

Avtale mellom Arbeiderpartiet og Høyre om Prop. 49 L (2010-2011)

Innledning

Partene er enige om å gjøre endringer i norsk lovgivning om lagring og sletting av elektroniske trafikkdata som følger av herværende avtale. Denne avtalen innebærer også en gjennomføring av EUs datalagringsdirektiv i norsk rett. Dette styrker kampen mot alvorlig kriminalitet. Trafikkdata fra elektronisk kommunikasjon går nå fra å bli lagret av et kommersielt hensyn – fakturering - til et samfunnsmessig hensyn - kriminalitetsbekjempelse. I dag lagres trafikkdata i enkelte tilfeller uten lovhjemmel, ofte i for kort tid og i blant lengre enn tillatt. Regelverket partene har blitt enige om vil styrke personvernet på dette og andre områder.

Å delta i det europeiske justis- og politisamarbeidet er avgjørende for kriminalitetsbekjempelsen i Norge. Kriminaliteten kjenner ingen grenser. Det må gjenspeiles i politiets arbeidsmetoder og verktøy. Teknologien kan ikke reguleres kun gjennom nasjonal lovgiving, den er grunnleggende internasjonal. Etterforskning av internasjonale terrorhandlinger er et godt eksempel på det. Endringene som nå gjøres i ekomloven mv. sikrer at norsk politi får nødvendige verktøy og sikrer samtidig den enkeltes trygghet og personvern. Politiet har hittil ikke kunnet etterforske og oppklare en rekke alvorlig straffbare forhold fordi Norge har manglet et lovverk som sikrer nødvendig lagring av kundeidentitet bak IP-adresser. Partene sikrer nå et slikt lovverk. Ekomtilbydere pålegges en plikt til å lagre data som sier noe om hvilke kommunikasjonsmidler som har vært i kontakt, hvor kommunikasjonen har funnet sted, når og hvordan.

Disse lovendringene er samtidig et viktig bidrag for å ivareta personvernet. På svært kort tid er det blitt slik at teknologien gjennomsyrrer hverdagen vår. Personvernet er i dag under press på mange områder i samfunnet. For å ivareta personvernet innføres det strenge regler for uthenting, oppbevaring og sletting av data. Eksempler på dette er 6 måneders lagringstid, at politiet må ha rettens kjennelse ved utlevering av data, høy strafferamme og sletteplikt. Samtidig forutsetter vi at Datatilsynet styrker sin kontrollvirksomhet medekomtilbyderne.

Som følge av denne avtalen styrkes den enkeltes rettssikkerhet, personvern og trygghet.

1. Typer data

Partene slutter seg til regjeringens forslag om hvilke typer data som skal lagres. Lovendringen vil medføre innføring av lagringsplikt for trafikkdata, lokaliseringsdata og abonnements-/brukerdata som fremkommer ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni.

2. Lagringstid

Partene er enige om at data som skal lagres i medhold av datalagringsdirektivet, lagres i 6 måneder. Hensynet til personvern tilsier at de relevante data ikke skal lagres lengre enn hva som er strengt nødvendig av hensyn til kriminalitetsbekjempelse. Lagringsplikten avløses av sletteplikt i medhold av § 2-7 annet ledd. Lagringstid er et av forholdene som skal være gjenstand for evaluering, jfr. avtalens pkt. 10.

Lagringspliktsbestemmelsen ser etter dette slik ut:

§ 2-7a. Plikt til lagring av data

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal lagre trafikkdata, lokaliseringsdata og data nødvendig for å identifisere abonnenten eller brukeren i 6 måneder til bruk for etterforskning, oppklaring og straffeforfølgning av alvorlige straffbare forhold. Plikten etter første punktum gjelder data som genereres eller behandles i tilbyders elektroniske kommunikasjonsnett ved bruk av fasttelefon, mobiltelefon, internettelefoni, internettaksess og e-post.

