

Justitiedepartementet

ju.remissvar@regeringskansliet.se  
ju.da@regeringskansliet.se

Stockholm den 17 januari 2025

## **Telenors svar i remiss av utkast till lagrådsremiss Ju2024/02286**

Telenor Sverige AB (Telenor) lämnar följande svar i regeringens remiss av utkast till lagrådsremiss om datalagring och åtkomst till elektronisk information.

### **Inledning**

EU-domstolen har i ett antal avgöranden om datalagring på senare år slagit fast att generell och odifferentierad datalagring som huvudregel inte kan accepteras inom EU, med hänvisning till EU:s stadga om de grundläggande rättigheterna och det s.k. ePrivacy-direktivet. Domstolen hänvisar till att datalagring för utredning av allvarliga brott måste begränsas så att lagringen endast sker i specificerade undantagsfall, exempelvis genom att införa riktad lagring. Däremot kan en generell och odifferentierad lagring accepteras om det är strängt nödvändigt i situationer där nationell säkerhet är hotad. I datalagringsutredningen SOU 2023:22 föreslogs därför att Sverige går över till riktad lagring för utredning av allvarliga brott och samtidigt inför en möjlighet att under exceptionella omständigheter införa en tidsbegränsad nationell säkerhetslagring. Regeringen föreslår i remitterat utkast till lagrådsremiss däremot endast att gå vidare med den nationella säkerhetslagringen. Det anges inte i utkastet varför riktad lagring eller annan begränsning av lagring för brottsutredning inte är aktuellt.

I utkastet till lagrådsremiss föreslås i stället en utökad datalagring för brottsutredning. Detta synes gå tvärt emot EU-domstolens avgöranden. Utkastet till lagrådsremiss gör ingen analys av hur EU-domstolens avgöranden står i relation till denna utvidgade och förlängda generella och odifferentierade lagringen för brottsutredning.

Lagringskraven har ändrats med jämna mellanrum under de senaste 10 åren och varje omtag har varit mycket resurskrävande för Telenor och andra lagringsskyldiga. Utkastet till lagrådsremiss föreslår stora ändringar i hur data ska lagras som bland annat innebär fler lagringssituationer, längre lagringstider och fler uppgiftskategorier, samtidigt som förutsättningarna för när lagring ska ske och hur lagringen och utlämningen av uppgifter ska genomföras blir mer komplexa att hantera.

Vid en analys av utkastet till lagrådsremiss är det uppenbart för Telenor att den föreslagna ordningen löper stor risk att underkännas vid en rättslig prövning med

utgångspunkt i e-Dataskyddsdirektivet och EU:s stadga om de grundläggande rättigheterna. I förlängningen riskerar detta leda till att kraven även framgent måste ändras och att Telenor och andra lagringsskyldiga på nytt måste bygga om och anpassa relevanta system och processer.

För att skapa en hållbar lösning är det viktigt att denna gång säkerställa en EU-omfattande harmonisering som både tillgodoser de brottsutredande myndigheternas behov och tar tillräcklig höjd för det grundlagsreglerade skyddet för privatlivet och konfidentialiteten i elektroniska kommunikationer. EU-harmoniserade bestämmelser skulle också underlätta marknadsinträde, säkerställa effektivitet och undvika snedvridning av konkurrensen. Regeringen anger i utkastet att EU-harmonisering ligger långt bort i tiden och att man med hänsyn till Sveriges säkerhet inte har tid att invänta harmoniserad reglering. Telenor vill dock anmärka att frågan nyligen lyfts av den tillträdde EU-kommissionen som prioriterad för 2025. Därtill är intresset av Sveriges säkerhet främst relevant i förhållande till förslaget om nationell säkerhetslagring, och motiverar inte att den ordinarie datalagringen för brottsutredning utökas.

