TRUESEC

Justitiedepartementet

Skickat per epost till: ju.remissvar@regeringskansliet.se med kopia till ju.da@regeringskansliet.se

Diarienummer Ju2024/02286

Stockholm den 17 januari 2025

# Ang. utkast till lagrådsremiss Datalagring och tillgång till ekonomisk information (diarienummer Ju2024/02286)

Truesec har genom remiss den 22 november 2024 beretts tillfälle att yttra sig över utkast till lagrådsremiss, Datalagring och åtkomst till elektronisk kommunikation, avseende betänkandet SOU 2023:22, Datalagring och åtkomst till elektronisk information. Truesec berörs enligt remissen särskilt av avsnitt 7.4 (”*Anpassningsskyldighet*”) och har i anledning av detta valt att inleda kommentarerna på remissunderlaget med en genomgång av avsnitt 7.4 innan övriga kommentarer följer därefter.

## Sammanfattning

Truesec instämmer i att brottsbekämpande myndigheter behöver kunna verkställa hemliga tvångsmedel och beivra brott på ett effektivt sätt. När det gäller just anpassningsskyldigheten anser vi dock att förslaget inte tillräckligt har belyst de praktiska konsekvenserna för säkerheten i de berörda kommunikationstjänsterna. Det finns utöver detta stora risker relaterade till både individens och samhällets rätt till skydd för privatliv och förtrolig kommunikation med förslaget. Därför avstyrker Truesec att förslaget i fråga om anpassningsskyldighet godtas och föreslår att ärendet utreds igen i denna fråga, helst med medverkan av cybersäkerhetsexpertis.

Till grund för denna generella kommentar om anpassningsskyldigheten ligger bl.a. följande:

- **Brister i utredningens allmänna säkerhetsperspektiv:** enligt Truesec saknas tillräcklig sakkunnig expertis inom cyber och cybersäkerhet i utredningen. Detta gör att konsekvenserna för totalsträckskrypterade s.k. *nummeroberoende interpersonella kommunikationstjänster* (”**NOIK**”) inte är tillräckligt utredda, särskilt hur förslaget kan leda till sämre säkerhet för samtliga användare.
- **Risk specifikt för försvagning av kryptering:** för att möjliggöra avlyssning ska leverantörer av NOIK införa någon form av teknisk anpassning, som sannolikt kommer röra sig om tekniska bakdörrar eller huvudnycklar för sådana tjänster som är krypterade (trots utredningens kommentar om motsatsen). Anpassningsskyldigheten riskerar att försvaga kommunikationen även för legitima användare samt kan öka risken för intrång och för att förtroende för säkra kommunikationstjänster undermineras.
- **Tveksam effektivitet mot kriminella:** risken för att kriminella väljer andra kanaler och/eller tjänster för sin kommunikation bör diskuteras närmare för att säkerställa att lagförslaget inte behöver ändras i närtid igen för att ytterligare utöka lagens räckvidd.

För frågor hänförliga till lagringsskyldighet noterar Truesec följande:

- **Nationell säkerhetslagring och rättssäkerhet:** om Säkerhetspolisen både beslutar om hotnivå och om omfattande lagring kan detta skapa en intressekonflikt. Avsaknad av tydlig separation mellan Säkerhetspolisen och kontrollorganet samt avsaknad av fasta tidsfrister/karenstider gör att lagringen kan bli långvarig utan tillräcklig granskning av oberoende instans, vilket kan vara ett hot mot rättssäkerheten.
- **Ändamålsglidning och integritetsrisker:** förslaget möjliggör att data insamlad med hänvisning till nationell säkerhet senare kan användas i andra syften. Truesec varnar för en successiv utvidgning av övervakningsbefogenheter som drabbar även laglydiga medborgare eller brottstyper som egentligen faller utanför den tänka omfattningen.

## Synpunkter på avsnitt 7.4

Lagrådet har i utkast till remiss över SOU 2023:22 föreslagit lagändringar som ålägger tillhandahållare av NOIK att utforma sina tjänster så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, samt inhämtning enligt inhämtningslagen (2012:278), kan verkställas effektivt och utan att verkställandet röjs. Utredningen betonar att brottsbekämpande myndigheter effektivt måste kunna genomföra beslut om hemliga tvångsmedel och framhåller att dessa myndigheters behov väger tyngre än enskildas motstående intressen av grundläggande fri- och rättigheter relaterade till integritet och skyddet för privatliv.

