **et punkt/fokusadresse** eller **et nøje afgrænset område**.*
c. *Hvis fokusområdet strækker sig ud over én adresse, afgrænses fokusområdet præcist – **som udgangspunkt** som en **polygon** via markering på et kort (fx et område mellem gader), gerne suppleret med koordinater for punkter, der afgrænser området.*
d. ***I sjældne tilfælde** kan fokusområdet være **cirkelformet** (punkt med en radius), hvis der er efterforskningsmæssige grunde hertil (fx flugtbilist med ukendt retning).*

9. Hvordan udvælger teleudbyderne de master, der dækker et sådant område? Shape med GPS-punkter, bydel, postnummer? Er der begrænsninger i størrelsen på områder?

SVAR:

Teleudbyderens udvælgelse af master (celleudvælgelsen) sker ud fra en radioteknisk vurdering af, hvilke masteceller, der giver dækning på fokusadressen/fokusområdet. Processen for celleudvælgelse er forskellige fra udbyder til udbyder. For detaljeret teknisk beskrivelse: Se side 5 i TI's notat om tekniske fakta vedr. teledata (faktumnotatet), sendt til Domstolsstyrelsen m.fl. i marts 2021 (vedhæftet og på https://www.teleindu.dk/brancheholdninger/logning-og-teledata/).

Det henstilles, at processen for celleudvælgelse ikke beskrives i lovforslag og regler, men at det blot nævnes i lovforslaget, at det altid er teleudbyderens ansvar at udpege, hvilke celler der dækker et fokusområde – ud fra en radioteknisk vurdering.

Det er væsentligt at bemærke, at de udvalgte masteceller, som dækker fokusadressen/fokusområdet, også dækker et stort område rundt om fokusområdet, og at loggede trafik- og lokaliseringsdata derfor på ingen måde kan afgrænses til kun at omfatte mobiltelefoner, der har befundet sig på fokusområdet. Ved pålæg om udlevering af oplysninger om hvilke numre, der har været registreret på masteceller, der dækker et

fokusområde, vil udlevering af loggede trafik- og lokaliseringsdata derfor indeholde en meget stor mængde "falske spor". Se også beskrivelsen af denne problemstilling på side 5-6 i TI's faktumnotat:

"Dertil kommer, at der ved udlevering af "lokaliseringsdata" for en given mastecelle, sker udlevering af oplysning om alle mobilterminaler/numre, der har benyttet cellen i hele cellens dækningsområde – et område som afhængig af mastetætheden i området kan være flere kvadratkilometer stort. Dette skyldes, at oplysning om hvilke terminaler/numre, der har været registreret på en mastecelle, ikke indeholder oplysning om terminalens afstand til masten eller terminalens præcise geografiske position i øvrigt.

Ved teleselskabernes udlevering til politiet af "lokaliseringsdata for et område/adresse" – dvs oplysninger om, hvilke mobilterminaler (numre), der har været registreret på masteceller, der dækker et nærmere afgrænset fokusområde/adresse – udleveres således oplysning om de mange personer [men ikke alle], som har befundet sig i hele det store område rundt om fokusadressen, som er radiodækket af alle de masteceller, der bidrager til dækning på fokusadressen. Afhængig af mastetætheden i det pågældende område udleverer hver af de 4 mobilskaber normalt oplysning om flere tusinde mobilnumre pr. time pr. fokusadresse i de større byer."

10. Er der noget, der proceduremæssigt er vigtigt for teleudbyderne ifm. politiets pålæg om målrettet logning?

SVAR:
Telebranchen vil vende tilbage med eventuelle yderligere input til det proceduremæssige, inden mødet den 28. april.

SVAR (27. april 2021):
Politiets pålæg om målrettet person logning skal indeholde oplysning om det eller de konkrete fokusnumre, der skal logges - se svar spørgsmål 5.

Politiets pålæg om målrettet geografisk logning skal indeholde præcis oplysning om fokusområdet - se svar på spørgsmål 8.

Telebranchen anbefaler, at politiets afgørelser om pålæg af målrettet logning altid træffes centralt af Rigspolitiet – det vil sige ikke af de enkelte politikredse. Telebranchen forudsætter endvidere, at der fastsættes præcise regler om i hvilke konkrete tilfælde, det vil være proportionalt at udstede pålæg om målrettet logning, og at der endvidere fastsættes regler om domstolskontrol af sådanne pålæg.

