Tele2 Sverige AB
Box 62
164 40 Kista
Telephone +46 8 562 640 00
Fax: +46 8 562 642 00
www.tele2.se

27-05-2024, FINAL

Försvarsdepartementet
Rättssekretariatet
103 33 Stockholm

Insänt via e-post till följande adresser:
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Yttrande över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Tele2 Sverige AB (”Tele2”) har tagit del av delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18), som Försvarsdepartementet remitterade den 6 mars 2024, med dnr. Fö2024/00496 (”Utredningen”). Tele2 får härmed inkomma med följande yttrande.

1. Tillämplighet

Utredningen konstaterar i avsnitt 5.2.2 att den juridiska eller fysiska personens verksamhet ska omfattas *i dess helhet* av lagens krav. Härvid anför Utredningen att det saknas en uttrycklig begränsning om att endast delar av den fysiska eller juridiska personens verksamhet skulle omfattas av NIS2-direktivet, och att det skulle kunna leda till gränsdragningsproblem om försök att dela upp verksamheten skulle göras.

Tele2 noterar härvidlag att Utredningen inte tillräckligt har analyserat huruvida EU-lagstiftaren kan antas vilja säkerställa ett adekvat och enhetligt cybersäkerhetsskydd av nätverks- och informationssystem som *används för viss verksamhet* hos de juridiska eller fysiska personer som pekas ut, eller om EU-lagstiftaren verkligen vill se identiskt skydd av *alla* nätverks- och informationssystem som används av utpekade juridiska eller fysiska personer, alldeles oavsett verksamhet.

I detta sammanhang uppmärksammar Tele2 att det redan i beaktandesats 1 i NIS2-direktivet framkommer att de sedan tidigare gällande cybersäkerhetsreglerna syftade till att ”begränsa hoten mot nätverks- och informationssystem ***som används för att tillhanda-hålla samhällsviktiga tjänster i centrala sektorer*** och säkerställa kontinuiteten i sådana tjänster (…)” (Tele2s kursivering).

I beaktandesats 6 i NIS2-direktivet uppmärksammas vidare att NIS2-direktivet ska säkerställa att ”tillämpningsområdet ***med avseende på olika sektorer*** [ska] ***utvidgas*** till en större del av ekonomin så att den ger omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden” (Tele2s kursivering).

Enligt Tele2 visar ovan nämna beaktandesatser att EU-lagstiftaren vill säkerställa ett adekvat och inom EU enhetligt cybersäkerhetsskydd av nätverks- och informationssystem *som* ***används vid tillhandahållandet av vissa tjänster och/eller bedrivandet av viss verksamhet***. Det är ***inte alla*** nätverks- och informationssystem ***inom alla*** sektorer som ska skyddas, och inte heller ***alla*** nätverks- och informationssystem inom utpekade sektorer, utan det är ***specifikt de nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer som ska skyddas***.

Den utvidgning som NIS2-direktivet ska innebära avser, vilket framkommer uttryckligen av beaktandesats 6 i NIS2-direktvet, ***antalet sektorer***.

Tele2 Sverige AB
Box 62
164 40 Kista
Telephone +46 8 562 640 00
Fax: +46 8 562 642 00
www.tele2.se

Det finns ingenting som antyder att tillämpligheten ska öka med avseende på antalet nätverks- och informationssystem inom en viss sektor, eller med avseende på antalet nätverks- och informationssystem som en tillhandahållare inom en viss sektor använder. I detta sammanhang gäller snarare den ***tydliga avgränsning som kommer till uttryck i beaktandesats 1 i NIS2-direktivet***.

Härvidlag drar Tele2 slutsatsen att Utredningen redan i första beaktandesatsen i NIS2-direktivet ges både skäl och möjlighet att avgränsa tillämpligheten av lagens krav till just de nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer, istället för att gälla alla de nätverks- och informationssystem som används av en verksamhetsutövare inom en utpekad sektor.

