Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
24/3567	24/205682 - 7	Oslo, 11.12.2024

Høringssvar - forslag til forskrift til digitalsikkerhetsloven - digitalsikkerhetsforskriften

Politidirektoratet (POD) viser til Justis- og beredskapsdepartementets høringsbrev av 11.09.2024 om forslag til forskrift til lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsforskriften). Høringsfristen er 11. desember 2024.

Det fremgår av høringsbrevets adresseliste at politidistriktene, Kripos og Økokrim har mottatt høringen direkte fra departementet. POD har bedt om å få tilsendt eventuelle høringsinnspill fra underliggende enheter, for sammenstilling av et felles høringssvar. Det har kommet innspill fra Kripos og Oslo politidistrikt, som ligger vedlagt dette dokumentet.

Innledende merknader

Sammen med blant annet Nasjonal sikkerhetsmyndighet (NSM) utgjør politiet og påtalemyndigheten sentrale brikker i Norges innsats mot kriminalitet og uønskede hendelser i det digitale rom.

I politiets virksomhetsstrategi for årene 2023-25 er «Trygghet i det digitale rom» utpekt som ett av tre strategiske mål og i Riksadvokatens «Mål og prioriteringer for straffesaksbehandlingen i 2024» heter det om IT-kriminalitet at «innsatsen på dette området må fortsatt intensiveres».

Det følger som kjent av politiloven § 2 at politiet skal drive forebyggende og avdekkende rettshåndheving blant annet ved å beskytte fellesgoder og verne om all lovlig virksomhet. Det følger videre av samme bestemmelse at når kriminalitet pågår eller har skjedd, skal politiet avdekke, stanse og straffeforfølge lovbruddene. Politiets samfunnsoppdrag er ikke begrenset til den fysiske verden, men gjelder fullt ut også i den digitale sfære.

I arbeidet med å redusere alle former for kriminalitet og øke tryggheten for innbyggerne er forebygging politiets hovedstrategi og forebygging ligger derfor til grunn for all oppgaveløsning. Vi vil understreke at denne hovedstrategien også gjelder for politiets

innsats mot cyberkriminalitet. Det reaktive etterforskningsarbeidet utgjør således ett av flere ledd i politiets samlede innsats mot cyberkriminalitet. Deteksjon, analyse og informasjonsdeling er bærende elementer i enhver forebyggingsstrategi. For forebygging av alvorlig cyberkriminalitet er disse elementene særlig viktige.

Politiet har således et helhetlig ansvar i det digitale rom. Ansvaret omfatter å forebygge, avdekke, avverge og stanse kriminell virksomhet, forfølge lovbrudd og å håndtere hendelser ved en krise.

Rask og adekvat tilgang til informasjon om kriminalitet og alvorlige hendelser er derfor helt avgjørende for at politiet skal klare å løse sitt samfunnsoppdrag også når kriminaliteten skjer digitalt.

Forskriftsforslaget § 18 – forslag om varsling til politiet

Virksomheter underlagt digitalsikkerhetsloven pålegges å varsle sine sektorielle tilsynsmyndigheter ved «hendelser som virker betydelig inn på tjenesteleveransen», se digitalsikkerhetsloven §§ 8 og 11. Eventuell taushetsplikt vil ikke være til hinder for at varsling skal gis. Innholdet i varslingsplikten er nærmere regulert i forskriftsforslaget § 17 hvor det blant annet fremgår at NSM skal motta varslingene i kopi.

I forskriftsforslagets § 18 første ledd gis unntak fra taushetsplikten for tilsynsmyndighetene som mottar varslingene. I bestemmelsens andre ledd innføres en informasjonsplikt for NSM når det vurderes å foreligge «fare for alvorlige hendelser». I så fall skal sikkerhetsmyndigheten informere «berørte nasjonale og internasjonale aktører om risiko og mulige tiltak».

POD mener at varslingsplikten i § 18 annet ledd bør inneholde en eksplitt henvisning til «politiet» og viser til Kripos´ høringsinnspill som ligger vedlagt. En slik varslingsplikt for NSM bør fremgå direkte av forskriften, slik at uklarheter unngås og for å sikre at politiet alltid involveres i den viktige initialfasen ved slike alvorlige hendelser som varslingsplikten omfatter.