Henset til den forventede store mængde af afgørelser/pålæg om iværksættelse af målrettet logning og de kapacitetsmæssige udfordringer dette vil give netudbyderne, hvis målrettet logning skal iværksættes eller nedtages for mange fokusnumre eller fokusområder samtidig, henstiller telebranchen, at Rigspolitiet etablerer et system, hvor Rigspolitiet med aftalte intervaller vedligeholder en liste i standardiseret format over igangværende målrettede logninger. Listen skal omfatte de konkrete fokusnumre og konkrete fokusområder, som politiet aktuelt har truffet afgørelse om at logge.

For målrettet geografisk logning, kan listen være fælles for alle netudbydere under hensyntagen til fortrolighed og sikkerhedsproblematikker. For målrettet personbestemt logning, bør listen af fortrolighedshensyn opdeles pr. netudbyder på baggrund af politiets opslag i OCH om, hvilken netværksudbyder fokusnumrene aktuelt benytter.

Det foreslås, at politiet tildeler hver enkelt målrettede logning et selvstændigt ID/løbenummer, som kan medvirke til overblik, således at fx en individuel målrettet logning for et fokusnummer kan

slettes/videreføres uafhængig af en målrettet geografisk logning for et fokusområde, hvor samme fokusnummer kan have opholdt sig.

Politiets system bør have et veldefineret API, hvorfra netudbyderne kan hente oplysningerne – på sigt automatisk, hvis netudbyderne hver især ønsker at indrette IT-systemer, der kan hente data om fokusnumre og fokusområder automatisk.

Telebranchen henstiller, at de proceduremæssige forhold ikke beskrives i lovforslaget, men håndteres og drøftes løbende mellem telebranchen og Rigspolitiet i regi af Rigspolitiets Telebrancheforum.

11. Hvad er den forventede tidshorisont fra politiets pålæg til logningen starter?

SVAR:
Telebranchen henstiller, at pålæg om målrettet logning som udgangspunkt udstedes indenfor almindelig kontortid. I særlige situationer, hvor det findes nødvendigt at udstede pålæg om målrettet logning "uden ugrundet ophold", kan politiet rette henvendelse 24/7 til netudbydernes døgnbetjente kontaktpunkter.

Det bemærkes, at trafik- og lokaliseringsdata også vil kunne hastesikres, idet teleselskaberne i alle tilfælde registrerer trafik- og lokaliseringsdata i kort tid (fx 14 dage) til brug for fejlretning. Se bilag til TI's mail den 19. januar 2021 (vedhæftet opdateret version fra april 2021).

12. Hvad er den forventede tidshorisont fra politiet oplyser, at personer og/eller geografiske områder ikke længere skal logges til logningen stopper?

SVAR: Det afhænger af proceduren.

13. Kan der være en fælles database for alle i telebranchen, som alle trækker logningspligtige oplysninger fra?

SVAR: Spørgsmålet bedes uddybet og forklaret. Se også svar på spørgsmål 10.

Hastesikring:

14. Hvilke trafik- og lokaliseringsdata, der ikke er logningspligtige, behandles af teleudbyderne?

SVAR:
Se bilag til TI's mail den 19. januar 2021 – vedhæftet findes opdateret version fra april 2021. Som det fremgår af den opdaterede version, registrerer netudbyderne (de fire mobiloperatører) også teleoplysning i form af indkommende kald (tilkald) i en kort periode til brug for fejlretning, og det tidligere oplyste "nej" i række 2 er derfor rettet.

15. Er der udfordringer ved, at et pålæg om hastesikring ikke har samme datamæssige omfang som et pålæg om målrettet logning?

Justitsministeriet har på mødet den 14. april uddybet spørgsmålet, som vedrører det forhold, at nogle teleselskaber hidtil har haft systemmæssige problemer med at reducere udtræk til hastesikring af data, hvis den efterfølgende editionskendelse omfatter en mindre datamængde (fx en kortere periode) end den datamængde, som politiet har pålagt teleselskabet at hastesikre.