Ytterligare skäl och möjlighet till en sådan avgränsning ges, då specifikt i fråga om lagens tillämplighet inom sektorn digital infrastruktur, i beaktandesats 92 i NIS2-direktivet. Där framgår att syftet med att låta tillhandahållare av allmänna elektroniska kommunikationsnät och/eller av allmänt tillgängliga elektroniska kommunikationstjänster omfattas av reglerna i NIS2-direktvet är att ”rationalisera” de skyldigheter som åläggs samt att göra det möjligt för företag och myndigheter inom dessa verksamheter att ”dra nytta av den rättsliga ram som inrättas" genom NIS2-direktivet. Av denna anledning ska ”de motsvarande bestämmelser som anges i förordning (EU) nr 910/2014 och i direktiv (EU) 2018/1972 och som gäller införande av säkerhets- och anmälningskrav för dessa typer av entiteter” enligt NIS2-direktivet utgå.

Syftet med NIS2-direktivet är således ***inte att utvidga tillämpligheten*** av de ”motsvarande bestämmelser” om ”säkerhets- och anmälningskrav” som finns i direktiv (EU) 2018/1972.

De ”motsvarande bestämmelser” om ”säkerhets- och anmälningskrav” som NIS2-direktivet i detta sammanhang hänvisar till finns i artikel 40 i direktiv (EU) 2018/1972 (i det följande kallad ”Kodexen”), som i Sverige har genomförts i lag (2022:482) om elektronisk kommunikation (”LEK”). Enligt artikel 40.1 Kodexen ska medlemsstaterna ”säkerställa att tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera ***risker som hotar näts och tjänsters säkerhet***.”

Enligt artikel 40.2 Kodexen ska medlemsstaterna ”säkerställa att tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster utan onödigt dröjsmål meddelar den behöriga myndigheten om säkerhetsincidenter som har haft en ***betydande påverkan på driften av nät och tjänster***.”

Definitionen av begreppet ”säkerhet i nät och tjänster” enligt artikel 2.21 Kodexen är ”***elektroniska kommunikationsnäts och kommunikationstjänsters*** förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten ***hos dessa nät och tjänster***, hos lagrade eller överförda eller behandlade uppgifter eller hos de närliggande tjänster som ***erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller kommunikations-tjänster***.”

Nämnda bestämmelser i artikel 40.1, 40.2 och 2.21 Kodexen innebär att Kodexens ”säkerhets- och anmälningskrav” ***avser de nätverks- och informationssystem som används för att tillhandahålla elektroniska kommunikationsnät och elektroniska kommunikationstjänster***.

Tele2 Sverige AB
Box 62
164 40 Kista
Telephone +46 8 562 640 00
Fax: +46 8 562 642 00
www.tele2.se

Eftersom NIS2-direktivet, enligt beaktandesats 92 i NIS2-direktivet, inte syftar till att utvidga tillämpligheten av Kodexens säkerhets- och anmälningsbestämmelser utan endast till att ”rationalisera” de skyldigheter som åläggs samt att göra det möjligt för företag och myndigheter inom elektroniska kommunikationer att ”dra nytta av den rättsliga ram som inrättas" genom NIS2-direktivet, måste slutsatsen dras att ***NIS2-direktivets säkerhets- och anmälningsbestämmelser – liksom de säkerhets- och anmälningsbestämmelser som tidigare gällt enligt Kodexen och som i enlighet med NIS2-direktivet flyttas över till detta direktiv – också ska gälla för de nätverks- och informationssystem som används för att tillhandahålla elektroniska kommunikationsnät och elektroniska kommunikationstjänster***. Utredningen själv uppmärksammar dessutom att EU-lagstiftaren i beaktandesats 95 i NIS2-direktivet framhåller ”***vikten av att upprätthålla nuvarande praxis när det gäller elektronisk kommunikation***”.

