



# POLITIET

POLITIDIREKTORATET

Det kongelige fornyings-, administrasjons- og kirkedepartementet  
Postboks 8004 Dep  
0030 OSLO

*Deres referanse*

*Vår referanse*

*Dato*

2012/01933-5 008

05.10.2012

## Høringssvar - forslag til endringer i personopplysningsforskriften

Vi viser til Fornyings-, administrasjons- og kirkedepartementets høringsbrev av 26. juni 2012 om forslag til endringer i personopplysningsforskriften. Politidirektoratet har fått utsatt høringsfrist til 05.10.2012.

Høringen er den del av implementeringen av Datalagringsdirektivet, hvor flere prosesser går over i hverandre. I den forbindelse viser vi til vårt svar av 18.01.2012 til Datatilsynets høring av 22.12.2011 om konsesjon til behandling av personopplysninger. Brevet følger vedlagt.

Kripos har som egen høringsinstans avgitt uttalelse av 28.09.2012. Vi viser til deres merknader med vedlegg, som vi slutter oss til.

### *§ 7-1 andre ledd – vilkår om kryptering:*

Politidirektoratet vil bemerke at det ved utforming av krav om kryptering ved overføring av data fra tilbyder til politiet må sikres at dette er en krypteringsløsning som er hensiktsmessig for politiet. Alle tilbydere bør benytte samme krypteringsløsning slik at politiet ikke må administrere en rekke ulike løsninger. Det bør videre være en enhetlig strukturering av dataformater som overføres til politiet fra de ulike tilbyderne. Vi viser her til høringssvaret fra Kripos.

Innføring av vilkår, herunder om tidspunkt for kryptering, må ta hensyn til at dette ikke skal hindre eller medføre forsinkelser i politiets tilgang til data. I situasjoner der liv og helse er i fare, eksempelvis bortføringsaker eller redningsoperasjoner, vil rask utlevering av data være avgjørende. I denne type saker kan være behov for både "ferske" posisjoneringsdata og data som er lagringspliktige etter datalagringsdirektivet.

Det er viktig å sikre fortsatt tilgang til dataene i lagringspliktig periode selv om tilbyder opphører å eksistere. Vilkår som settes må ivareta behov for å kunne tilgjengeliggjøre og dekrryptere data også i slike tilfeller.

### *§ 7-1 tredje ledd – vilkår for å sikre lukket lagring*

I tillegg til fysisk sikring må det oppstilles krav om personellsikkerhet. Politidirektoratet vil påpeke at det bør oppstilles krav om vandelskontroll av personell hos tilbyder. Det gjelder

## Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo  
Besøk: Hammersborggata 12  
Tlf: 23 36 41 00 Faks: 23 36 42 96  
E-post: [politidirektoratet@politiet.no](mailto:politidirektoratet@politiet.no)

Org. nr.: 982 531 950 mva  
Bankgiro: 7694.05.02388

både personell som skal ha tilgang til lagringspliktige data og personell som håndterer anmodningene fra politiet. Dette både for å ivareta personvernet og av hensyn til en pågående etterforskning. Det må utformes en klar hjemmel for utstedelse av politiattest (uttømmende) enten i personopplysningsforskriften eller i datalagringsforskriften. Det fremgår av høringsnotatet at Post- og teletilsynet utarbeider datalagringsforskrift parallelt med denne høringen. Tidligere høring om datalagringsforskrift hadde forslag om autorisasjon og fremleggelse av politiattest i § 3-4.

Avslutningsvis vil vi påpeke at tredje ledd bokstav e bør presiseres nærmere. Vi forutsetter at forbudet mot at data kan hentes ut "on-line" (høringsnotatet side 6) ikke er til hinder for at dedikerte personer hos tilbyder har tilgang til dataene for kvalitetssikring eller for å bistå politiet ved eventuelle spørsmål.

Med hilsen

  
Christian Budberg Pettersen  
*avdelingsdirektor*

  
Daniel S. Billaud  
*fung. seksjonssjef*

Saksbehandler:  
Bente Storruste  
Geir Jonatan Sharabi

Kopi til:  
Det kongelige justis- og  
beredskapsdepartement



# POLITIET

POLITIDIREKTORATET

ARKIVKOP

Det kongelige justis- og politidepartement  
Politiavdelingen  
Postboks 8005 Dep  
0030 OSLO

Deres referanse  
Silje Nilsen

Vår referanse  
2012/00080-5 008

Dato  
18.01.2012

## Høring - konsesjon til behandling av personopplysninger

Vi viser til Datatilsynets høringsbrev av 22.12.2011 om ovennevnte, oversendt Politidirektoratet ved Justisdepartementets e-post av 05.01.2012.

Vi har merket oss at Politiets data- og materieltjeneste (PDMT) har mottatt høringen som egen høringsinstans. Vi har etter avtale med førstekonsulent Silje Lien Nilsen bedt PDMT om å sende kopi av sitt høringssvar til Justisdepartementet og Politidirektoratet. Vi har videre forelagt høringen for Kripos, som ved e-post av 16.01.2012 har gitt sin uttalelse i saken. Uttalelsen fra Kripos er innarbeidet i vår uttalelse.