SVAR:
Det forventes ikke, at problemstillingen vil gælde tilsvarende ift. pålæg om målrettet logning, da det vil være nødvendigt for teleselskaberne at implementere nye tekniske systemer som understøtter muligheden for målrettet logning at trafik- og lokaliseringsdata. Telebranchen er opmærksom på at eventuel efterfølgende udlevering af loggede data (efter kendelse) ikke vil omfatte samtlige de loggede data.

16. Hvordan hastesikrer teleudbyderne i dag på baggrund af et pålæg om hastesikring fra politiet? (Og kan det bruges til inspiration for ordningen om målrettet logning?)

SVAR:

Hastesikring af teledata og målrettet logning af teledata minder på mange måder om hinanden, men der er dog forskelle:

Hastesikring vedrører en bestemt fokusperiode, som er passeret (bagudrettet) – og hastesikrede data vil normalt altid skulle udleveres til politiet (når kendelse er indhentet).

Målrettet logning skal ske løbende fremadrettet – og skal kun udleveres delvist, hvis der opstår konkrete nye straffesager, der vedrører fokuspersonen eller fokusområdet. Dertil kommer, at målrettet geografisk logning løbende skal tilpasses mht. genberegning af celleudvælgelse ved ændringer i mobilnettet, ligesom målrettet person logning, løbende skal tilpasses, hvis politiets efterforskning afdækker, at der sker ændringer mht. hvilke numre, der benyttes af en person.

17. Oplever teleudbyderne udfordringer med administrationen af sådanne pålæg om hastesikring?

SVAR: Hastesikring af lokaliseringsdata fra analysesystemerne (prober) er p.t. en tung manuel procedure, idet systemerne ikke er beregnet til udtræk af data.

Tværgående elementer:

18. Hvis teleudbyderne skal levere i ensartet format – hvilket format vil så være det mest egnede? (det gør sig både gældende for indhold og format, således at det er ens på tværs af alle udbydere uanset nye teknologier)

(3. Hvilket format vil [lokaliseringsdata] kunne leveres i?)

SVAR:

Som aftalt på mødet mellem telebranchen og JM den 14. april afventes input om Rigspolitiets foretrukne format.

Teleselskaberne er åbne overfor at udvise fleksibilitet mht. den form, som benyttes til selve udleveringen af trafik- og lokaliseringsdata til politiet, herunder indrette udleveringen i den form som politiet ønsker, fx kommasepareret fil (CSV), Excel-fil eller andet. Teleselskaberne er også åbne overfor politiets ønsker om rækkefølgen i kolonnerne i filer med udtræk af trafik- og lokaliseringsdata.

Teleselskaberne kan derimod ikke tilbyde at acceptere begrænsninger for selve dataformatet for trafik- og lokaliseringsdata (selve indholdet/syntax for data), idet dataformatet i disse rå-data kan variere afhængig af hvilken systemleverandør netudbyderen har valgt (fx Ericsson, Nokia eller Huawai). Selve produktionsapparatet er således forskelligt fra netudbyder til netudbyder og fra tjeneste til tjeneste. Idet omfang teleselskaberne har teknisk mulighed for at tilpasse dataformatet uden systemtilpasninger, vil teleselskaberne dog også ift. selve dataformatet for trafik- og lokaliseringsdata kunne udvise fleksibilitet i forhold til Rigspolitiets ønsker.

Det bemærkes, at oplysning om geografiske koordinater for mastecellers placering ikke i sig selv er en del af trafik- og lokaliseringsdata (lokaliseringsdata omfatter således kun selve celle-ID samt tidsstempling og nummer). De geografiske koordinator for mastecellers placering registreres derimod i netudbyderens basestation-tabeller, som er separate databaser. Hvis anvendelse af forskellige koordinatsystemer fra netudbyder til netudbyder er et problem ift. politiets arbejde med brug af lokaliseringsdata, anbefales det, at der iværksættes en undersøgelse hos de fire mobiloperatører (netudbydere) om muligheden for at netudbyderen konverterer til det fælleseuropæiske koordinatsystem ETRS89, herunder de administrative byrder forbundet hermed.

Det bemærkes endvidere, at oplysninger om kundedata (navn, adresse og telefonnummer/abonnementer) registreres i separate administrative systemer hos tjenesteudbyderne. Netudbyderen og tjensteudbyderen er ofte to forskellige teleselskaber.