

DIGITALISERINGS- OG  
FORVALTNINGSDEPARTEMENTET (DFD)  
Postboks 8004 Dep  
0030 OSLO

Deres referanse  
25/2152-1

Vår referanse  
25/03231-2

Dato  
06.10.2025

## Høringssvar – utlevering av IP-data for forebygging av alvorlig kriminalitet

### 1. Bakgrunn og oppsummering

#### 1.1 Bakgrunn

Datatilsynet viser til høringsbrev av 4. juli 2025, hvor Digitaliserings- og forvaltningsdepartementet ber om innspill på et forslag om å etablere hjemmel for utlevering av IP-data for å forebygge alvorlig kriminalitet.

I høringsnotatet foreslår Digitaliserings- og forvaltningsdepartementet og Justis- og beredskapsdepartementet (departementene) at det, innenfor nærmere angitte rammer, åpnes for utlevering av IP-data til PST og politiet.

Utlevering av IP-data til forebyggingsformål vil ifølge forslaget bare være tillatt dersom inngrepet ivaretar et legitimt formål, har tilstrekkelig hjemmel og er forholdsmessig. Dette følger av kravene etter blant annet Den europeiske menneskerettskonvensjon (EMK) artikkel 8 og Grunnloven § 102 om retten til privatliv. For at opplysninger skal kunne utleveres til forebyggingsformål foreslår departementene et vilkår om at det må være grunn til å undersøke om noen forbereder nærmere bestemte straffbare handlinger.

Datatilsynet forstår intensjonen med forslaget og har forståelse for at muligheten for å kunne undersøke aktivitet på internett kan ha betydning for forebygging av kriminalitet. Tilgang til informasjon om hvem som kan knyttes til bruk av en konkret IP-adresse vil kunne være viktig i denne sammenheng. Samtidig innebærer forslaget utfordringer knyttet til retten til privatliv, personvern, kommunikasjonsvern og ytringsfrihet (inkludert pressens kildevern), slik disse grunnleggende rettighetene er vernet av blant annet EMK og Grunnloven, slik departementene også peker på.

Som bakgrunn viser Datatilsynet også til vårt [tidligere høringssvar](#) i tilknytning til endringer i e-komloven i 2020, som drøfter prinsipielle og rettslige utfordringer knyttet til innhenting og utlevering av IP-adresser.

Datatilsynets merknader i dette høringsvaret vil i første rekke knytte seg til retten til privatliv og personvern i tråd med Datatilsynets mandat.

## 1.2 Oppsummering

Datatilsynets synspunkter er oppsummert:

- Forslaget bør ikke gjennomføres i sin nåværende form. Forslaget innebærer et potensielt alvorlig inngrep i retten til privatliv og andre grunnleggende rettigheter. Datatilsynet er ikke overbevist om forslagets forholdsmessighet – og at forslaget ligger innenfor rammene som EMK, Grunnloven og EØS-retten oppstiller.
- Det er en prinsipiell forskjell på utlevering av opplysninger til *forebyggingsformål*, som nå foreslås, sammenlignet med dagens adgang til utlevering med formål om å oppklare allerede *begått kriminalitet*. Forslaget åpner for utlevering av IP-opplysninger som følge av lovlige ytringer og handlinger. Konsekvensene førstnevnte kan ha for retten til privatliv og andre grunnleggende rettigheter er potensielt langt større enn for sistnevnte.
- Kretsen av personer som omfattes av datainnsamlingen vil øke betraktelig, informasjonstilgangen vil bli langt større og inngangskriteriet for forebyggingsformål er svært skjønnsmessig. Dette øker risikoen for en nedkjølingseffekt på kommunikasjon, informasjoninnhenting og annen lovlig aktivitet på nett. Økt skjønn tillagt myndighetene vil også øke rommet for formålsutglidning. Til bildet hører det også at en vil befinne seg utenfor de alminnelige rettssikkerhetsgarantiene som et individ vil ha i et straffespor.
- Etter Datatilsynets syn bør innhenting av IP-opplysninger helst underlegges en forutgående uavhengig domstolskontroll. Dette vil styrke forslagets forholdsmessighet og redusere betenkelighetene ved en skjønnsmessig ordlyd, så vel som bidra til økt rettssikkerhet og tillit. Etterkontroll er et svakt substitutt for forutgående kontroll.
- Forslagets inngangsvilkår for utlevering av IP-opplysninger i forebyggingsformål er vagt og skjønnsmessig og setter potensielt en (svært) lav terskel for utlevering. Etter Datatilsynets syn bør ordlyden i alle tilfeller kvalifiseres og klargjøres.
- Datatilsynet mener at hensynene til klarhet og tillit tilsier at politiets metode for innhenting av IP-opplysninger burde vært regulert selvstendig i lov.
- Forslaget bør ses i sammenheng med andre etablerte tiltak og virkemidler. Det er uklart for Datatilsynet hvordan IP-data man her vil kunne innhente, vil kunne kobles til annen informasjon som PST og politiet besitter. Summen av tiltak bør inngå i forholdsmessighetsvurderingen av forslaget. Generelt sett savner Datatilsynet noe mer prinsipielle og helhetlige vurderinger av behov for og konsekvenser av forslaget.