Något stöd för Utredningens förslag att cybersäkerhetslagens krav ska omfatta den juridiska eller fysiska personens verksamhet i dess helhet – d.v.s. i princip alla nätverks- och informationssystem som utpekade juridiska eller fysiska personer använder alldeles oavsett i vilken del av verksamheten som dessa nätverks- och informationssystem används – saknas således i fråga om tillhandahållare av elektroniska kommunikationsnät och/eller tillhandahållare av elektroniska kommunikationstjänster.

Mot bakgrund av det ovanstående **avstyrker** Tele2 Utredningens förslag om att cybersäkerhetslagens krav ska omfatta den juridiska eller fysiska personens verksamhet i dess helhet. Tele2 **föreslår** att cybersäkerhetslagens krav ska, åtminstone i fråga om tillhandahållare av elektroniska kommunikationsnät och/eller tillhandahållare av elektroniska kommunikationstjänster, omfatta nätverks- och informationssystem som används för att tillhandahålla elektroniska kommunikationsnät och elektroniska kommunikationstjänster.

2. Tillsynsansvar och föreskriftsrätt

I avsnitt 8.4.2 föreslår Utredningen att Post- och telestyrelsen (”PTS”) ska vara tillsynsmyndighet för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster och sektorn rymden.

I avsnitt 8.4.5 anför Utredningen vidare att det är tillsynsmyndigheterna som har kunskap om eventuella sektorsspecifika förutsättningar som behöver beaktas i föreskrifter om riskhanteringsåtgärder och att det finns fördelar med att så långt möjligt hålla samman normgivning och tillsyn. Utredningen anför vidare att rätten att meddela föreskrifter om systematiskt informationssäkerhetsarbete bör hållas ihop med rätten att meddela föreskrifter om riskhanteringsåtgärder. Utredningen föreslår därför att det ska vara tillsynsmyndigheterna som får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning om riskhanteringsåtgärder inom sitt tillsynsområde. Utredningen uppmärksammar också särskilt att EU-lagstiftaren i beaktandesats 95 i NIS2-direktivet framhåller ”vikten av att upprätthålla nuvarande praxis när det gäller elektronisk kommunikation”.

Tele2 **tillstyrker** Utredningens föreslag i dessa delar.

3. Sanktionsmöjlighet snarare än sanktionsskyldighet

I avsnitt 9.6.1 noterar Utredningen att systemet med obligatorisk sanktionsavgift i den nu gällande NIS-lagen skulle kunna överföras till den nya cybersäkerhetslagen, men att det då skulle behöva införas begränsningar kring vilka överträdelser som ska kunna leda till sanktionsavgift.

Tele2 Sverige AB
Box 62
164 40 Kista
Telephone +46 8 562 640 00
Fax: +46 8 562 642 00
www.tele2.se

Utredningen argumenterar istället för att tillsynsmyndigheten förvisso ska kunna ta ut sanktionsavgifter vid samtliga typer av överträdelser av lagen, men att den ***inte ska vara skyldig att meddela sanktionsavgifter***. Istället får tillsynsmyndigheten enligt Utredningen avgöra i varje enskilt fall om förutsättningarna för att ta ut sanktionsavgift är uppfyllda. Utredningen föreslår därför att sanktionsavgift ***får tas ut*** av en verksamhetsutövare som har åsidosatt sina skyldigheter enligt cybersäkerhetslagens bestämmelser om att utse företrädare, anmälningsplikt, riskhanteringsåtgärder, utbildning och incidentrapportering eller enligt föreskrifter som meddelats med stöd av dessa bestämmelser.

Tele2 **tillstyrker** Utredningens förslag i denna del.

4. **Behov av att undvika konkurrenssnedvridning**
I avsnitt 5.3.2 konstaterar Utredningen att tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster enligt artikel 26.1 a i NIS2-direktivet ska omfattas av jurisdiktionen i det land de tillhandahåller sina tjänster. Enligt Utredningen betyder detta att en sådan verksamhetsutövare ska omfattas av den svenska cybersäkerhetslagen om verksamhetsutövarens tjänster tillhandahålls i Sverige.