Myndigheten kan gi forskrift, treffe enkeltvedtak eller inngå avtale om plikten til å lagre data, herunder om tiltak for å ivareta dataenes konfidensialitet, integritet og tilgjengelighet. Myndigheten kan gi forskrift om at tilbyder kan kreve fremlagt politiattest fra personer som skal behandle lagringspliktige data på tilbyderens vegne. Myndigheten kan ved forskrift eller enkeltvedtak helt eller delvis frita fra plikten til å lagre data etter første ledd eller helt eller delvis pålegge andre enn de som omfattes av første ledd plikt til å lagre data dersom dette må til for å oppnå formålet med bestemmelsen.

3. Innskjerpelse av sletteplikten

Partene er enige om ytterligere tydeliggjøring av sletteplikten knyttet til lagringsplikten i forhold til det som kommer fram av forslaget til endringer i ekomloven § 2-7 med tilhørende særmerknad i Prop. 49 L (2010-2011). Sletteplikten kommer tydelig til uttrykk i forslag til endringer i ekomloven § 2-7 annet ledd. Overskriften bør endres for å avspeile dette.

Overskriften i ekomloven § 2-7 skal lyde:

“§ 2-7. Kommunikasjonsvern mv. *Plikt til å slette data.*”

4. Ansvar for lagring

Partene er enige om at ekomtilbyderne selv skal ha ansvar for lagring. Partene har særlig vektlagt personvern- og sikkerhetsmessige hensyn når det ikke foreslås å etablere en sentral lagringsløsning. Det er da opp til den enkelte tilbyder å velge lagringsløsning. Små tilbydere kan også gå sammen om en felles lagringsløsning.

5. Sikringstiltak

a) Konesjonsplikt

Partene er enige om å endre forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften) slik at § 7-1 lyder:

”§ 7-1. Konesjonsplikt for behandling av personopplysninger i ekomsektoren

Behandling av personopplysninger for kommunikasjons- og faktureringsformål, samt for å oppfylle plikten til å lagre data i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 2-7 a første ledd hos tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste, er konesjonspliktig etter personopplysningsloven.

Sanksjoner

Partene er enige om at det må knyttes sanksjoner til brudd på konesjonsvilkårene fastsatt i medhold av personopplysningsloven.

- Sanksjoner er straff i form av bøter eller fengsel, jf. personopplysningsloven § 48 og erstatning, jf. personopplysningsloven § 49.
- I tillegg kan det ilegges administrative sanksjoner i form av overtredelsesgebyr for manglende regeletterlevelse, jf. personopplysningsloven § 46 eller tvangsmulkt for manglende oppfyllelse av pålegg om overtredelsesgebyr, jf. personopplysningsloven § 47.

b) Autorisering av personell

Partene er enig om at personer som på vegne av den enkelte ekomtilbyder skal behandle data som faller under lagringsplikten, skal godkjennes (autoriseres) av ekomtilbyderen i hvert enkelt tilfelle:

- Ved vurdering av om autorisasjon skal gis, og ved revurdering av om autorisasjon skal opprettholdes, følges gjeldende retningslinjer. Slike retningslinjer utformes av Datatilsynet og Post- og teletilsynet i fellesskap. Retningslinjene skal omtale behov for politiattest.

- Pålegg om taushet om det en person blir kjent med under behandlingen av lagringspliktige data, herunder etter at han fratrer sin stilling, samt undertegning av taushetserklæring.
- Ekomtilbyderen gjennomfører periodevise autorisasjonssamtaler med den autoriserte. Samtaler gjennomføres minst årlig, samt ved tiltreden og fratreden fra stilling.
- Ekomtilbyderen skal føre kontroll med at de personer som behandler data har god kunnskap om regelverket for tilgang til og beskyttelse av dataene.

c) Kryptering og lukket lagring

Partene er enige om at kryptering er et godt tiltak for å sikre dataenes konfidensialitet. Partene er enige om at Datatilsynet gis myndighet til å gi pålegg til tilbydere om å foreta kryptering av data som faller under lagringsplikten etter (ny) ekomlov § 2-7 a. Omfanget av krypteringen, herunder knyttet både til lagring og forsendelse, fastsettes nærmere av Datatilsynet i det enkelte pålegg. Det skal utarbeides forskriftsbestemmelser for kryptering, som skal tilfredsstillende etablerte internasjonale standarder.