## **Närmare om förslagen i utkastet**

### *Uppgiftskategorier*

Redogörelsen på s. 33 i utkastet bekräftar Telenors syn på att begreppet "uppgift om abonnemang" inte är tydlig. Regeringen hänvisar i denna del till praxis och möjligheten för PTS att meddela föreskrifter. Det framstår för Telenor alltjämt som oklart när en IP-adress ska anses utgöra en uppgift om abonnemang eller när den har karaktär av trafikuppgift. Enligt tidigare uttalande från PTS bör det vara avhängigt hur adressen tilldelats och huruvida den genereras vid trafikfallet eller är bestämd på förhand. En IP-adress torde således kunna omfattas av olika krav utifrån omständigheterna i det enskilda fallet. IP-adresser är också generellt mer integritetskänsliga än uppgifter om abonnemanget.

### *Lagring för brottsutredning*

Regeringen anger på s. 34 att uppgifter om abonnemang är mindre känsliga än andra uppgifter och ser därför inga problem att frångå den hittills gällande principen att uppgifter som lagras för brottsutredande ändamål inte får behandlas för något annat ändamål. Detta är mycket olyckligt och Telenor saknar förståelse för regeringens inställning. Det påstås i sammanhanget att den hittills gällande begränsningen riskerar "att leda till att uppgifterna behöver hållas separerade från andra uppgifter om abonnemang och att samma uppgifter lagras dubbelt, vilket kan innebära en ökad börda för de lagringsskyldiga". Detta är inte korrekt. Det uppkommer inget behov av att separera uppgifter och det uppstår inget dubbelt lagringsbehov om begränsningen vidhålls. Tvärtom har det varit styrande för designen och säkerheten i lagringssystemen att uppgifter som lagras i dessa avskilda system endast får behandlas i samband med förfrågningar från brottsutredande myndigheter i ärenden som gäller allvarlig brottslighet. Det ligger inte i linje med grundläggande principer om proportionalitet att öppna upp tillgången till lagrade uppgifter för andra ändamål än brottsbekämpning. Det står också uttryckligen i strid med de överväganden som tidigare lagts till grund för att tvinga operatörer att lagra uppgifter som de inte behöver för andra ändamål.

Regeringen föreslår ingen begränsning av den generella lagring som krävs i nuvarande reglering. I stället föreslår regeringen att denna lagring utökas. Detta står i kontrast till de avgöranden från EU-domstolen som tydligt anvisar att lagring av trafikuppgifter för brottsutredning måste inskränkas så att den inte utgör huvudregel. Förslaget förefaller dessutom inte förenligt med de utredningsdirektiv som låg till grund för 2023-års datalagringsutredning, där det angavs att utredningen särskilt skulle beakta den senaste rättsutvecklingen på EU-nivån.

9 kap. 22 § LEK anger avseende telefonitjänst och meddelandehantering via mobil nätanslutningspunkt att lokaliseringssuppgifter endast ska lagras i två månader. Anledningen till begränsningen av lagringstiden är att lokaliseringssuppgifter är särskilt känsliga med hänvisning till skyddet för privatlivet och den personliga integriteten. I praktiken krävs dock att lokaliseringssuppgifter vid användning av mobiltelefon lagras i 6 månader. Förklaringen till detta är uppgift som identifierar den utrustning där kommunikationen slutligt avskiljs i dessa fall utgör en lokaliseringssuppgift. Lagen ger sken av att lokaliseringssuppgifter endast lagras i 2 månader medan det i praktiken således råder ett krav på att positioner lagras av mobiloperatörerna i 6 månader (se prop.2018/19:86 på sid 45-46). Förslaget till ändringar i 9 kap. 22 § bör tydligt anvisa att lokaliseringssuppgift endast får lagras i 2 månader, även i de fall den utgör uppgift om den utrustning där kommunikationen slutligt avskiljs.

### *Nationell säkerhetslagring*

Den nationella säkerhetslagring som föreslås ska endast kunna aktualiseras under exceptionella omständigheter. Det måste finnas konkreta bevis att det råder ett allvarligt hot mot Sveriges säkerhet som är verkligt och aktuellt eller tydligt förutsebart. Lagringen måste vara tidsmässigt begränsad till vad som är strikt nödvändigt och beslut om nationell säkerhetslagring måste upphävas omedelbart om förutsättningarna inte längre är för handen. I ett beslut måste det anges i detalj vilka aktörer som beslutet riktar sig mot och vilka uppgiftskategorier och lagringstider som gäller. Även i situationer där nationell säkerhetslagring är motiverad, är det inte nödvändigtvis påkallat att alla uppgiftskategorier ska lagras, att lagringstiden ska vara den maximala eller att samtliga lagringsskyldiga ska aktivera lagringen.

Nationell säkerhetslagring får inte i praktiken bli en permanent lagring, såsom exempelvis blivit fallet i Danmark. Begreppet "Sveriges säkerhet" får inte urvattnas. Åtkomsten till lagrade uppgifter bör därtill inskränks till åtgärder som syftar till att förebygga, förhindra eller upptäcka hot mot Sveriges säkerhet.

Regeringen föreslår att lokaliseringssuppgifter som inte är trafikuppgifter ska innefattas i nationell säkerhetslagring med en lagringstid på 1 år. Denna typ av uppgifter har inte omfattats av lagringsskyldighet sedan tidigare och Telenor vill betona att det rör sig om en oerhört stor mängd uppgifter. Då nästan alla personer har mobiltelefon med sig hela tiden innebär lagringen en tidigare aldrig skådad massövervakning av befolkningen i nära realtid. Det är en stor skillnad mot att endast lagra positioner som genereras vid enskild användning av elektroniska kommunikationstjänster.

### *Sanktionsavgifter mm*

Sanktionsavgifter kan på grund av sin straffrättsliga karaktär endast motiveras när en skyldighet är tydlig vad gäller tolkning och tillämpning, och detta gäller även om skyldigheten som sådan kan betraktas som särskilt angelägen utifrån allmänna intressen. De föreslagna reglerna kring lagring av uppgifter är inte allt genom tydliga när det gäller definitioner och de närmare förutsättningarna för lagringsskyldighet. Detta bekräftas av regeringen i utkastet som bl.a. anger att vissa definitioner kräver ytterligare praxis och föreskrifter för att klargöras.

Vid tillkomsten av nya lagen om elektronisk kommunikation (2022:482) valde lagstiftaren att inte koppla sanktionsavgifter till lagringsskyldigheten och det finns inget som visar att de nu föreslagna reglerna gör skyldigheten tydligare och enklare att efterleva. Tvärtom blir skyldigheten nu ännu svårare att tolka och det kommer att krävas detaljerad vägledning för att bringa klarhet i de olika lagringsfallen och uppgiftskategorierna.

Sanktioner är inte heller motiverade utifrån tidigare erfarenheter av tillämpning av de existerande skyldigheterna för telekomoperatörer. De lagringsskyldiga operatörerna har gjort stora ansträngningar för att på ett effektivt sätt bistå de brottsutredande myndigheterna med lagrade uppgifter. Då skyldigheten nu blir än mer komplex och svår att efterleva är det direkt olämpligt att förena den med hot om sanktionsavgift. Det finns därtill en inte obetydlig risk att den fortsatta generella och mycket omfattande lagringen för brottsutredning underkänns vid en prövning av EU-domstolen, vilket ytterligare styrker uppfattningen att sanktionsavgifter är olämpliga. Inom ramen för tillsyn kan PTS ge vägledning och ställa upp konkreta krav förenat med hot om vite, vilket måste ses som fullt tillräckligt i de sällsynta fall det kan finnas misstanke om att en lagringsskyldig inte gör helt rätt.

Om en sanktionsmöjlighet ändå införs bör det vara tydligt att den inte är tillämplig för lagringsskyldiga som på ett seriöst sätt tillämpas regelverket men haft ursäktliga brister, t.ex. grundade på tolkningen av otydligheter i definitioner och kravställning. Sanktionsavgifter bör vara reserverad för uppsåtliga eller grovt oaktsamma beteenden eller för situationer där den lagringsskyldige inte medverkar vid tillsyn eller inte hörsammat tillsynsmyndighetens tydliga anvisningar.

Det ska i sammanhanget anmärkas att det krävs tid och resurser för att anpassa operatörernas system till de nya lagringskraven. Det tar normalt 18 månader för Telenor att kravställa, utveckla, testa och implementera nya it-system. Det råder höga krav på säkerhet för dessa lagringssystem, så det är inte lämpligt att forcera införandet med korta deadlines och sanktionshot. Utkastets målsättning med ett införande av skyldigheterna redan den 1 mars 2026 är inte realistiskt.

### *Ersättning*

Finansieringen av förslaget och verksamhetsutövarnas rätt till ersättning behöver utredas och omprövas. I dag får verksamhetsutövarna bara ersättning för kostnader som uppstår då uppgifter lämnas ut. Förslaget innebär att stora investeringar i system och processer för lagring måste göras ännu en gång och att kostnaderna för lagring och verkställighet kommer att öka avsevärt. Då det rör sig om olika uppgiftskategorier och

lagringstider för nationell säkerhetslagring jämfört med lagring för brottsutredning kommer systemen för lagring bli mer komplexa och ställa krav på en enorm utökning av lagringskapacitet.

Skydd för nationell säkerhet och brottsbekämpning är statliga angelägenheter. Kostnader som uppstår i sådan verksamhet bör som utgångspunkt finansieras av det allmänna. Att som nu är fallet de rättsliga kraven ändras flera gånger innebär att befintliga system skrotas eller måste byggas om i grunden. Vi har nu nått en gräns för hur ofta kraven kan ändras utan att staten går in och finansierar de nödvändiga investeringarna. En statlig finansiering skulle också möjliggöra en kravställning som både garanterar funktionalitet och skapar möjligheter för effektivitet baserat på stordriftsfördelar för de aktörer som upphandlar denna typ av system. Statlig finansiering för nödvändiga investeringar i datalagring är huvudregel i många andra EU-länder och det är rimligt att så också blir fallet för Sverige.

Därtill krävs en översyn av den ersättning som lämnas för själva utlämningen av uppgifter. Vad gäller nationell säkerhetslagring så kommer den generera väldigt stora lagringsvolymmer när den är aktiv och samtidigt kan antalet verkställigheter förväntas bli lågt, då utredning och underrättelseverksamhet med bäring på Sveriges säkerhet mer sällan kan förväntas leda till utlämning av lagrade uppgifter. Att vidhålla dagens modell för ersättning kommer därför inte att vara hållbart för de lagringsskyldiga. I stället krävs en ersättning som reflekterar de faktiska kostnader som verkställigheten driver med hänsyn till hur kraven är utformade.

Regeringen anför på s. 107 i utkastet att *"även om regleringen i sig innebär att företagen behöver ha beredskap för lagringen oaktat om en sådan beslutat är förhoppningen att en sådan lagringsskyldighet inte kommer att vara vanligt förekommande och att det, sett över tid, rör sig om en hanterbar kostnad"*. Uttalandet är märkligt. Det förefaller som att regeringen tror att lagringen driver mindre kostnader om beslut om nationell säkerhetslagring inte blir så vanligt förekommande. Det är naturligtvis inte korrekt. De lagringsskyldiga måste investera i system, lagringskapacitet och ha tillräckliga personalresurser redo även om sådana beslut inte är vanligt förekommande. Om staten däremot bidrar till kostnaderna för de nödvändiga lagringssystemen så stämmer det däremot att de totala kostnaderna kan bli hanterbara.

## Övrigt

Telenor står till regeringens förfogande om det finns behov av ytterligare upplysningar. Telenor åberopar inte sekretess för någon uppgift i detta remissvar.

Telenor Sverige AB

Martin Sjöberg  
Bolagsjurist