Dette innebærer at varslingene som NSM mottar skal viderebringes til politiet uten opphold og uten filtrering/siling. Begrunnelsen er at politiet selv har de beste forutsetningene til å vurdere innholdet i varslingene opp imot sitt samfunnsoppdrag. Eksempelvis om den aktuelle hendelsen bør håndteres av politiet i etterretningssporet og/eller om det bør iverksettes en påtalestyrt etterforskning. Disse vurderingene vil skje i nær dialog og samråd med NSM og andre relevante aktører.

Risikovurdering og risikohåndtering (§§ 7 og 8)

POD deler vurderingen av at risikovurdering er en helt nødvendig del av arbeidet med digital sikkerhet jf. forskriftens § 7, og at konkrete krav til hva den minst skal inneholde vil være til god hjelp for virksomhetene for å kunne etterleve forskriften. Virksomheter som er omfattet av forskriften er av ulik størrelse og karakter, og en risikovurdering bør ikke gjøres for byrdefull. Vi støtter derfor vurderingen om at metode for risikovurdering ikke beskrives nærmere, slik at de ulike virksomhetene selv kan tilpasse metodikk ut fra eget behov.

Vi deler også vurderingen av at sikkerhetstiltak som foreslås i §§ 9-14 bør suppleres med veiledningsmateriale fra Nasjonal sikkerhetsmyndighet, som kan benyttes i kombinasjon med anerkjente standarder. Forskriften bør ikke bli for omfattende, og virksomhetene vil ha ulik grad av behov for tiltak.

Sikkerhetstiltak

I forskriftsforslaget er det valgt å ikke ta inn en unntaksbestemmelse, slik at virksomheter kan søke dispensasjon fra enkelte krav til sikkerhetstiltak, ut fra vurderinger knyttet til eksempelvis relevans og kostnadsnivå. I begrunnelsen pekes det på viktige argumenter både for og mot. POD anbefaler at det uavhengig av utfall, etter en virkeperiode bør gjennomføres en evaluering av om beslutningen har vist seg å være hensiktsmessig.

Behandling av personopplysninger

Forslaget inneholder supplerende rettslig grunnlag for behandling av personopplysninger ved varsling, som det kan vises til ved utførelse av oppgaver som nasjonalt kontaktpunkt og ved tilsyn. Ved behov for behandling av personopplysninger i selve hendelseshåndteringen er det derimot ikke satt opp noe supplerende rettslig grunnlag, men det vises til høringsnotatet at man kan bruke "berettiget interesse". Det kan vurderes i det videre arbeidet om det er behov for å tydeliggjøre det rettslige grunnlaget dersom det er nødvendig å behandle kategorier i hendelseshåndteringen.

Overtredelsesgebyr

Vi observerer at overtredelsesgebyr skal være tvangsgrunnlag for utlegg. Det er nærliggende at det kan bli tvister rundt ileggelse og størrelse. Tvangskraften suspenderes først ved saksanlegg mot staten for å prøve vedtaket. Namsmyndigheten kan dermed måtte ta prejudisielt stilling til vanskelige og komplekse saker og rettslige spørsmål. Det antas å bli få saker, men det synes ikke å være gjort vurderinger av saksvolum.

Avsluttende bemerkninger

Norske virksomheter vier stadig mer oppmerksomhet mot og øker ressursbruken på digital sikkerhet. Politiet erfarer samtidig at stadig flere borgere og virksomheter velger å anmelde så vel cyberrettede som cyberstøttede lovbrudd. Dette er en positiv og nødvendig utvikling.

Gjennom ikrafttredelse av digitalsikkerhetsloven med tilhørende forskrift vil disse trendene formentlig fortsette i samme retning, og ved innføringen av NIS2 er det all grunn til å tro at den positive utviklingen vil styrke seg ytterligere.

POD mener det er viktig at informasjon knyttet til politiets mandat og rolle i det digitale rom kommuniseres til offentligheten regelmessig og i ulike fora og sammenhenger. I tillegg til momentene som er anført ovenfor, vil politiets rolle som varslingsmottaker i medhold av forskriftens § 18 andre ledd, kunne bidra positivt til nevnte kommunikasjonsoppgave.