Partene er enige om at data undergis nødvendig sikring (lukket lagring):

- Krav om identitetskontroll ved innpassering til de lokaler hvor data lagres.
- Adgang til de lokaler hvor data lagres og tilgang til data som er omfattet av lagringsplikten gis kun til personell som har tjenstlig behov for adgang og tilgang og har autorisasjon til det.
- Lagringsmediet og omgivelsene rundt sikres fysisk, slik at uvedkommende ikke får adgang til området uten at det etterlater spor.
- Lagringsmediet sikres elektronisk ("brannmur" mv).
- Det skal ikke være anledning til eksternt å koble seg til lagringsmediet, dvs. at data ikke kan hentes ut "on-line".
- Enhver forsendelse av lagringspliktige data over landegrensene skal sikres ved at krypteringsteknologi anvendes. Nasjonal sikkerhetsmyndighet gir retningslinjer for hvilken krypteringsgrad som er nødvendig for å ivareta sikkerheten.

d) Krav til sporbarhet

Partene er enige om at enhver bruk av lagrede data skal kunne spores for å forhindre uautorisert bruk. Med dette menes at det i ettertid kan konstateres hva som er gjort i et dataanlegg/informasjonsystem, herunder hvem som har fått tilgang til opplysningene og at all elektronisk behandling av opplysninger, skal være sporbare.

e) Lagringssted

Partene er enige om at plikt for den enkelte tilbyder til å informere kunder om lagringsstedet bør inntas i forskrift 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), jf. § 1-8 om avtalevilkårene (forskriftsendringsforslag i kursiv):

§ 1-8. Avtale

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal tilby sluttbruker avtale for abonnements tjenester, herunder kontantkorttjenester. Avtalen skal blant annet omfatte opplysninger om:

1. tilbyders navn og adresse
2. avtalens omfang, herunder relevante opplysninger om nett og tjenester, kvalitetsparametre, vedlikeholdsvilkår og tidspunkt for tilknytning
3. pris samt hvor man får tilgang til oppdatert informasjon om pris
4. avtalens varighet og vilkår for fornyelse og opphør
5. *sted for lagring av lagringspliktig data i medhold av ekomloven § 2-7 a*
6. kompensasjons- og refusjonsordninger ved kvalitetsavvik eller ved manglende levering
7. prosedyre for klagebehandling.

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal etter ekomloven § 2-4 annet ledd varsle om endring i avtalen minst en måned før endringer iverksettes. Varslingsplikten gjelder endringer som må antas å ha en viss betydning for bruker, *men uansett for flytting av lagringssted for lagringspliktig data til en annen stat*. Dersom endringen er til ugunst for bruker skal bruker samtidig gjøres oppmerksom på adgangen til vederlagsfritt å kunne heve avtalen.

Annet ledd kan fravikes ved avtale utenfor forbrukerforhold.

Det tas forbehold for så vidt ikke internasjonalt regelverk er til hinder for å pålegge tilbyderne å opplyse om lagringssted.

6. Vilkår for utlevering av trafikkdata

Partene slutter seg til regjeringens forslag om strafferammer som ett av vilkårene for å få tilgang til data i etterforskningsøyemed. Dette innebærer at data bare skal utleveres etter rettens kjennelse i saker der det foreligger skjellig grunn til mistanke om en straffbar handling som kan medføre fengsel i 4 år eller mer. Basestasjonssøk er mest inngripende i forhold til personvernet, blant annet fordi man da får med seg mye overskuddsinformasjon. Utlevering av data etter basestasjonssøk forutsetter rettens kjennelse og at den straffbare handlingen kan

medføre straff av fengsel i 5 år eller mer. I begge tilfeller skal utlevering av data dessuten kunne skje dersom handlingen er utøvet som ledd i organisert kriminalitet og kan straffes med fengsel i 3 år eller mer. Det åpnes også for utlevering i enkelte andre typer saker som vil være særlig vanskelige å etterforske uten tilgang til data.

I dag er det ingen krav til den straffbare handlingens alvorlighetsgrad. Med denne lovendringen blir terskelen for å hente ut trafikkdata derfor vesentlig høyere.

Strafferammekrav sikrer at innhenting av data bare kan skje i forbindelse med etterforskning av alvorlig kriminalitet.