Flera remissinstanser (däribland Bahnhof, Institutet för mänskliga rättigheter och Sveriges Advokatsamfund) har i remissvar över SOU 2023:22 betonat nödvändigheten av en fördjupad problematisering kring riskerna för den personliga integriteten. Truesec — i rollen som cybersäkerhetsexpert och expert inom dataskydd med lång praktisk erfarenhet av att hantera avvärja, upptäcka och avhjälpa dataintrång — vill härutöver även lyfta de säkerhetsmässiga implikationer som förslaget innebär för såväl tillhandahållare som användare av NOIK.

En allmän anmärkning – utan att detta ska uppfattas som en värdering av de inblandades faktiska kompetens – är att utredningen vid en genomgång av bidragande personers roller på s. 3-4 i SOU 2023:22 till synes saknar sakkunskap inom cyber och cybersäkerhet. Mot bakgrund av utredningens uppdrag hade sådan kompetens varit önskvärd för att klargöra bland annat vad den nu eftersträvade ”teknikneutraliteten” kan resultera i vid implementering, hur säkerhets- och krypteringsfrågor påverkas av att krypterad data ska kunna göras tillgänglig för utomstående, samt hur viktigt ett högt förtroende för en säkerhetslösning är.

Genomgående för detta remissvar utgår Truesec från situationen att en NOIK erbjuder användaren en totalsträckskrypterad (”end-to-end encrypted”) kommunikationslösning, då detta är den kommunikationslösning idag som erbjuder användaren högsta möjliga säkerhetsnivå och som därför är sannolik att användas både av kriminella och för legitima ändamål av andra än kriminella.

**Bristande utredning av säkerhetsperspektivet**

Tillhandahållare av NOIK som erbjuder krypterad kommunikation som ska leva upp till den föreslagna anpassningsskyldigheten ska enligt förslaget anpassa sin tjänst så att brottsbekämpande myndighet kan avlyssna eller övervaka denna. Av nödvändighet betyder detta att myndighet ska kunna läsa krypterad kommunikation i klartext. Utredningen anger att det är fullt möjligt för tillhandahållare av NOIK att utforma sina tjänster så att kraven på säkerhet och skyddet för kommunikation tillgodoses.

Truesec är kritiska mot utredningens summariska genomlysning av anpassningsskyldighetens praktiska konsekvenser och vilka säkerhets- och integritetsrisker som skyldigheten kan leda till. Det kan också noteras att lagrådsremissen saknar konkret återkoppling på den oro för säkerhet och integritet som tidigare remissinstanser uttryckt i sina remissvar till utredningen. I stället hänvisar lagrådsremissen till tillhandahållarnas möjlighet att leva upp till de säkerhetskrav som ställs i lagen om elektronisk kommunikation, vilket blir särskilt anmärkningsvärt som remissinstansernas oro riktar sig till säkerheten och skyddet för användarnas kommunikation, inte till tillhandahållarnas eventuella möjligheter att leva upp till en minimisäkerhetsstandard som fastställs i lagen om elektronisk kommunikation. Frånvaron av en robust analys av denna del av frågan – en enligt Truesecs mening avgörande del för att utvärdera förslagets lämplighet, proportionalitet och ändamålsenlighet – är ett värdefullt exempel på den ensidiga vikt utredningen lägger vid myndigheternas behov och önskemål samt för Truesecs generella invändningar mot att acceptera utredningens lagförslag.

För sådan NOIK som är totalsträckskrypterad har endast användare som använder NOIK:en tillgång till de krypteringsnycklar som krävs för att kunna dekryptera specifikt deras kommunikation. Ingen mellanhand kan med andra ord få tillgång till kommunikationen. (”Mellanhand” i det här sammanhanget omfattar såväl brottsbekämpande myndigheter, tjänsteleverantörer och nätverksoperatörer som hotaktörer.) I Truesecs mening hade det därför inte bara varit värdefullt för tillhandahållare av NOIK, utan nödvändigt för att kunna utvärdera de praktiska effekterna av förslaget, att utredningen i större utsträckning genomlyst konsekvenser för säkerheten i krypterade data till följd av att ålägga tillhandahållare av NOIK en anpassningsskyldighet.

I enlighet med vad utredningen för fram innebär förslaget inte uttryckligen att någon generell sårbarhet ska införas i kryptering eller att systematiska bakdörrar ska introduceras. I praktiken kommer ett genomförande av anpassningsskyldigheten kräva att krypterade NOIK:ar anpassas tekniskt för att kommunikationen ska kunna övervakas eller avlyssnas. En sådan anpassning kommer, för att vara enkelt tillgänglig och kostnadseffektiv, att behöva inkludera någon form av sårbarhet, ”bakdörr”, tillgång till huvudnycklar eller teknisk möjlighet att agera s.k. ”*man in the middle*” eller ”mellanhand” för att bryta en krypterad kommunikationskanal. Oavsett hur anpassningen genomförs riskerar tillhandahållare av NOIK i realiteten att behöva vidta säkerhetssänkande åtgärder. Skälet till att användare av en krypterad (och särskilt totalsträckskrypterad) kommunikationskanal kan lita på att det som kommuniceras inte övervakas eller avlyssnas är att detta har säkerställts kryptografiskt, dvs. att anpassningar inte har skett.

Exempel på hur en anpassning i form av en ”mellanhand” eller ”man in the middle” är att krypterad kommunikation leds genom tillhandahållarens infrastruktur där den krypterade kanalen dekrypteras, kommunikation avlyssnas i klartext och sedan återkrypteras för att transporteras vidare till den andra parten i samtalet. En uppenbar och kritisk sårbarhet öppnas därmed i den del av kanalen där kommunikationen dekrypteras för att läsas ut i klartext, vilket därmed också blir en attackyta att exploatera av annan part än svensk brottsbekämpande myndighet.

Om den nu föreslagna anpassningsskyldigheten innebär att tillhandahållaren ska kunna möjliggöra hemlig avlyssning eller övervakning av kommunikation i NOIK:en skulle detta med andra ord innebära att NOIK som finns tillgänglig i Sverige inte kan betraktas som totalsträckskrypterad, eftersom sådan anpassning introducerar just sådana säkerhetsbrister som lösningarna syftar till att lösa.

Utöver att den enskilda kommunikationen mellan särskilda användare ska kunna dekrypteras riskerar den säkerhetssänkande åtgärden att påverka även andra användare av den specifika NOIK:en. Detta för att t.ex. en hotaktör som framgångsrikt bereder sig tillgång till tillhandahållarens miljö och en sådan huvudnyckel därmed har möjlighet att läsa annars krypterad kommunikation i realtid samt, om denna finns lagrad, även dekryptera sådan information för samtliga användare vars krypteringsnycklar kan dekrypteras med den aktuella huvudnyckeln. Detta är ett väsentligt annorlunda scenario från att en enskild användares krypteringsnyckel kompromet teras, för i detta fall drabbas inte någon annan användare.[1]

Att totalsträckskryptering försvåras är problematiskt även i kontexten av brottsbekämpande myndigheters arbete i relation till nationell säkerhet eller särskilt grov brottslighet eftersom den säkerhetssänkande anpassningen drabbar samtliga användare av krypterade NOIK (inte endast misstänkta och kriminella som *de facto* blir föremål för hemliga tvångsmedel). Utan ett internationellt samarbete i dessa frågor är det enligt Truesecs mening en överhängande risk att såväl legitima som kriminella användare byter till utländska tjänster som orsakar en

[1] En intressant fallstudie som berör svårigheten i att hålla centrala kryptonycklar säkra är att Microsoft i juli 2023 blev hackade av den Kina-baserade hackergruppen *Storm-0558* som med stulna inaktiva kryptonycklar lyckades stjäla viss kundinformation. Värt att notera i sammanhanget är Microsofts mycket stora fokus på, och stora investeringar i, cybersäkerhet, och att de ändå blev framgångsrikt angripna.

nettoförsämring i brottsbekämpande myndigheters möjligheter att bedriva sitt arbete och särskilt att verkställa beslut om hemliga tvångsmedel.

Den osäkerhet kring medborgares rätt till skydd av sitt privatliv och sin förtroliga kommunikation som uppstår riskerar i sin tur att orsaka en betydande inskränkning i medborgarnas grundläggande fri- och rättigheter och får ses som ett ytterligare steg på ett sluttande plan mot ett inte önskvärt övervakningssamhälle. Om det sker en ändamålsglidning i tillämpningen av bestämmelserna riskerar det i sin tur dessutom att orsaka ytterligare inskränkningar i fri- och rättigheter som ingen medborgare i en demokrati och rättsstat ska behöva tåla.

**Definitionen av NOIK, teknikneutralitet och ändamålsenlighet**

Det uppställs krav på att en NOIK ska tillhandahållas mot ersättning för att omfattas av lagförslagets definition,[2] vilket t.ex. Apple argumenterar för i remissvar till SOU 2023:22 ska undanta deras tjänster. Det skulle med motsvarande tolkning kunna undanta även populära tillhandahållare av krypterade NOIK som är ideella organisationer som finansierar sina verksamheter genom offentliga bidrag/anslag och donationer men som inte har monetiserat sina kommunikationstjänster.

En NOIK ska därutöver vara en tjänst som "möjliggör ett direkt interpersonellt och interaktivt informationsutbyte [...] mellan ett begränsat antal personer." Såsom Truesec förstår förslaget innebär detta att tillhandahållare av lagringsytor eller delning av dokument (t.ex. SharePoint, OneDrive, Drive, Dropbox och Box) inte omfattas av motsvarande krav på anpassningsskyldighet (såvida detta inte framgår av annan lagstiftning). Däremot är det inte uppenbart i vilken utsträckning t.ex. kommunikation genom att dela lagringsytor eller dokument skulle underställas motsvarande krav på att tillhandahållarna av sådan tjänst ska kunna dekryptera lagrade eller delade data. Med lagförslaget riskerar vi i sådant fall att vara på ett sluttande plan mot ett allt starkare övervakningssamhälle utan att de enskildas grundläggande fri- och rättigheter tillmäts tillräcklig vikt, då samma argument om "behov" och "nödvändighet" att bereda sig åtkomst till potentiella bevis vid brottsbekämpning kan återanvändas för att ytterligare utöka omfattningen av dylika befogenheter och tvångsmedel.

Med hänvisning till samma motivation att brottsbekämpande myndigheter har behov att kunna verkställa beslut om vissa hemliga tvångsmedel föreslår utredningen en "teknikneutral lagstiftning". Syftet med teknikneutralitet är enligt utredningen och lagrådet dels att säkerställa möjligheten att verkställa omnämnda beslut, dels att hantera risken för att kriminella väljer en NOIK framför en traditionell kommunikationstjänst för att undvika obehörigas åtkomst till deras kommunikation.

[2] SOU 2023:22 s. 327.

Utöver riskerna:

- för att skada syftet med totalsträckskrypterade kommunikationstjänster även för legitima ändamål och därmed enskildas förtroende för och tillgång till säkra kommunikationskanaler; samt
- för att det i praktiken blir svårt till omöjligt att verkställa beslut mot utländska tillhandahållare

bör således även frågan om "teknikneutralitet" och huruvida utredningens ändamål uppfylls av de föreslagna lagändringarna behandlas.

I Truesecs mening tar inte utredningen tillräcklig hänsyn till skillnaderna mellan formen för de tjänster som idag omfattas av lagen om elektronisk kommunikation och NOIK: dels det faktum att många NOIK är (totalsträcks)krypterade, dels att användarnas rimliga förväntningar på sådana tjänster och på rättssamhället i stort är att (totalsträcks)kryptering skyddar data från obehörigas åtkomst. Detta bör, i motsats till utredningens slutsats, leda till förhöjda och svåraccepterade risker både i fråga om säkerhet och integritet. Till detta kommer även det faktum att mängden och typen av data som produceras och delas inom en NOIK med många magnituder överstiger vad som produceras och delas genom traditionella telefonsamtal, sms och e-posttjänster, vilket ytterligare bör leda till förhöjd risk i fråga om både säkerhet och integritet.

**Slutsatser**

Oavsett hur anpassningsskyldigheten implementeras av de enskilda tillhandahållarna finns det i vår mening en överhängande risk att tillgången till totalsträckskrypterade kommunikationstjänster begränsas för svenska medborgare och företag. Detta får betraktas som en avsevärd säkerhetssänkade åtgärd för såväl enskilda som för samhället i stort – detta dessutom i en tid både av oroande politisk utveckling och polarisering samt där lagstiftare inom EU tvärtom stiftar lagar med avsikten att höja den gemensamma cybersäkerheten.