Med hilsen

Tone Elisabeth Vangen
Avdelingsdirektør

Nicolay Bjertnæs Nakstad
Seksjonssjef

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:
Høringsinnspill - forslag til forskrift til digitalsikkerhetsloven - digitalsikkerhetsforskriften - Oslo politidistrikt
Høringsinnspill - forslag til forskrift til digitalsikkerhetsloven - digitalsikkerhetsforskriften - Kripos

Politidirektoratet
Postboks 2090 Vika
0125 Oslo

Deres referanse:	Vår referanse:	Sted, dato:
	24/206046 - 6	Oslo, 27.11.2024

Høringssvar - forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Oslo politidistrikt viser til høringsbrev fra Politidirektoratet (POD) datert 04.10.2024, med vedlegg fra Justis- og beredskapsdepartementet (JD), der det bes om innspill og høringsinstansenes syn på enkelte av departementets vurderinger av forslag til forskrift til digitaliseringssikkerhetsloven (digitalsikkerhetsforskriften).

4 Lovens virkeområde

4.2.4 Innmelding av samfunnsviktige tjenester

Det vises til at det i NIS1, NIS 2 og DSBs temarapport "Samfunnets kritiske funksjoner" sies noe om tjenester og virksomheter som kan/vil bli underlagt digitalsikkerhetsloven med forskrift. Det benyttes ulike benevninger/definisjoner, som f. eks. samfunnsviktige tjenester og samfunnskritiske funksjoner, som kan gjøre det noe uklart for hvilke virksomheter som omfattes av digitalsikkerhetsloven.

Det kan vurderes om det i det videre høringsarbeidet bør utpekes virksomheter som tilbyr samfunnsviktige tjenester og som omfattes av digitalsikkerhetsloven, på samme måte som etter sikkerhetsloven §7-1 andre ledd. Digitalsikkerhetsloven vil dermed også implisitt gjelde for virksomhetens tilbydere av digitale tjenester, og det kan stilles samme krav til sikkerhet for dem.

5 Krav til sikkerhet for samfunnsviktige tjenester

5.3.3 Risikovurdering

Oslo politidistrikt deler vurderingen av at risikovurdering er en helt nødvendig del av arbeidet med digital sikkerhet jf. forskriftens § 7, og at konkrete krav til hva den minst skal inneholde vil være til god hjelp for virksomhetene for å kunne etterleve forskriften. Virksomheter som er omfattet av forskriften er av ulik størrelse og karakter, og en risikovurdering bør ikke gjøres for byrdefull. De ulike virksomhetene bør derfor ha noe frihet til selv å tilpasse metodikk, men følge anerkjente og relevante standarder for risikovurdering.

5.3.4 Risikohåndtering
Oslo politidistrikt deler vurderingen av at sikkerhetstiltak som foreslås i §§ 9-14 bør suppleres med veiledningsmateriale fra Nasjonal sikkerhetsmyndighet, som kan benyttes i kombinasjon med anerkjente standarder. Forskriften bør ikke bli for omfattende, og virksomhetene vil ha ulik grad av behov for tiltak.

5.3.5 Sikkerhetstiltak
Det kan vurderes å ta inn en unntaksbestemmelse i forskriften, slik at virksomheter kan søke dispensasjon fra enkelte krav til sikkerhetstiltak, ut fra vurderinger knyttet til eksempelvis relevans og kostnadsnivå.

5.3.7 Oppfølgingsplikt
Distriktet ser viktigheten av tydelige avtalevilkår og sikkerhetskrav overfor leverandører, et regelverk som stiller krav om å følge opp underleverandører og å ha oversikt over hele leverandørkjeden. Det er da nødvendig med en bestemmelse som § 22 for at dette skal ha tilstrekkelig fokus i virksomhetene ved inngåelse av leverandøravtaler, samtidig som det bør klargjøres hvor langt i leverandørkjeden virksomhetens ansvar skal gå.

11 Behandling av personopplysninger
Oslo politidistrikt har merket seg at det er satt opp supplerende rettslig grunnlag som det kan vises til, for behandling av personopplysninger ved varsling, ved utførelse av oppgaver som nasjonalt kontaktpunkt og ved tilsyn. Ved behov for behandling av personopplysninger i selve hendelseshåndteringen er det derimot ikke satt opp noe supplerende rettslig grunnlag, men det vises til høringsnotatet at man kan bruke "berettiget interesse". Det kan vurderes i det videre arbeidet om det er behov for å tydeliggjøre det rettslige grunnlaget dersom det er nødvendig å behandle kategorier i hendelseshåndteringen.

12 Overtredelsesgebyr
OPD observerer at overtredelsesgebyr skal være tvangsgrunnlag for utlegg. Det er nærliggende at det kan bli tvister rundt ileggelse og størrelse. Tvangskraften suspenderes først ved saksanlegg mot staten for å prøve vedtaket. Namsmyndigheten kan dermed måtte ta prejudisielt stilling til vanskelige og komplekse saker og rettslige spørsmål. Det antas å bli få saker, men det synes ikke å være gjort vurderinger av saksvolum.

Med hilsen

Rune Solberg Swahn — *Avdelingsdirektør*

Karianne Seim — *Seksjonssjef*

Dokumentet er elektronisk godkjent uten signatur.

POLITIET
KRIPOS

Politidirektoratet
Postboks 2090 Vika
0125 OSLO

Deres referanse:	Vår referanse:	Sted, dato:
24/205682	24/205699 - 3	Oslo, 22.11.2024

Høringssvar - forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften)

Det vises til høringsbrev fra Justis- og beredskapsdepartementet av 11. september 2024 om forslag til digitalsikkerhetsforskrift og til brev fra Politidirektoratet av 4. oktober 2024.

Innledende merknader

Sammen med blant annet Nasjonal sikkerhetsmyndighet utgjør politiet og påtalemyndigheten sentrale brikker i Norges innsats mot kriminalitet og uønskede hendelser i det digitale rom.

I politiets virksomhetsstrategi for årene 2023-25 er «Trygghet i det digitale rom» utpekt som ett av tre strategiske mål og i Riksadvokatens «Mål og prioriteringer for straffesaksbehandlingen i 2024» heter det om IT-kriminalitet at «innsatsen på dette området må fortsatt intensiveres».

Det følger som kjent av politiloven § 2 at politiet skal drive forebyggende og avdekkende rettshåndheving blant annet ved å beskytte fellesgoder og verne om all lovlig virksomhet. Det følger videre av samme bestemmelse at når kriminalitet pågår eller har skjedd skal politiet avdekke, stanse og straffeforfølge lovbruddene. Politiets samfunnsoppdrag er ikke begrenset til den fysiske verden, men gjelder fullt ut også i den digitale sfære.

I arbeidet med å redusere alle former for kriminalitet og øke tryggheten for innbyggerne er forebygging politiets hovedstrategi og forebygging ligger derfor til grunn for all oppgaveløsning. Kripos vil understreke at denne hovedstrategien også gjelder for politiets innsats mot cyberkriminalitet. Det reaktive etterforskningsarbeidet utgjør således ett av flere ledd i politiets samlede innsats mot cyberkriminalitet. Deteksjon, analyse og informasjonsdeling er bærende elementer i enhver forebyggingsstrategi. For forebygging av alvorlig cyberkriminalitet er disse elementene særlig viktige.

KRIPOS
Post: Postboks 2094 Vika, 0125 Oslo / Besøk: Nils Hansens vei 25, 0667 Oslo / (+47) 23 20 80 00
kripos@politiet.no / www.politiet.no / Organisasjonsnummer: 974760827

Politiet har således et helhetlig ansvar i det digitale rom. Ansvaret omfatter å forebygge, avdekke, avverge og stanse kriminell virksomhet, forfølge lovbrudd og å håndtere hendelser ved en krise.

Rask og adekvat tilgang til informasjon om kriminalitet og alvorlige hendelser er derfor helt avgjørende for at politiet skal klare å løse sitt samfunnsoppdrag også når kriminaliteten skjer digitalt.

Disse utgangspunktene utgjør bakteppet for nærværende høringsuttalelse. I vårt høringssvar vil vi peke på politiets behov for å bli varslet og involvert idet Nasjonal sikkerhetsmyndighet mottar lovpålagte varslinger om tilsiktede alvorlige hendelser fra virksomhetene som omfattes av varslingsplikten, jf. digitalsikkerhetsloven §§ 8 og 11, jf. forskriftsforslaget § 17.

Først gis en kortfattet redegjørelse for hvordan politiet jobber for å bekjempe kriminaliteten i cyberdomenet.

Kort om politiets informasjonsinnhenting i cyberdomenet og hvordan informasjonen brukes til å løse samfunnsoppdraget

For at politiet skal settes i best mulig stand til å arbeide forebyggende, avvergende og reaktivt med alvorlig cyberkriminalitet er umiddelbar informasjonstilgang om mulige lovbrudd helt avgjørende. Hvorvidt det anses hensiktsmessig å igangsette etterforskning eller om den aktuelle hendelsen best håndteres i det forebyggende sporet, beror på flere forhold, herunder en vurdering av hvordan straffeprosessuell tvangsmiddelbruk vil opplyse saken.

Informasjonsinnhenting i det forebyggende sporet

Politiet mottar daglig informasjon om mulige lovbrudd i det digitale rom. Noe tilkommer politiet i form av anmeldelser, og i en del andre tilfeller velger politiet på eget initiativ å iverksette etterforskning.

Informasjon som ikke genererer strafforfølgelse kan brukes til å arbeide forebyggende. På cyberkriminalitetsfeltet velger politiet i utstrakt grad å benytte informasjonen til avdekkende og forebyggende virksomhet. Dette beror på en erkjennelse av at iretteføring og domfellelse er et urealistisk saksforløp i mange datakrimsaker.

Den mottatte informasjonen benyttes i stedet til å søke å forebygge, avdekke og avverge cyberkriminalitet. Dette skjer typisk ved at politiet varsler virksomheter om at de, basert på politiets opplysninger, står i nærliggende fare for å bli utsatt for datakriminalitet. I andre sammenhenger benyttes politiets etterretningsinformasjon til å underbygge egen etterretningsproduksjon til strategisk og taktisk beslutningsstøtte.

Informasjonsinnhenting i etterforskningssporet

Det er Kripos' erfaring at politiet bør komme på banen så raskt som mulig ved mulige cyberrettede lovbrudd.

Rask iverksettelse av etterforskning er høyst nødvendig slik at flyktige bevis kan sikres, blant annet gjennom politiets tvangsmiddelbruk. Ved bruk av disse verktøyene kan etterforskningen skaffe tilgang til de cyberkriminelles digitale infrastruktur. Det er primært politiet som kan ta seg lovlig inn på sentrale sporsteder som dette.

Politiet kan videre sitte på unik informasjon som kan utfylle den akutte situasjonsforståelsen, samt peke på sannsynlige scenarioer basert på politiets kunnskap om gjerningspersonene og deres modus operandi.

Gjennom etterforskningene skaffer politiet seg kunnskap om trender, fenomener og om kriminelle aktører. I tillegg til å opplyse den konkrete straffesaken bidrar denne informasjonsinnhentingen inn i samfunnets samlede forebyggende og avdekkende arbeid. Kripos vil særlig trekke frem tre måter dette skjer på:

1. Ved å undersøke infrastruktur tilknyttet en trusselaktør kan politiet finne spor som peker på andre fornærmede som enten allerede er blitt kompromittert, eller som vil bli det i nær fremtid. Denne informasjonen kan politiet, eller andre aktører, bruke til å varsle virksomheter som da kan gjøre tiltak for å redusere skaden eller hindre et fremtidig cyberlovbrudd.

2. Ved at etterforskningen identifiserer modus, fremgangsmåter, verktøy og teknikker som benyttes av cyberkriminelle kan politiet informere andre virksomheter om forslag til forebyggende eller avvergende tiltak. Eksempelvis ved å installere oppdateringer eller filtrere trafikk i nettverket sitt.

3. Ved at informasjonen som innhentes benyttes av politiet til å produsere etterretning som gjør beslutningstakere i stand til å prioritere den helhetlige innsatsen innen bekjempelse av datakriminalitet, samt gi fornærmede og andre aktører taktisk beslutningsstøtte som kan være nyttig i håndteringen av en konkret hendelse, eksempelvis aktørforståelse.

Som en kommer nærmere inn på, anser Kripos det som maktpåliggende for politiet å bli varslet om hendelser som er varslingspliktige etter digitalsikkerhetsloven §§ 8 og 11. Ved å bli varslet og involvert kan politiet blant annet bidra som beskrevet over.