## 2. Datatilsynets vurdering

### 2.1 Rettslige utgangspunkter

EMK, Grunnloven og EØS-retten setter rammer for adgangen til å lagre og utlevere IP-opplysninger. Sentralt står retten til i privatliv, hjem og kommunikasjon som følger av EMK artikkel 8 og Grunnloven 102, så vel som ytringsfriheten (inkludert kildevernet) som følger av EMK artikkel 10 og Grunnloven § 100. I tillegg kan kommunikasjonsvernet etter kommunikasjonsdirektivet nevnes og særlig direktivets artikkel 15, som var gjenstand for behandling i sak [C-470/21 \(La Quadrature du Net II\)](#) som omtales i høringsnotatet.

Reguleringene har ulikt innhold, men grovt sammenfattet stiller bestemmelsene krav om at utlevering av IP-opplysninger til forebyggingsformål bare vil være tillatt dersom inngrepet er tilstrekkelig hjemlet, har et legitimt formål og er nødvendig og forholdsmessig sett opp mot det angitte formålet.

Lovkravet innebærer at det ikke bare skal foreligge en nasjonal lov som regulerer inngrepet, men stiller også kvalitetskrav til loven: Lovgivningen må være tilstrekkelig klar og forutberegnelig. Det kreves også at det foreligger tilstrekkelig rettssikkerhetsgarantier. Lovkravet i tilknytning til EMK artikkel 8 er nylig drøftet av Høyesterett i [HR-2024-775-A6](#).<sup>1</sup>

Forholdsmessighetsvurderingen, som ofte blir avgjørende i praksis, må foretas konkret og helhetlig. Vurderingen vil kunne variere fra sak til sak, men noen rettesnorer som en kjenner igjen fra EMDs praksis er om:

- inngrepet møter et presserende samfunnsmessig behov;
- inngrepet er egnet til å nå formålet/behovet;
- inngrepet kan oppnås med mer lempelige midler;
- om statens begrunnelse for inngrepet er relevant og tilstrekkelig; og
- om staten har funnet en rimelig balanse mellom behovet for inngrepet og de samfunnsmessige fordelene på den ene siden og hvor inngripende det er for individets rettigheter på den andre.<sup>2</sup>

Inngrepets art og karakter er sentralt i vurderingen. Jo mer inngripende og tyngende inngrepet er, samt jo mer i kjernen av den aktuelle rettigheten man befinner seg, desto mer vil kreves av formålet som rettferdiggjør inngrepet.

---

<sup>1</sup> Se HR-2024-775-A avs. 46 flg.

<sup>2</sup> Ibid. avs. 47 der det omtales som et krav om at «inngrepet må stå i rimelig forhold til det som søkes oppnådd». Det vises også til EMDs praksis om at nødvendighetskravet innebærer noe mer enn «useful», «reasonable» eller «desirable».

## *2.2 Innledende om inngrepets karakter*

Datatilsynet finner det klart at utlevering av en persons IP-adresse utgjør et inngrep i retten til privatliv etter EMK artikkel 8 og andre relevante rettigheter.

Spørsmålet er hvor stort eller alvorlig inngrepet er, herunder hvor omfattende utlevering til politi og PST vil være. I den forbindelse er det grunn til å se på forslagens inngangsvilkår, hvilke straffebud som er omfattet og den konkrete innvirkningen forslaget potensielt kan ha for retten til privatliv og andre grunnleggende rettigheter.