Som påpekt i høringsbrevet pågår det flere samtidige prosesser knyttet til implementeringen av direktiv 2006/24 EF (Datalagringsdirektivet) i norsk rett. Politidirektoratet og Kripos deltar i flere av prosessene og Kripos uttaler innledningsvis at "vi opplever dem på enkelte områder utfordrende, særlig fordi det etter vår vurdering mangler en felles behandling av spørsmål hvis løsninger klart vil ha betydning for hverandre. Deler av prosessene har også en form og et tempo som er problematiske sett hen til omfanget av implementeringsarbeidet. Vi har tatt dette opp blant annet med Post- og teletilsynet (som ansvarlig for deler av forskriftsarbeidet), og etter vår mening bør dette også kunne påpekes i forhold til Datatilsynet her."

I lys av andre pågående prosesser på området har vi valgt å begrense vår uttalelse til tre punkter.

1. Både av hensyn til personvernet og for å følge opp Stortingets vedtak er det viktig at lagrede data sikres på en tilfredsstillende måte. I Datatilsynets høringsbrev og konsesjonsutkast er det lagt til grunn at "... lagring av data skal skje i henhold til ETSI 102 661 eller at det innføres tilsvarende sikkerhetstiltak". Ved valg av krypteringsløsning skal det ses hen til kravene i nevnte standards ANNEX C. Politidirektoratet vil påpeke at løsningen i ETSI-rapporten synes å beskrive et særdeles høyt sikkerhetsnivå som vil kunne medføre ulemper i forhold til formålet med lagringen. Det har vært antatt løsningen hindrer at utvalgte personer hos tilbyder kan ha tilgang til dataene, at løsningen er svært kostbar, samt at den kan ha negative konsekvenser i forbindelse med utlevering av data til politiet.

## Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo  
Besøk: Hammersborggata 12  
Tlf: 23 36 41 00 Faks: 23 36 42 96  
E-post: [politidirektoratet@politiet.no](mailto:politidirektoratet@politiet.no)

Org. nr.: 982 531 950 mva  
Bankgiro: 7694.05.02388

Kripos uttaler i samme retning at:

”Slik prosessene står pr i dag er det vanskelig for Kripos å uttale seg nærmere om valget av standard for sikkerhetstiltak. Det er imidlertid viktig å få frem at man ved valg av løsning i tilstrekkelig grad må ta hensyn til formålet med lagringen, nemlig å sikre politiet et verktøy for etterforskning av alvorlig kriminalitet. Vi ser i den sammenheng at valg av sikkerhetsløsninger vil kunne ha innvirkning både på hvordan data i praksis vil bli gjort tilgjengelig for politiet og de eventuelle kostnader som vil være forbundet med bruk av data. Begge disse elementer vil ha betydning for hvordan politiet reelt sett vil kunne nyttiggjøre seg dataene i praksis.”

Dedikerte personer hos tilbyderne bør ha tilgang til de lagrede dataene for kvalitetssikring av dataene, for å bistå politiet ved eventuelle spørsmål og for å utøve behandlingsansvaret i form av anmodninger fra den registrerte om innsyn i lagrede data. Det må heller ikke etableres løsninger som hindrer eller forsinket utlevering av data i til politiet eller Hovedredningsentralene i akutte nødsituasjoner. Politidirektoratet mener at det bør utredes om det finnes andre og enklere løsninger for kryptering enn det som fremkommer av ETSI TR 102 661 Annex C, men som allikevel har et sikkerhetsnivå som er tilstrekkelig.

Når det gjelder uthenting av data og overføring til politiet vil vi bemerke at dersom data overføres til politiet gjennom kryptert elektronisk oversendelse, må krypteringsløsningen være ensartet for alle lagringspliktige (samme type kryptering).


For å oppfylle formålet med datalagringen må det utarbeides et regelverk – fortrinnsvis i konsesjon eller forskrift - som sikrer en sikker, rask og god overlevering av korrekte data til politiet. Det er behov for krav om blant annet kvalitet, replikeringstid, responstid og tilgjengelighet hos tilbyder.

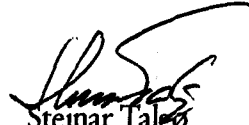
2. I konsesjonsforslagets punkt 4 og punkt 10 nevnes retten (domstol) og påtalemyndighet som eneste beslutningsmyndighet for utlevering av data. Det bør vurderes om man også skal omtale Finanstilsynet i disse bestemmelsene, da de skal ha tilgang til data etter verdipapirhandelloven § 15-3. Videre er vi, i likhet med Kripos, usikker på om formuleringen i disse punkter i tilstrekkelig grad hensyntar den uthenting som skjer på nødrettsgrunnlag, for eksempel gjennom Redningsentralen, jf. også ovenfor. Politidirektoratet vil understreke viktigheten av dette.

Heller ikke samtykketilfellene er omhandlet. Kripos påpeker at uthenting til bruk i straffesaker i dag i utstrakt grad skjer på bakgrunn av samtykke gitt av "den registrerte" - typisk den mistenkte/siktede. I disse tilfeller vil utlevering skje direkte til politiet uten beslutning fra påtalemyndighet eller domstol. Implementeringen av DLD innebærer ingen endring i forhold til at samtykke gir grunnlag for uthenting, og det bør derfor vurderes om dette bør fremkomme klart i konsesjonsskrivet.

3. Til konsesjonsforslagets punkt 8 om "Slettefrist", reiser vi, i likhet med Kripos, spørsmålet om det av konsesjonen burde presiseres et unntak fra sletting etter 6 måneder der det er gitt sikringspålegg etter straffeprosessloven § 215a.

Med hilsen

  
Christian Budsberg Pettersen  
avdelingsdirektor

  
Steinar Talgø  
seksjonssjef

Saksbehandler:  
Gunnvor Hovde  
Tlf: 23364129