Truesec anser mot bakgrund av ovan att utredningens förslag har metodologiska och systematiska brister vad gäller vilka säkerhetsrisker som berörs, omfattningen av dessa och kopplingen till grundläggande fri- och rättigheter. Enligt vår mening går det också ifrågasätta huruvida lagförslaget kommer att uppfylla sitt syfte. Truesec anser därför att utredningen inte tar tillräcklig hänsyn till eller utreder relevanta säkerhets- och rättighetsrisker. Truesec avstyrker därför lagrådet från att godta den presenterade utredningen vad gäller anpassningsskyldigheten och dess säkerhets- och rättighetsrisker, samt att utredningen, trots den tidsutdräkt som detta innebär, kompletteras. För sådan ny utredning bör en expertgrupp med lämpliga representanter från relevanta aktörer inom cybersäkerhet och informationssäkerhet tillsättas som stöd till utredaren.

## Synpunkter på vissa övriga avsnitt

I följande avsnitt presenteras vissa mer allmänt hållna kommentarer och synpunkter på utkastet till lagrådsremiss.

**Avsnitt 6.2—6.4**
Truesec är positiva till förslaget i stort. Däremot finns ett flertal kommentarer och risker som Truesec vill lyfta i enlighet med nedan.

Om Säkerhetspolisen både bedömer hotnivån och beslutar om mer omfattande lagring uppstår en risk för intressekonflikt och otillräcklig oberoende granskning, vilket kan underminera rättssäkerheten. Därtill finns en risk att ett beslut om allvarligt hot mot Sveriges säkerhet och därtill relaterad nationell säkerhetslagring kan kvarstå under lång tid, vilket i praktiken medför att stora datamängder lagras under avsevärda tidsperioder. Detta skapar betydande informationssäkerhets- och dataskyddsrisker för såväl individer som företag vars uppgifter omfattas av lagringen.

Mot bakgrund av dessa långtgående konsekvenser anser Truesec att Säkerhetspolisen, i stället för att själv besluta om nationell säkerhetslagring, bör ges befogenheten att påkalla ett förfarande hos Försvarsunderrättelsedomstolen. Domstolen skulle då kunna pröva Säkerhetspolisens förslag och besluta om att godkänna eller avslå det. En sådan modell skulle bättre säkerställa proportionalitetsprincipen. Vidare bör den enskilde fortfarande garanteras lämplig representation i processen. Att begränsa ombudet till en enda person och tillsätta denne för en kort tidsperiod (t.ex. tre år) kan enligt Truesec dock medföra en alltför stor beroenderisk av en enda person samt begränsa möjligheten för ombudet eller dennes ställföreträdare att utveckla tillräcklig kompetens för att effektivt värna den enskildes intressen.

**Avsnitt 6.3—6.4**
Med hänsyn till att Säkerhetspolisen kan fatta både hotbedömningsbeslut och beslut om nationell säkerhetslagring, samt att ett sådant lagringsbeslut får omedelbar effekt och inte prövas mot någon fast tidsfrist, vill Truesec påpeka att prövningen riskerar att dra ut på tiden. Under tiden gäller beslutet om lagring utan att en rättslig prövning har skett. Detta blir särskilt problematiskt då Säkerhetspolisen kan fatta nya beslut om samma förhållanden utan karenstid, att enskilda företräds endast genom ett ombud, att det sker i en hemlig process, och att det saknas möjlighet att överklaga Försvarsunderrättelsedomstolens beslut. Truesec ser en risk för att sådan ordning inte tillräckligt garanterar den enskildes rättssäkerhet och riskerna för inskränkningar i den personliga integriteten.

**Avsnitt 6.6**

Truesec vill också, mot bakgrund av den föreslagna brottskatalogen, understryka vikten av att data som insamlats med hänvisning till nationell säkerhet endast inhämtas eller görs tillgänglig just i syfte att skydda nationell säkerhet. Här uppstår frågan om ändamålsglidning, särskilt med beaktande av att brottsrubriceringen ”sabotage” i vissa fall använts mot exempelvis miljöaktivister under senare år (även om detta framgångsrikt överklagades till Svea hovrätt visar det på riskerna t.ex. med ändamålsglidning och behovet av noggranna överväganden även av följdrisker vid denna typ av mer långtgående och potentiellt inskränkande lagförslag).

*Vänligen,*

Levi Bergstedt
*Chefsjurist*
Epost: levi.bergstedt@truesec.se

Mårten Thomasson
*Informationssäkerhetschef*
Epost: marten.thomasson@truesec.se