Sentralt for Datatilsynets vurdering er det at det er en prinsipiell forskjell mellom innsamling av opplysninger til forebyggingsformål sammenlignet med formål for å oppklare allerede begått kriminalitet, slik en har hjemmel til i dag. Konsekvensene førstnevnte kan ha for privatlivssfæren og de grunnleggende rettighetene til borgerne er potensielt langt større enn for sistnevnte.

Ved å inkludere forebyggingsformål vil kretsen av personer som omfattes øke betraktelig og informasjonstilgangen vil bli langt større. Inngangskriteriet for forebyggingsformål vil være langt mer skjønnsmessig. Dette kan igjen øke opplevelsen av statlig overvåkning med den nedkjølingseffekt det kan ha på utøvelsen av ytrings- og informasjonsfrihet så vel som retten til privatliv og kommunikasjon. En nedkjølingseffekt, eller «chilling effect» slik EMD omtaler det, kan oppsummeres som at borgere legger en demper på eller avstår fra lovlige ytringer, informasjonssøk eller handlinger som følge av en usikkerhet om eller bekymring for konsekvensene. Frykten for at ens ytringer og handlinger etterprøves, overvåkes eller brukes til formål en ikke er klar over, kan altså føre til en endret atferd og at individers rettigheter svekkes.

Videre vil en i forebyggings situasjoner normalt befinne seg utenfor de alminnelige rettssikkerhetsgarantiene som eksisterer i et straffespor ved etterforskning av begått kriminalitet (f.eks. ved at en ikke vil være «siktet» i et forebyggingsspor). Økt skjønn vil også øke rommet for formålsutglidning og vilkårlighet.

*Oppsummert* mener Datatilsynet en her står overfor et potensielt alvorlig inngrep i grunnleggende rettigheter. Vi kommer nærmere tilbake til dette under forholdsmessighetsvurderingen nedenfor.

## *2.3 Nærmere om forslagens ordlyd og lovkravet*

I henhold til lovforslaget kan informasjon om abonnent knyttet til IP-adresse utleveres til politiet og PST når det er «grunn til å undersøke» om noen «forbereder en handling» som etter loven kan medføre straff av fengsel i seks år eller mer, som nevnes i politiloven § 17 b, samt en rekke nærmere angitte straffebud med lavere strafferamme, jf. forslaget til ny § 3-14 første ledd bokstav b og c jf. fjerde ledd

Rammen for lovbrudd som omfattes er vid, noe som gjør det potensielle omfanget av forslaget svært stort.

Etter Datatilsynets syn kunne det vært en fordel i forarbeidene å foreta en gjennomgang og vurdering av hvilke straffebud en anser som mer relevante enn andre, for å gi en pekepinn for skjønnsutøvelsen. En kunne også vurdert en mer kasuistisk tilnærming, der loven konkret gjengir hvilke straffebud som omfattes, snarere enn å inkludere samtlige med en strafferamme på mer enn seks år (i tillegg til nærmere angitte straffebud). I lys av høringsnotatets vurdering av virkeområde og om strafferammen bør være tre eller seks år, vil Datatilsynet understreke at en eventuell reduksjon av inngangsvilkåret til å omfatte straffebud med en strafferamme på tre år eller mer klart *ikke* støttes av Datatilsynet. En grunn til det er at en da blant annet vil inkludere flere ytringsstraffebud, som straffeloven § 185 om hatefulle ytringer.

Videre er grunnvilkåret i ordlyden («grunn til å undersøke») vagt og skjønnsmessig – og setter potensielt en (svært) lav terskel. Selv om et slikt vilkår nødvendigvis vil måtte inneholde noen grad av skjønn og det er positivt at lovteksten peker på at det alltid skal foretas en konkret forholdsmessighetsvurdering ved utlevering, mener Datatilsynet likevel at ordlyden her er for uklar i lys av lovkravet. Ordlyden bør i alle tilfeller kvalifiseres og klargjøres. Akkurat hva en slik kvalifikasjon skal være må blant annet ses i sammenheng med hvorvidt Datatilsynets anbefaling om å innføre domstolskontroll imøtekommes.

I alle tilfeller kunne det også være en fordel med ytterligere retningslinjer i forarbeider for skjønnsutøvelsen. Dette kan bidra til å sikre tillit til systemet, og redusere risiko for nedkjølingseffekt.