Tele2 noterar härvidlag att risk för konkurrenssnedvridning skulle uppstå om inte alla tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i Sverige omfattades av samma cybersäkerhetsregler.

Tele2 **tillstyrker** därför Utredningens förslag i denna del.

5. **Behov av begreppsförtydliganden**
Tele2 uppmärksammar att flera helt centrala begrepp lämnas odefinierade i Utredningen. I huvudsak berör detta följande begrepp:

- ”*Personalsäkerhet*” och ”*säkrade lösningar för kommunikation*”: I avsnitt 7.1.2 beskriver Utredningen nio obligatoriska tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder som utpekade verksamhetsutövare ska vidta för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Flera av begreppen analyseras och konkretiseras av Utredningen. Begreppen ”personalsäkerhet” och ”säkrade lösningar för kommunikation” analyseras eller konkretiseras emellertid inte alls. Det är därmed oklart vad Utredningen avser med dessa begrepp.

- ”*Utbildning om riskhanteringsåtgärder*”: I avsnitt 7.2 föreslår Utredningen att ledningen i enskilda verksamheter (vilket i Utredningen preciseras som verkställande direktör samt styrelse) ska genomgå utbildning om riskhanteringsåtgärder. Utredningen noterar att detta krav övergripande ska framgå av lag, men att den närmare utformningen av krav på utbildning ska följa av föreskrifter. Det beror enligt Utredningen på att utbildningen behöver sektorsanpassas och även anpassas till olika målgrupper. Tele2 noterar härvidlag att ytterligare precisering bör kunna framgå direkt av lag eller av förarbetena till lagen. Exempelvis bör det redan i lag och/eller förarbete framgå vad syftet med utbildningen ska vara och om utbildningen ska vara på övergripande eller detaljerad nivå.

- ”*Särskilda skäl*” i fråga om säkerhetsrevisioner: I avsnitt 8.4.6 föreslår Utredningen att tillsynsmyndigheten, om det finns särskilda skäl, får ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

Tele2 Sverige AB
Box 62
164 40 Kista
Telephone +46 8 562 640 00
Fax: +46 8 562 642 00
www.tele2.se

Utredningen noterar att en liknande bestämmelse redan finns i 8 kap. 2 § LEK, enligt vilken tillsynsmyndigheten, om det finns särskilda skäl, får ålägga den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning av hela eller delar av verksamheten och att redovisa resultatet av granskningen för myndigheten. Tele2 uppmärksammar att en sådan åtgärd, som är mycket ingripande, enligt Utredningens förslag endast ska få vidtas ”om det finns särskilda skäl”. Någon vägledning om vilka skäl som ska kunna anses som särskilda ges emellertid inte alls i Utredningen. Det är därmed mycket svårt, hart när omöjligt, för båda verksamhetsutövare och tillsynsmyndigheter att bedöma när denna åtgärd skulle kunna bli aktuell.

Mot bakgrund av det ovanstående **föreslår** Tele2 att begreppen ”*personalsäkerhet*” och ”*säkrade lösningar för kommunikation*” (i fråga om riskhanteringsåtgärder), ”*utbildning om riskhanteringsåtgärder*” och ”*särskilda skäl*” (i fråga om säkerhetsrevisioner) ska konkretiseras och preciseras närmare i lag eller i förarbete till lag.

6. Anslagsfinansierad tillsyn

I avsnitt 12.6.7 föreslår Utredningen att kostnaderna för myndigheternas tillsyn inte ska avgiftsfinansieras utan anslagsfinansieras.

Tele2 **tillstyrker** Utredningens förslag i denna del.

*** * ***

Kontaktperson på Tele2
Carl-Johan Rydén
Regleringschef