7. Domstolsbehandling

Partene er enige om at begjæring om utlevering av trafikkdata skal domstolsbehandles. For at domstolene, som med dette blir tillagt nye oppgaver, sikres nødvendig kompetanse innen personvern og tekniske spørsmål, skal regjeringen sørge for at det gjennomføres kompetansehevende tiltak.

For å sikre at hastebestemmelsen ikke brukes unødig mye, skal én domstol ha en vaktordning, for å sikre kontinuitet og tilgjengelighet hos domstolene. Den nødvendige lovbestemmelsen foreslås nedfelt i tilknytning til bestemmelsene om utlevering av data i etterforskningsøyemed i straffeprosessloven ny §§ 210 b og 210 c, jf. følgende forslag:

§ 210 b skal lyde:

Retten kan ved kjennelse pålegge utlevering for et bestemt tidsrom av trafikkdata, og lokaliseringsdata som ikke omfattes av § 210 c, og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger

- a) som etter loven kan medføre straff av fengsel i 4 år eller mer, eller
- b) som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller
- c) som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, 145 annet ledd, 145 a, 145 b, 162, 162 b, 162 c, 190 a, 201 a, 203, 204 a, 270 første ledd nr. 2, 317, jf. § 162, eller § 390 a, eller av utlendingsloven § 108 fjerde ledd.

Forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning.

Utlevering etter paragrafen her kan bare pålegges dersom det må antas at opplysningene vil være av vesentlig betydning for etterforskningen.

Utenfor domstolenes ordinære kontortid fremsettes begjæringer om utlevering for Oslo tingrett etter nærmere bestemmelser gitt av departementet.

§ 210 annet og fjerde ledd gjelder tilsvarende.

§ 210 c skal lyde:

Retten kan ved kjennelse pålegge utlevering for et begrenset tidsrom av opplysninger om hvilke telefoner eller annet kommunikasjonsutstyr som innenfor et nærmere bestemt geografisk område har vært satt i forbindelse med bestemte telefoner eller kommunikasjonsutstyr og som tilbyder har plikt til å lagre etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon § 2-7 a. Pålegg kan gis når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger

a) som etter loven kan medføre straff av fengsel i 5 år eller mer, eller

b) som etter loven kan medføre straff av fengsel i 3 år eller mer og det er grunn til å tro at handlingen er utøvet som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 60 a, eller

c) som rammes av straffeloven §§ 90, 91, 91 a, 94 jf. 90, 104 a annet ledd, § 162, 162 b, 162 c, eller § 317, jf. § 162, eller av utlendingsloven § 108 fjerde ledd.

§ 210 b annet til femte ledd gjelder tilsvarende.

Hastekompetansen for påtalemyndigheten følger av § 210 b femte ledd jf § 210 annet ledd og er subsidiær i forhold til å begjære rettens samtykke uavhengig av om det er tale om samtykke fra den stedlige rett eller fra vakthavende Oslo tingrett. Dette gjelder tilsvarende for basestasjonssøk, jf. § 210 c annet ledd og henvisningen til § 210 b femte ledd.

Partene er enige om at det skal føres statistikk over bruken av beredskapsordningen og hastebestemmelsene. Bruken av hastebestemmelsene er et av de forholdene som skal være gjenstand for en evaluering, jfr. avtalens pkt. 10.

8. Politiregisterloven

Partene er enige om at lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) og endringer i ekomloven og straffeprosessloven mv. (gjennomføringen av EUs datalagringsdirektiv i norsk rett) trer i kraft samtidig, og senest 1. april 2012. De elementer av politiregisterloven som gjelder logging og registrering av politiets bruk av data, forutsetter betydelige endringer i politiets IKT-systemer. Partene er enige om at fornyelse av politiets IKT-systemer skal prioriteres og følges opp, slik at gjenstående elementer i politiregisterloven kan tre i kraft raskt.

9. Datatilsynet

Partene er opptatt av at personvernet styrkes ved disse endringene i ekomloven mv.

Datatilsynet fører i dag kontroll etter personopplysningsloven.

Partene er enige om behovet for at Datatilsynet styrker sin kontrollvirksomhet rettet mot ekomtilbydere og justissektoren/politiet betydelig, herunder overholdelse av sletteplikt, lagringstid og sikring av lagrede data, inkludert lagringssted.