Datatilsynet mener også at det er en mulig risiko at ordlyden i vilkåret ikke vil gjenspeile det som faktisk vil ende opp med å gi grunnlag for innhenting i praksis. Slik Datatilsynet forstår grunnvilkåret så knyttes det til forberedelse av en handling som omfattes av nevnte straffebud. Når det er tale om internettbruk så vil dette i mange tilfeller knytte seg til ytringer. Her er det grunn til å nevne at mange ytringsstraffebud (slik som hatefulle ytringer) ikke har en strafferamme på seks år, og følgelig ikke vil ligge innenfor bestemmelsens regulering. I høringsnotatet er det likevel uklart hvordan dette vil stille seg i praksis. Vi viser her til for eksempel høringsnotatet side 18 der det heter at:

«der politiet ser en person bli tiltakende radikalisert i diskusjonsfora på internett, eller nærmer seg grensen for straffbare ytringer i kommentarfelter, kan identifisering gjøre det mulig å sette i verk forebyggende tiltak, eksempelvis samtale med den aktuelle personen. Identifiseringen vil på denne måten kunne bidra til å forebygge lovbrudd».

Datatilsynet stiller altså spørsmål ved hvordan dette eksemplet forholder seg til lovens inngangsvilkår om at det må gjelde straffebud med seks års fengsel, som innebærer at mange ytringsstraffebud faller utenfor reguleringen. Selv om for eksempel terroroppfordring (straffeloven § 136) vil falle innenfor, kan eksemplet likevel illustrere risikoen for formålsutgliding, som er en iboende risiko ved en så skjønnsmessig ordlyd.

*Oppsummert* mener Datatilsynet at forslaget ordlyd er for vag og skjønnsmessig, og at den bør kvalifiseres og klargjøres.

## 2.4 Nærmere om forholdsmessighetsvurderingen og forslaget begrunnelse

Som redegjort for i foregående punkter mener Datatilsynet at man står overfor et potensielt vidtgående inngrep i retten til privatliv og personvernet så vel som ytrings- og informasjonsfriheten.

Spørsmålet blir da om dette alvorlige inngrepet likevel kan forsvares – og er forholdsmessig – sett opp mot behovet for og formålet bak inngrepet.

Forebygging av alvorlig kriminalitet representerer åpenbart et legitimt og tungtveiende formål. Det er likevel uklart for Datatilsynet i hvor stor grad forslaget vil bidra til oppnåelse av dette formålet i praksis. Spørsmålet er i hvilken grad utlevering av opplysninger om IP-adresser til forebygging vil øke oppnåelsen av de kriminalitetsforebyggende hensyn sammenlignet med de tiltakene som allerede eksisterer i dag. Forslaget innebærer at informasjonstilgangen blir større for PST og politiet, men det er ikke nødvendigvis noen automatikk i at økt mengde informasjon fører til at kriminalitetsbekjempelsen blir mer effektiv.

Sett i lys av inngrepets karakter mener Datatilsynet at effektene av inngrepet – så vel som sammenhengen med andre tiltak – kunne vært grundigere vurdert i høringsnotatet. I og med utleveringskriteriet knytter seg til handling kunne det for eksempel være relevant å se på de omfattende tvangsmidler for å avverge alvorlig kriminalitet som er hjemlet i straffeprosessloven § 222 bokstav d.

Datatilsynet savner også en grundigere vurdering av antatte ulemper ved forslaget, herunder den prinsipielle forskjellen som ligger mellom å *forebygge* kriminalitet sammenlignet med å oppklare allerede *begått* kriminalitet. Datatilsynet antar at allmennhetens forståelse for og tillit til utlevering for å oppklare begått kriminalitet vil være større enn utlevering i forebyggingsøyemed, ettersom sistnevnte også vil omfatte det som *de facto* er lovlige handlinger og ytringer på internett og vil omfatte langt flere personer. Dette vil også kunne inkludere barn og unge, som kan forsterke behovet for tydeligere rammer og vurderinger. Barn har et særlig vern etter EMK og Grunnloven så vel som etter for eksempel FNs barnekonvensjon.