Forskriftsforslaget § 18 – Kripos foreslår at politiet skal varsles

Virksomheter underlagt digitalsikkerhetsloven pålegges å varsle sine sektorielle tilsynsmyndigheter ved «hendelser som virker betydelig inn på tjenesteleveransen», se lovens §§ 8 og 11. Eventuell taushetsplikt vil ikke være til hinder for at varsling skal gis. Innholdet i varslingsplikten er nærmere regulert i forskriftsforslaget § 17 hvor det blant annet fremgår at Nasjonal sikkerhetsmyndighet skal motta varslingene i kopi.

I forskriftsforslagets § 18 første ledd gis unntak fra taushetsplikten for tilsynsmyndighetene som mottar varslingene. I bestemmelsens andre ledd innføres en informasjonsplikt for Nasjonal sikkerhetsmyndighet når det vurderes å foreligge «fare for alvorlige hendelser». I så fall skal sikkerhetsmyndigheten informere «berørte nasjonale og internasjonale aktører om risiko og mulige tiltak.»

Sett i lys av politiets samfunnsoppdrag og dets sentrale posisjon i statens innsats mot cyberkriminalitet er det Kripos' oppfatning at varslingsplikten i § 18 andre ledd bør inneholde en eksplitt henvisning til «politiet». En slik varslingsplikt for Nasjonal sikkerhetsmyndighet bør fremgå direkte av forskriften slik at uklarheter unngås og for å sikre at politiet alltid involveres i den viktige initialfasen ved slike alvorlige hendelser som varslingsplikten omfatter. Det vises til foregående avsnitt hva gjelder politiets bidrag til den akutte hendelseshåndteringen og til spørsmålet om det skal iverksettes etterforskning. Etablering av en varslingsplikt til politiet vil dessuten bidra til å understreke politiets rolle som rettshåndhever i det digitale rom.

Ved at politiet umiddelbart varsles om slike hendelser settes dessuten politiet i stand til å avdekke og avverge ytterligere lovbrudd fra den aktuelle trusselaktøren. Dette vil eksempelvis skje ved at politiet deler informasjon fra hendelsen med internasjonale samarbeidspartnere. Ikke rent sjelden viser det seg at cyberkriminalitet rettet mot norske virksomheter har klare forgreininger til identisk eller lignende straffbar virksomhet i andre land. Ved hjelp av internasjonalt politisamarbeid kan virksomheter, som ennå ikke er utsatt for cyberlovbrudd, dermed varsles om at deres virksomhet står i fare for å bli utsatt for en tilsvarende kriminell handling.

Kripos er videre av den oppfatning at varslingene til politiet skal skje uten en forutgående silingsprosess fra Nasjonal sikkerhetsmyndighets side. Dette innebærer at varslingene som sikkerhetsmyndigheten mottar skal viderebringes til politiet uten opphold og uten filtrering. Begrunnelsen er at politiet selv har de beste forutsetningene til å vurdere innholdet i varslingene opp imot sitt samfunnsoppdrag. Eksempelvis om den aktuelle hendelsen bør håndteres av politiet i etterretningssporet og/eller om det bør iverksettes en påtalestyrt etterforskning. Disse vurderingene vil skje i nær dialog og samråd med Nasjonal sikkerhetsmyndighet og andre relevante aktører.

Avsluttende bemerkninger

Norske virksomheter vier stadig mer oppmerksomhet mot og øker ressursbruken på digital sikkerhet. Politiet erfarer samtidig at stadig flere borgere og virksomheter velger å anmelde så vel cyberrettede som cyberstøttede lovbrudd. Dette er en positiv og nødvendig utvikling.

Gjennom ikrafttredelse av digitalsikkerhetsloven med tilhørende forskrift vil disse trendene formentlig fortsette i samme retning, og ved innføringen av NIS2 er det all grunn til å tro at den positive utviklingen vil styrke seg ytterligere. Fra Kripos sitt ståsted er det viktig at informasjon knyttet til politiets mandat og rolle i det digitale rom kommuniseres til offentligheten regelmessig og i ulike fora og sammenhenger. I tillegg til momentene som er anført ovenfor til støtte for vårt forslag, vil politiets rolle som varslingsmottaker i medhold av forskriftens 18 andre ledd, kunne bidra positivt til nevnte kommunikasjonsoppgave.

Med hilsen

Ketil Haukaas
assisterende sjef Kripos

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Terje Nedrebø Michelsen
politiadvokat