Partene legger til grunn at ekomtilbydernes behandling av lagringspliktige data vil bli gjenstand for særlig oppmerksomhet i Datatilsynets tilsynsvirksomhet.

10. Evaluering

Lovforslaget siktemål er å imøtekomme behovet for data i kriminalitetsbekjempelsen og å sikre personvernet, blant annet ved strengere regler for politiets tilgang til data.

Reglene skal anvendes på et teknologisk område som er i stadig utvikling. Lagring og utlevering av data utfordrer dessuten personvernet.

Partene er derfor enige om at det etter en periode på fire år etter ikrafttreddelsen skal foretas en evaluering for å undersøke om lovgivningen og tilhørende forskrifter har virket etter sin hensikt.

Følgende punkter bør inkluderes i en slik evaluering:

- Politiets bruk av hastekompetanse
- Lagringstid
- Vilkårene for utlevering av data i etterforskningsøyemed
- Erfaringer med domstolskontroll
- Lagringsikkerhet og personvern hos både ekomtilbydere og politiet
- Konkurransesituasjonen i ekommarkedet
- Eventuelle andre relevante forhold

Evalueringen skal legges frem for Stortinget på egnet måte senest fem år etter ikrafttredelse.

11. Videre arbeid

Partene er enige om at forskrifter skal utformes i tråd med intensjonen i denne avtalen.

Partene er enige om at hvis det i perioden fremlegges forslag til revisjon av datalagringsdirektivet skal Stortingets Europautvalg konsulteres.

12. Styrking av det generelle personvernet

Partene er enige om at personvernet skal styrkes på en rekke samfunnsområder. Partene legger til grunn at regjeringen som ledd i oppfølgingen av Personvernkommisjonens rapport, legger fram en stortingsmelding om personvern. Et grunnleggende personvernprinsipp er den enkeltes kontroll over egne personopplysninger og retten til å vite hvilke opplysninger andre behandler og hvem disse opplysningene overføres til. Partene ber derfor regjeringen i stortingsmeldingen særlig drøfte dette prinsippet og hvordan det kan ivaretas, blant annet gjennom logging av hvem som får tilgang til opplysningene og den enkeltes innsyn i disse loggene.

Partene er enige om at et grunnleggende prinsipp er at enhver har rett til innsyn i hvem som får tilgang til opplysninger om en selv. Plikten til logging og retten til innsyn i egen logg skal være det bærende prinsipp for alle større offentlige og private registre. I den avtalte stortingsmeldingen om personvern skal det drøftes hvilke avgrensninger som bør gjøres i loggplikten, innsynsretten, omfanget av innsynet i det enkelte forhold og framdriften i arbeidet med å virkeliggjøre prinsippet. Arbeiderpartiet viser her til unntaket for skattelistene.

Partene er også enige om å sikre personvernet gjennom å:

- a) Be regjeringen sikre at det legges til rette for loggføring av interne oppslag i personregistre med sensitive personopplysninger i NAV, jf personopplysningsloven med forskrifter, og i behandlingsrettede registre i helsevesenet, jf helseregisterloven.
- b) Legge til grunn at regjeringen sikrer at den registrerte gis innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne, det vil si innsyn i blant annet journal- og informasjonssystemer, jf helseregisterloven.
- c) Ber regjeringen sørge for at det etableres systemer for logging av elektroniske spor ved all tilgang til Norsk pasientregister (NPR), som forutsatt i forskrift om innsamling og behandling av helseopplysninger i Norsk pasientregister (NPR), hjemlet i helseregisterloven. Det skal også være utarbeidet oversikt over hvem som har fått

utlevert opplysninger fra NPR, samt hjemmelsgrunnlaget for utleveringen. Oversikt over utleveringer skal også være utarbeidet for de øvrige sentrale helseregistrene.

- d) Sikre at Arbeids- og velferdsetaten fortsatt avskjæres fra å innhente trafikk- og lokaliseringsdata fra elektronisk kommunikasjon, jfprop. 49 L (2010-2011).
- e) Be regjeringen i forbindelse med framlegging av egen stortingsmelding om Personvernsspørsmål gjennomgå og vurdere rutiner og praksis for håndtering av taushetsbelagt informasjon i Arbeids- og velferdsetaten.
- f) Følge opp trygdovens bestemmelse om at NAVs mulighet til å innhente fullstendig journal kun gjelder ved mistanke om trygdemisbruk hos behandlende helsepersonell og sørge for at fullstendige journaler utelukkende behandles i Arbeids- og velferdsetatens særskilte kontrollenheter.
- g) Viser til at det i henhold til politiregisterloven skal etableres en ordning med personvernrådgiver i justissektoren. Partene ber regjeringen sørge for at det etableres ordning med personvernrådgiver/-koordinator ved større statlige etater som behandler sensitive personopplysninger og at dette skal gjøres i NAV og helsesektoren.
- h) Be regjeringen styrke ivaretagelse av arbeidstakernes personvern i arbeidsmiljølovens kapittel 9, slik at personvern synliggjøres i HMS-arbeidet.
- i) I påvente av avklaring av muligheter for å begrense innsyn i lovlig lagrede data i elektroniske betalingsanlegg, er partene enige om at bomselskapene ikke skal utlevere passeringsopplysninger til ligningsmyndighetene.

13. Pressens kildevern

Partene er enige om at pressens kildevern er særdeles viktig i en tid der ny teknologi har skapt store utfordringer for personvernet. Partene har registrert at pressen er bekymret for at egen arbeidssituasjon vil bli vanskeligere med pliktig lagring av trafikkdata. Partene mener det er viktig å styrke journalistenes kildevern, og at en god måte å gjøre dette på er å oppstille begrensninger i adgangen til å avlytte telefoner eller lokaler som brukes av journalister, og til å bruke slike opptak som bevis. Partene er derfor enige om at de i forbindelse med behandlingen av Prop. 49 L (2010-2011) skal gi uttrykk for at det er behov for å endre straffeprosessloven § 216m slik at journalister får et særskilt vern mot romavlytting, på linje med det som tilkommer avlytting av de øvrige yrkesgrupper som nå er nevnt i § 216 m fjerde ledd, og at man ber regjeringen fremme et slikt lovforslag som ledd i oppfølgingen av NOU 2009: 15.

14. Taushetsplikt

Partene er enige om at det er avgjørende for personvernet til de som opplever at trafikkdata om dem blir gjenstand for etterforskning, at de som i sitt arbeid kan få tilgang til slike data, har taushetsplikt. Partene er enige om at det i forbindelse med behandlingen av Prop. 49 L (2010-2011) skal gis uttrykk for at det er behov for å oppstille en straffesanksjonert taushetsplikt for advokater, og at man ber regjeringen fremme et slikt forslag som ledd i oppfølgingen av NOU 2009: 15.

15. Nødrett

Partene konstaterer at utlevering av data i nødrettssituasjoner ikke er lovregulert. Et krav til mistanke mot en konkret person kan være et problem for uthenting av data i en nødrettssituasjon. Blant annet derfor er kravet til mistanke i lovforslaget nå bare knyttet til skjellig grunn til mistanke om straffbar handling. Utlevering av data i nødrettssituasjoner som ikke oppfyller vilkårene i lovforslaget (straffeprosessloven §§ 210 b og 210 c) vil imidlertid fortsatt skje på ulovfestet grunnlag. Generelt innebærer utlevering på ulovfestet grunnlag muligheten for en rask innhenting av data i en nødrettssituasjon. På den annen side er lettere tilgjengelighet et argument for å lovfeste reglene.

Partene mener det vil være riktig å se nærmere på utformingen av en lovbestemmelse om dette. Utformingen må følge vanlig saksbehandling, herunder utredning og høring. Det er bl.a. viktig i lovarbeidet å sikre at utlevering bare skjer i de situasjoner hvor man mener de hensynene som tilsier det er tilstrekkelig tungtveiende. Det er uheldig både om man stenger noen muligheter ute eller favner for mange situasjoner.

Partene er enige om at et lovforslag om nødrett blir sendt på høring.

16. Forpliktelser for avtalepartene

Partene forplikter seg til å stemme for de konkrete budsjettmessige konsekvenser og de konkrete forslag som følger av avtalen.