*Oppsummert*, Datatilsynet mener at vurderingene og begrunnelsene som ligger til grunn for forslaget burde vært redegjort for i større detalj, sett i lys av inngrepets karakter og omfang. EMDs praksis viser at begrunnelsen og vurderinger som ligger til grunn for inngripende lovforslag, kan få betydning i en etterfølgende rettslig vurdering.<sup>3</sup> Datatilsynet er ikke overbevist over forslagets helhetlige forholdsmessighet ut fra forslagets nåværende form og begrunnelse.

---

<sup>3</sup> Se f.eks. *Animal Defenders International v. Storbritannia* (48876/08) avs. 108 og oppsummeringen i EMDs guide om EMK artikkel 8 (fra 28. februar 2025), side 15.

Videre vil forholdsmessigheten av inngrepet henge sammen med rettsikkerhetsgarantiene som er tilknyttet forslaget.<sup>4</sup> En presis lovtekst er en slik rettsikkerhetsgaranti, mens kontrollmekanismer er en annen sentral garanti. Disse to vil også henge sammen og kunne påvirke hverandre, slik vi kommer inn på i neste punkt.

### *2.5 Behovet for forutgående domstolskontroll*

Uavhengig domstolskontroll er en sentral rettsikkerhetsgaranti, som blant vil kunne redusere noen av betenkelighetene ved en skjønsmessig ordlyd, siden praktiseringen av inngangsvilkåret da vil avgjøres av en domstol fremfor PST og politiet selv.

Datatilsynet mener at forslaget, slik det foreligger nå, bærer preg av skjult overvåking på grunn av manglende informasjon til de registrerte og deres mulighet til å ivareta sine rettigheter. Dette er et viktig bakteppe for Datatilsynets vurderinger.

Det er gjort betydelig inngrep i borgernes rettigheter til informasjon og innsyn i personopplysningsloven § 16 bokstav b om unntak fra retten til informasjon og innsyn etter personvernforordningen artikkel 13, 14 og 15 for opplysninger som det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger. Hensynet til de registrertes rettigheter er spesielt tungtveiende når det gjelder utlevering til forebygging hvor det ikke er begått lovbrudd. De registrerte vil ikke ha noen mulighet til å ivareta sine rettigheter utover kontrollmekanismene.

Departementene vurderer behovet for en forutgående domstolskontroll, men konkluderer med at dette ikke anses nødvendig. Departementene oppsummerer det slik i høringsnotatet (side 30):

«I lys av hvor inngripende tiltaket er, de rammer som er satt for uthenting, reglene for politiets behandling av opplysningene og at behandlingen er underlagt tilsynskompetansen til Datatilsynet og EOS-utvalget, mener departementene at uavhengig forhåndskontroll ikke er en nødvendig sikkerhetsmekanisme for at uthenting av IP-data i forebyggingsøyemed skal være forholdsmessig».

I selve vurderingen baserer departementene seg særlig på at de tolker EU-domstolens avgjørelse i sak *La Quadrature du Net II* til ikke å stille noe slikt krav for det foreliggende forslaget.

Datatilsynet mener at en slik tolkning ikke nødvendigvis er opplagt. Avgjørelsen tar ikke stilling til spørsmålet en her står overfor. Dette er heller ikke et spørsmål som er tatt stilling til av EMD. Likevel kan deler av EU-domstolens avgjørelse etter vårt syn i det minste tas til

---

<sup>4</sup> Se EMDs guide om EMK artikkel 8 s. 15–16, der det heter at: «The procedural safeguards available to the individual will be especially material in determining whether the respondent State has, when fixing the regulatory framework, remained within its margin of appreciation. In particular, the Court must examine whether the decision-making process leading to measures of interference was fair and such as to afford due respect to the interests safeguarded to the individual by Article 8.»

inntekt for at domstolskontroll vil være et viktig tiltak for å sikre at forslaget er forholdsmessig.

Datatilsynet fremhever at avgjørelsen angår utlevering av opplysninger knyttet til allerede begått kriminalitet (om enn mindre alvorlig kriminalitet). Dette skiller seg etter vårt syn prinsipielt fra forebygging, siden førstnevnte formålsramme betraktelig snevrer inn både virkeområde og antall personer som kan omfattes.

Videre vektlegger EU-domstolen at myndighetene i saken ikke vil kunne koble nevneverdig med informasjon, men domstolens drøftinger viser at dette vil kunne være et sentralt hensyn i vurderingen av om domstolskontroll er påkrevd. For politiet og PSTs del vil mulighetene for sammenkobling med annen informasjon potensielt være betydelige så vidt Datatilsynet kan forstå. Det har etter vårt syn også betydning at forslaget vil ligge nærmere kjernen av grunnleggende rettigheter enn hva tilfellet var i den franske avgjørelsen, som gjaldt opphavskrenkelser på nett.

Uansett mener Datatilsynet at departementene med fordel kunne foretatt en grundigere vurdering av hvilke fordeler og ulemper forhåndskontroll ved domstol kunne gitt for forslaget, uavhengig av hvorvidt lovligheten av innhenting av IP-opplysninger til forebyggingsformål er endelig avklart av EU-domstolen, EMD eller en annen autoritativ instans.

*Oppsummert*, Datatilsynet mener at dette er en type forslag der forutgående domstolskontroll typisk vil kunne være en viktig rettssikkerhetsmekanisme – og et viktig bidrag til å sikre tiltakets lovlighet og forholdsmessighet. Datatilsynet anbefaler at domstolskontroll revurderes og helst innføres.

## *2.6 Etterfølgende tilsyn har ikke samme effekt som domstolskontroll*

Departementenes vurdering av at forhåndskontroll ikke er nødvendig begrunnes blant annet med at behandlingen av opplysningene er underlagt tilsynskompetansen til Datatilsynet og EOS-utvalget.

Selv om etterfølgende kontrollmekanismer har betydning i forholdsmessighetsvurderingen, mener Datatilsynet at en etterfølgende kontroll gir (klart) svakere rettssikkerhetsgarantier enn en forutgående domstolskontroll. Betydningen av forutgående kontroll understøttes av praksis fra EMD.<sup>5</sup>

Sett i lys av Datatilsynets brede mandat, store saksmengde og dagens ressurser, mener tilsynet selv det er tvilsomt om Datatilsynets kontrollmekanisme på dette feltet vil kunne tillegges nevneverdig vekt i forholdsmessighetsvurderingen.

---

<sup>5</sup> Se f.eks. Big Brother Watch og andre v. Storbritannia (58170/13) avs. 350 som understreker betydningen av «end-to-end safeguards» i tilknytning til statlige overvåkingstiltak.



Datatilsynet er også enig med KK-utvalget som i sin høringsuttalelse påpeker at rammene for tilsyn og kontroll er uklare. Dette bør i alle tilfeller klargjøres nærmere.

### *2.7 Metodebruken bør reguleres i lov*

Datatilsynet mener at politiets og PSTs metode for innhenting av IP-data burde vært regulert selvstendig i lov. Generelt er det en svakhet at politiets metoder kan være uhjemlet, herunder av hensyn til klarhet overfor individene som berøres og deres rettigheter så vel som den demokratiske forankringen. Tiltak som kan gi større klarhet rundt politiets metode og bruken vil generelt kunne øke tilliten til systemet – noe som vil spille positivt inn i en forholdsmessighetsvurdering.

Dette bør særlig være utgangspunkt på et område hvor legalitetsprinsippet gjør seg tungt gjeldende, slik tilfellet vil være her.

### **3. Helhetsbildet og sammenhengen med øvrige virkemidler**

Datatilsynet mener at det er viktig å se forslaget som nå er på høring i sammenheng med andre etablerte tiltak, overvåkningsmetoder (hjemlede og uhjemlede) og adgang til informasjonsutveksling, for å være i stand til å vurdere den samlede effekten. Et spørsmål er hvordan utleverte IP-opplysninger i henhold til lovforslaget kan kobles til annen informasjon. Dette er uklart for Datatilsynet. Selv om ett inngrep isolert kan ha en mer avgrenset negativ konsekvens for den enkelte borger, vil summen av inngrep kunne være stor.

Flere har de seneste år etterlyst en mer samlet vurdering av statlige myndigheters hjemler, kapasiteter og praksis på dette området. Departementenes lovforslag gir etter Datatilsynets syn en god foranledning til å vurdere disse spørsmålene mer helhetlig. For det foreliggende forslagets del vil også den helhetlige kapasiteten påvirke den konkrete forholdsmessighetsvurderingen.

Datatilsynet er tilgjengelig for nærmere utdypninger og kommentarer.

Med vennlig hilsen

Line Coll  
direktør

Jan Henrik Mjønes Nielsen  
juridisk spesialrådgiver

*Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer*