kahn pedersen

Försvarsdepartementet
Rättssekretariatet

Endast per e-post:
fo.remissvar@regeringskansliet.se

Kopia till:
visnja.raguz@regeringskansliet.se

REMISSYTTRANDE ÖVER DELBETÄNKANDET NYA REGLER OM CYBERSÄKERHET, SOU 2024:18, FÖ2024/00496

1. INLEDNING

1.1 Advokatfirman Kahn Pedersen får härmed inkomma med remissyttrande över delbetänkandet Nya regler om cybersäkerhet, SOU 2024:18 (nedan "**Utredningen**"), avseende implementeringen av Europaparlamentets och rådets direktiv (EU) 2022/2555 ("**NIS 2-direktivet**").

1.2 Remissyttrandet inleds med allmänna synpunkter på författningsförslaget. Därefter behandlas vissa av Utredningens slutsatser som har betydelse för den framtida cybersäkerhetslagens tillämpning, men som saknar tillhörande bestämmelser i lagen. Slutligen behandlas anmärkningar på författningsförslaget som sådant.

2. SAMMANFATTNING

2.1 Advokatfirman Kahn Pedersen delar i stort de bedömningar som Utredningen gjort.

2.2 Advokatfirman Kahn Pedersen förordar att den föreslagna cybersäkerhetslagen genomförs, dock med beaktande av de förslag till ändringar med mera som behandlas nedan.

Advokatfirman Kahn Pedersen KB
Sveavägen 17
Box 16119
103 23 Stockholm

Tel: 08-121 50 220
E-post: info@kahnpedersen.se
Org.nr 969769-0775
Moms nr SE969769077501

3. ALLMÄNNA SYNPUNKTER

3.1 Advokatfirman Kahn Pedersen anser att den föreslagna lagens struktur samt vissa enskilda bestämmelsers lydelser är svårtillgängliga, vilket i förlängningen riskerar öka behovet av kompletterande föreskrifter och praxis på ett sätt som inte kan anses nödvändigt.

3.2 Som exempel kan nämnas den föreslagna bestämmelsen i 1 kap. 4 § avseende lagens tillämpningsområde. För att kunna göra bedömningen av om den egna verksamheten omfattas måste den enskilda läsaren dels gå in i bilagorna till NIS 2-direktivet, dels kontrollera om verksamheten inryms i bestämmelserna i 1 kap. 5-8 §§ och dels gå vidare in kommissionens rekommendation 2003/361/EG för att läsa sig till kravet på att utgöra ett medelstort företag. En sådan form av vidarehänvisning till olika lagar och bestämmelser kan inte anses tillgängligt.

3.3 Advokatfirman Kahn Pedersen förordar därför att lagens struktur med bland annat korsvisa referenser till annan lagstiftning ses över, samt i förekommande fall förenklas.

4. ANMÄRKNINGAR TILL VISSA AV UTREDNINGENS SLUTSATSER

4.1 Verksamhetsutövare (kapitel 5.2.2)

4.1.1 Advokatfirman Kahn Pedersen delar inte bedömningen att hela verksamheten behöver uppfylla cybersäkerhetslagens krav, om endast någon del av verksamheten omfattas. Utredningens förslag innebär en oproportionerlig överimplementering av NIS 2-direktivet, och saknar tydligt juridiskt stöd.

4.1.2 Enligt Advokatfirman Kahn Pedersen skulle en sådan tillämpning av NIS 2-direktivets bestämmelser leda till kraftigt ökade kostnader för de som berörs av den framtida cybersäkerhetslagen, på ett sätt som inte är motiverat.

4.1.3 Att det, som Utredningen nämner, i enskilda fall kan uppstå gränsdragningsproblem i förhållande till informationssystem som används i flera delar av en verksamhet är enligt Advokatfirman Kahn Pedersens mening inte i sig ett argument för att även övriga delar av verksamheten automatiskt ska omfattas av lagens krav.

4.1.4 Istället är det nödvändigtvis så att varje verksamhetsutövare som använder ett informationssystem inom ramen för flera delar av sin verksamhet behöver utreda om det innebär att systemet måste uppfylla cybersäkerhetslagens krav.

4.1.5 Utredningens argument förutsätter dessutom att sådana gränsdragningsproblem ofta uppkommer, vilket knappast kan anses vara utrett. På motsatt sätt kan det istället ofta anses vara så att de informationssystem i form av exempelvis styrsystem m.m. som används inom ramen för en verksamhet som producerar energi särskiljer sig både logiskt och rent fysiskt från andra former av informationssystem som används inom ramen för samma bolag, exempelvis i form av epostsystem.

4.1.6 Det kan i ett sådant sammanhang knappast anses rimligt att ett företag som ägnar sig åt flera typer av verksamheter måste säkerställa att logiskt och verksamhetsmässigt separerade system ska uppfylla kraven i cybersäkerhetslagen när det står klart att de inte används i sådan verksamhet som omfattas av lagens tillämpningsområde.

4.1.7 Det kan i detta avseende även noteras att Utredningen använder vad som anges i direktivets skäl 16 till stöd för sin bedömning. Detta skäl avser dock en helt annan situation, och utgör en undantagsregel från NIS 2-direktivets tillämpningsområde. Att använda denna till stöd för att kraftigt utöka tillämpningsområdet för cybersäkerhetslagen låter sig enligt Advokatfirman Kahn Pedersens mening inte göras.

4.1.8 Tvärtom finns det tungt vägande skäl i NIS 2-direktivet för att endast de delar av verksamheten som uttryckligen ingår i de verksamhetsområden som omfattas av den föreslagna cybersäkerhetslagen även bör omfattas av lagens skyldigheter. Detta oavsett om NIS 2-direktivet saknar en sådan uttrycklig begränsning eller inte (som Utredningen konstaterat).

4.1.9 I skäl 6 anges att NIS 2-direktivet syftar till att täcka de sektorer som är av ”*avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden*”. Om all den övriga verksamhet som bedrivs i ett bolag också omfattas av direktivets krav enbart på grund av att vissa delar gör det, skulle det innebära att NIS 2-direktivets fokus på särskilda verksamheter av avgörande betydelse försvinner.

4.1.10 Som teoretiskt exempel kan i detta fall nämnas ett stort företag inom tillverkningsindustrin som tillverkar leksaker. Sådan tillverkning omfattas uppenbarligen inte av NIS 2-direktivet, eftersom verksamheten på inget sätt kan anses vara av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden.

4.1.11 Detta företag har dock monterat ett mindre antal solpaneler på en av sina fastigheter. Bolaget kan därför i strikt mening anses utgöra en elproducent som omfattas av den framtida lagen.

4.1.12 Eftersom bolaget överskrider gränserna för att utgöra ett medelstort företag skulle förekomsten av ett mindre antal solpaneler medföra att bolagets samtliga informationssystem skulle omfattas av kraven i cybersäkerhetslagen, enbart genom att bolaget i en mycket liten utsträckning kan anses utgöra en elproducent.

4.1.13 Därmed skulle exempelvis även bolagets epostsystem, kundhanteringssystem och ordersystem för beställning av varor till de leksaker som produceras omfattas av cybersäkerhetslagens krav.

4.1.14 En sådan tillämpning kan knappast anses proportionerlig i förhållande till NIS 2-direktivets legitima mål och syften, utan går istället långt utöver vad som krävs för att uppnå dessa. Det kan därför ifrågasättas om en sådan tillämpning kan anses uppfylla grundläggande EU-rättsliga krav på proportionalitet (jfr EU-domstolens dom i de förenade målen C-293/12 och C-594/12, punkt 45).

4.1.15 Det kan i detta sammanhang även noteras att lagstiftaren i förarbetena till NIS-lagen gjort motsatt tolkning. Där anges följande vad gäller den lagens krav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete:

> *Till skillnad från utredningen anser regeringen dock att lagbestämmelsen bör utformas på så sätt att det tydligt framgår att kravet endast avser sådana nätverk och informationssystem som en leverantör använder för att tillhandahålla samhällsviktiga tjänster.* (Se prop. 2017/18:205, s. 39).

4.1.16 Enligt Advokatfirman Kahn Pedersen saknas det i sammanhanget anledning att i förhållande till den föreslagna cybersäkerhetslagen göra en annan tolkning än den lagstiftaren gjorde inom ramen för föregående lagstiftningsarbete.

4.1.17 I sammanhanget kan det särskilt noteras att NIS 1-direktivet inte är fundamentalt annorlunda strukturerat i aktuellt avseende jämfört med NIS 2-direktivet. Istället är även NIS 1-direktivet tillämpligt på leverantörer av samhällsviktiga/digitala tjänster vilka definieras som ”*offentlig eller privat enhet*” respektive ”*juridisk person*”. Det saknas enligt Advokatfirman Kahn Pedersens mening därmed hinder att göra samma tolkning som lagstiftaren tidigare gjort i denna fråga.

4.1.18 Advokatfirman Kahn Pedersen vill därutöver särskilt betona att Utredningens tolkning leder till uppenbara tolkningssvårigheter i förhållande till vissa av cybersäkerhetslagens bestämmelser.

4.1.19 Ett sådant exempel är den föreslagna bestämmelsen i 3 kap. 4 §, i vilken regleras vad som utgör en betydande incident. Av bestämmelsen framgår att en avgörande aspekt för bedömningen av vad som är en betydande incident bland annat är den skada som kan uppstå för den ”*erbjudna tjänsten*”. Vad som utgör den erbjudna tjänsten får anses relativt klart i förhållande till de sektorsmässiga verksamheter som uttryckligen omfattas av NIS 2-direktivets tillämpningsområde.

4.1.20 Om hela den verksamhet som en verksamhetsutövare bedriver skulle omfattas av cybersäkerhetslagen kan det däremot bli mycket svårt att klargöra vad som faktiskt utgör den ”*erbjudna tjänsten*”. Är det exempelvis all den externa verksamhet som bedrivs där det finns motparter i form av exempelvis kunder eller tjänstemottagare?

4.1.21 Detta skulle i sin tur leda till att betydligt fler incidentrapporter görs i förhållande till såväl tillsynsmyndigheter som tjänstemottagarna/kunderna, även avseende situationer som inte är direkt hänförliga till den verksamhet som primärt omfattas av cybersäkerhetslagens tillämpningsområde.

4.1.22 En sådan utveckling kan enligt Advokatfirman Kahn Pedersens mening knappast anses vara varken önskvärd eller leda till en ökad effektivitet avseende möjligheterna att bekämpa cyberhot riktade mot samhällets mest skyddsvärda tjänster.

4.1.23 På motsvarande sätt riskerar den aktuella tolkningen och tillämpningen att leda till att vissa begränsningar av regelverkets tillämpningsområde tappar sitt syfte.

4.1.24 Som exempel kan nämnas ett bolag som i begränsad utsträckning bedriver viss verksamhet i form av avfallshantering, genom att avfallet från den egna produktionen omhändertas. Sådana verksamheter är undantagna NIS 2-direktivets tillämpningsområde i de fall där avfallshanteringen inte utgör verksamhetsutövarens huvudsakliga näringsverksamhet, se bilagan 2 till NIS 2-direktivet, sektor 2.

4.1.25 I det aktuella exemplet utgör avfallsverksamheten inte bolagets huvudsakliga näringsverksamhet, och bolaget omfattas därmed inte heller av cybersäkerhetslagens bestämmelser. Bolaget bedriver däremot annan verksamhet som omfattas av cybersäkerhetslagens tillämpningsområde, i form av tillverkning av sådan elapparatur som omfattas av bilagan 2 till NIS 2-direktivet, sektor 5, delsektor C.

4.1.26 Om Utredningens förslag skulle genomföras innebär det att avfallsverksamheten därmed ändå omfattas av cybersäkerhetslagens bestämmelser, genom den övriga verksamheten som bedrivs i bolaget.

4.1.27 På motsvarande sätt skulle rimligen även de informationssystem som används av exempelvis kommunfullmäktige omfattas, även om kommunfullmäktige uttryckligen undantagits från lagens tillämpningsområde genom den föreslagna bestämmelsen i 1 kap. 3 §.

4.1.28 En sådan tillämpning kan knappast anses förenlig med NIS 2-direktivets syften och systematik, utan skulle istället leda till att bestämmelser som syftar till att begränsa tillämpningen av NIS 2-direktivet riskerar att bli helt utan verkan.

4.1.29 Vidare talar avgränsningsproblem gentemot säkerhetsskyddslagen för en mer nyanserad tillämpning. Enligt den föreslagna bestämmelsen i cybersäkerhetslagens 1 kap. 13 § ska kapitel 3 (riskhanteringsåtgärder och incidentrapportering) inte tillämpas på säkerhetskänslig verksamhet som bedrivs av en enskild verksamhetsutövare.

4.1.30 Det är dock inte ovanligt att en verksamhet som omfattas av NIS 2-direktivet också utgör säkerhetskänslig verksamhet på grund att det rör sig om nationellt samhällsviktig verksamhet.

4.1.31 Effekten av Utredningens bedömning kan alltså bli att ett bolag behöver tillämpa cybersäkerhetslagens centrala åligganden på all verksamhet utom den som faktiskt faller in under NIS 2-direktivets tillämpningsområde, eftersom säkerhetsskyddslagen ska tillämpas på just den delen av verksamheten.

4.1.32 Advokatfirman Kahn Pedersen förordar mot denna bakgrund att det tydligt anges i lag eller förarbeten att det endast är den del av verksamheten som uttryckligen omfattas av cybersäkerhetslagens uttalade tillämpningsområde som också omfattas av lagens krav.

4.2 Termen verksamhetsutövare

4.2.1 Advokatfirman Kahn Pedersen avstyrker att termen ”*verksamhetsutövare*” används för att definiera den som omfattas av cybersäkerhetslagens tillämpningsområde.

4.2.2 Anledningen till detta är att termen redan används för sådana verksamheter som bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. Eftersom cybersäkerhetslagen och säkerhetsskyddslagen i vissa fall har ett helt eller delvis överlappande tillämpningsområde i förhållande till samma typer av verksamheter vore det olyckligt om samma term användes för att definiera vilka som omfattas av respektive lag.

4.2.3 Advokatfirman Kahn Pedersen förordar därför att den mer neutrala och NIS 2-specifika termen ”*entitet*” används för att definiera de verksamheter som omfattas av cybersäkerhetslagen.

4.3 Små företag med det offentliga som ägare

4.3.1 Som Utredningen kunnat konstatera innehåller bestämmelsen i art. 2.1 andra stycket NIS 2-direktivet ett undantag från art. 3.4 i bilagan till kommissionens rekommendation 2003/361/EG.

4.3.2 Genom att detta undantag sker kan även bolag som ägs av det offentliga ingå i SMF-kategorin, och därmed undantas bestämmelserna i NIS 2-direktivet om de inte överstiger gränserna för att utgöra ett medelstort företag.

4.3.3 Bestämmelsen i art. 2.1 i NIS 2-direktivet utgör med andra ord en undantagsregel, som syftar till att begränsa tillämpningsområdet för NIS 2-direktivet till att enbart avse medelstora företag (och större), även om de ägs av det offentliga.

4.3.4 Det aktuella undantaget har dock inte sin motsvarighet i den föreslagna cybersäkerhetslagen. Det innebär, rent formellt sett, att undantaget inte föreslås implementeras i svensk rätt.

4.3.5 Detta skulle innebära att den undantagsregel som återfinns i art. 2.1 i NIS 2-direktivet inte blir tillämplig för svenska offentligt ägda företag.

4.3.6 En sådan reglering är förvisso inte rättsstridig, eftersom enskilda medlemsstater har möjligheter att anta strängare regler än de NIS 2-direktivet föreskriver, och då särskilt i förhållande till rent nationella företag.

4.3.7 Enligt Advokatfirman Kahn Pedersens mening innebär dock det faktum att det aktuella undantaget inte återfinns i den föreslagna lagen en indirekt överimplementering av NIS 2-direktiet.

4.3.8 Eftersom det rör sig om ett undantag från en annars bindande EU-rättslig akt så innebär det att motsvarande undantag enligt Advokatfirman Kahn Pedersens mening måste införlivas i lag för att kunna vara tillämpligt.

4.3.9 Advokatfirman Kahn Pedersen förordar därför att det tydliggörs i lag att bestämmelsen i art. 3.4 i kommissionens ovan nämnda rekommendation inte ska tillämpas vid bedömningen av om ett företag är medelstort, enligt cybersäkerhetslagen.

4.4 Säkerhet i leveranskedjan (avsnitt 7.1.2)

4.4.1 Advokatfirman Kahn Pedersen delar bedömningen att krav på åtgärder som rör säkerhet i leveranskedjan lämpligen enbart sträcker sig i ett led.

4.4.2 Advokatfirman Kahn Pedersen förordar dock att det tydligt klargörs om kravet på säkerhet i leveranskedjan enbart gäller framtida avtal som tecknas efter det att cybersäkerhetslagen träder ikraft, eller om bestämmelsen även är tillämplig för befintliga avtalsrelationer.

4.4.3 Enligt Advokatfirmans mening talar huvudprincipen om att civilrättslig lagstiftning inte ska ges retroaktiv verkan mot att även befintliga avtal omfattas av krav på säkerhet i leveranskedjan, se och jfr prop. 2020/21:194, s. 120.

4.4.4 Det kan dock inte uteslutas att en ändamålsenlig tolkning av NIS 2-direktivet innebär att även befintliga avtal omfattas av krav på säkerhet i leveranskedjan. Detta särskilt eftersom det skulle kunna uppstå uppenbara risker i enskilda verksamhetsutövares verksamhet om äldre avtal utan krav på cybersäkerhetsåtgärder lämnades utan åtgärd, enbart på grund av att de ingicks innan lagen trädde ikraft.

4.4.5 Advokatfirman Kahn Pedersen förordar därför att det tydliggörs i lagens övergångsbestämmelser om kraven på säkerhet i leveranskedjan även gäller för redan ingångna avtal.

4.5 Upphävande av auktorisation eller certifiering (avsnitt 9.5.5)

4.5.1 Advokatfirman Kahn Pedersen delar Utredningens bedömning att upphävandet av en verksamhetsutövares auktorisation eller certifiering kan innebära mycket långtgående konsekvenser för den enskilda verksamhetsutövaren. En sådan sanktion bör som regel inte komma ifråga annat än vid ytterst allvarliga överträdelser, eftersom den har likheter med bestämmelser om näringsförbud.

4.5.2 Advokatfirman Kahn Pedersen vill dock poängtera att en sådan effekt alltid uppstår som en följd av sanktioner av denna karaktär. De oöverblickbara konsekvenser som indragandet av en auktorisation eller en certifiering skulle kunna få kan därför knappast anses vara unikt ur ett svenskt perspektiv, vilket Utredningens bedömning kan anses implicera.

4.5.3 Att Sverige skulle ha möjlighet att inte implementera den föreslagna bestämmelsen kan enligt Advokatfirman Kahn Pedersen därför ifrågasättas, ur ett EU-rättsligt perspektiv.

4.5.4 Direktiv ger förvisso rätt till visst utrymme för skönsmässiga bedömningar i samband med medlemsstaternas implementering av desamma, förutsatt att direktivet fortfarande uppnår önskat resultat.

4.5.5 Advokatfirman Kahn Pedersen vill i detta sammanhang understryka att bestämmelsens uttryckliga och detaljerade innehåll i artikel 32.5 a i NIS 2-direktivet bör anses innebära ett mycket litet utrymme för en sådan nationell skönsmässig bedömning, oaktat bestämmelsens konsekvenser för enskilda verksamhetsutövare.

4.5.6 Advokatfirman Kahn Pedersen anser inte att Utredningens bedömning av att det är oklart vilka former av auktorisationer eller certifieringar som avses i bestämmelsen utgör ett giltigt argument för att inte implementera densamma i svensk rätt.

4.5.7 Advokatfirman Kahn Pedersen anser därför att det kan ifrågasättas om nuvarande förslag till implementering uppfyller de krav som uppställs för att säkerställa att behöriga myndigheter får tillgång till den form av befogenheter som NIS 2-direktivet föreskriver.

5. ANMÄRKNINGAR TILL FÖRFATTNINGSFÖRSLAGET

5.1 En ny cybersäkerhetslag

5.1.1 Advokatfirman Kahn Pedersen delar Utredningens bedömning att NIS 2-direktivets bestämmelser bör implementeras i en ny lag om cybersäkerhet. Advokatfirman Kahn Pedersen förordar dock att lagen får en något annorlunda namnsättning, så att det tydligt framgår att lagens bestämmelser enbart är tillämpliga för väsentliga och kritiska verksamhetsutövare.

5.1.2 Cybersäkerhet är ett brett begrepp, och behovet av cybersäkerhetsåtgärder finns inom i stort sett alla sorters verksamheter som på ett eller annat sätt använder sig av olika former av IT-system och andra tekniska lösningar.

5.1.3 För att det inte ska uppstå någon oklarhet i frågan om vem som omfattas av den framtida lagen förordar Advokatfirman Kahn Pedersen därför att det redan i lagens namn tydligt framgår att den enbart är tillämplig för väsentliga och kritiska verksamhetsutövare.

5.2 Definitionerna

5.2.1 I den föreslagna bestämmelsen i 1 kap. 2 § definieras vissa för lagen centrala begrepp. Därutöver används det i lagen definitioner som inte återspeglas i den föreslagna definitionslistan, och begrepp definieras även på övriga platser i lagen.

5.2.2 Advokatfirman Kahn Pedersen förordar att samtliga definitioner som används i lagen återfinns i lagens definitionslista.

5.2.3 Advokatfirman Kahn Pedersen förordar mot denna bakgrund att definitionen av vad som utgör en betydande incident enligt den föreslagna 3 kap. 4 § flyttas till lagens definitionslista.

5.2.4 Advokatfirman Kahn Pedersen förordar även att begreppet medelstort företag definieras i lagens definitionslista, istället för att löpande hänvisningar görs till kommissionens rekommendation 2003/361/EG (se den föreslagna 1 kap. 4 § p. 3 och 2 kap. 1 § pp. 1 och 3).

5.2.5 Advokatfirman Kahn Pedersen avstyrker att vissa definitioner sker genom hänvisning till annan EU-lagstiftning. Advokatfirman Kahn Pedersen ser stora fördelar med att definitionerna skrivs ut i sin helhet i lagen som sådan. Framförallt underlättar det för löpande hänvisningar, och gör lagstiftningens innehåll mer lättillgängligt.

5.2.6 Advokatfirman Kahn Pedersen avstyrker att begreppet ”*tillbud*” definieras i lagen, eftersom ordet i övrigt inte återfinns i lagen som sådan. Istället förekommer begreppet enbart i den föreslagna cybersäkerhetsförordningen. Advokatfirman förordar därför att begreppet istället definieras i den föreslagna cybersäkerhetsförordningen, där det också tillämpas.

5.2.7 Av den föreslagna bestämmelsen i 3 kap. 3 § följer att ledningen i ”*enskilda och offentliga verksamheter*” ska genomgå viss utbildning.

5.2.8 Eftersom cybersäkerhetslagen i övrigt utgår från termen ”*verksamhetsutövare*” förordar Advokatfirman Kahn Pedersen att samma terminologi även används i denna bestämmelse, i syfte att undvika onödig begreppsförvirring.

5.2.9 Advokatfirman förordar även att begreppet ”*ledning*” i den aktuella bestämmelsen definieras, så att det är tydligt vem som ska genomgå den aktuella utbildningen. Enligt Advokatfirman Kahn Pedersen mening så bör begreppet rimligtvis avse samma personkrets som kan bli föremål för sanktioner enligt den föreslagna bestämmelsen i 5 kap. 8 §.

5.2.10 På motsvarande sätt förordar Advokatfirman Kahn Pedersen att enhetlig terminologi används för väsentligen samma begrepp. Advokatfirman Kahn Pedersen kan i detta avseende notera att det enligt den föreslagna bestämmelsen i 3 kap. 6 § fjärde stycket återfinns en skyldighet att informera de ”*kunder*” som kan antas påverkas av en betydande incident. Denna term avviker dock från NIS 2-direktivet, där termen ”*mottagare av tjänster*” används, se art. 23.2.

5.2.11 Advokatfirman Kahn Pedersen förordar att termen ”*kunder*” byts ut mot termen *”mottagare”*, dels för att ge begreppet ett mer direktivkonformt uttryck, dels eftersom mottagare av en tjänst passar bättre i förhållande till exempelvis offentliga verksamhetsutövare, där det kan diskuteras om medborgarna som mottar tjänster utgör ”*kunder*”.

5.2.12 För att uppnå en enhetlig terminologi i detta avseende förordar Advokatfirman Kahn Pedersen att den föreslagna bestämmelsen i 5 kap. 7 § andra stycket ändras på så sätt att ordet ”*användare*” byts ut mot ”*mottagare*” alternativt ”*kunder*”. Syftet med en sådan ändring är att säkerställa att olika termer inte används för i princip samma sak, vilket kan leda till onödiga juridiska frågeställningar.

5.3 Undantagsregeln för företag som annars skulle anses som medelstora

5.3.1 Av den föreslagna bestämmelsen i 1 kap. 4 § andra stycket framgår att regeringen kan meddela undantag enligt den tidigare punkten 3 ”*avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet*”.

5.3.2 Bestämmelsen innehåller enligt Advokatfirman Kahn Pedersens mening en felsyftning, på så sätt att det bakomliggande undantaget i NIS 2-direktivet inte avser partnerföretag eller anknutna företag som inte själva uppfyller storlekskravet.

5.3.3 Bestämmelsen avser istället möjligheten att undanta enskilda verksamhetsutövare som inte själva uppfyller storlekskriteriet från tillämpningen av bestämmelserna om partner- och anknutna företag, förutsatt att vissa förutsättningar är uppfyllda. Det är med andra ord verksamhetsutövaren som ska understiga storlekskriteriet, och inte de eventuella anknutna företagen eller partnerföretagen.

5.3.4 Advokatfirman Kahn Pedersen förordar därför att bestämmelsen ändras, så att detta förhållande tydligt framgår av lagen.

5.4 Möjligheten att meddela föreskrifter

5.4.1 Av den föreslagna bestämmelsen i 1 kap. 8 § framgår att regeringen har rätt att meddela föreskrifter, men inte i vilket avseende detta får ske. Därmed skiljer sig bestämmelsen åt från liknande föreslagna bestämmelser (se exempelvis 1 kap. 4 § andra stycket), på ett sätt som i det närmaste synes vara en korrekturmiss.

5.4.2 Advokatfirman Kahn Pedersen förordar mot denna bakgrund att det tydligt anges i den aktuella paragrafen vilket slags föreskrifter som regeringen eller den myndighet regeringen bestämmer har befogenhet att meddela.

5.5 Väsentliga verksamhetsutövare

5.5.1 Av den föreslagna bestämmelsen i 2 kap. 1 § p. 2 framgår att verksamheter som bedriver verksamhet enligt bilagan 1 samt kommuner är att anse som väsentliga verksamhetsutövare, förutsatt att de även är att betrakta som medelstora.

5.5.2 Av bestämmelsen följer dock inte att regioner utgör väsentliga verksamhetsutövare. Därmed skulle regioner, till skillnad från statliga samt kommunala verksamhetsutövare, utgöra kritiska verksamheter.

5.5.3 Advokatfirman Kahn Pedersen kan inte se att det finns anledning till att regioner inte anges i den aktuella punkten, givet att både statliga myndigheter och kommuner gör det i sin egenskap av offentliga organ.

5.5.4 Advokatfirman Kahn Pedersen förordar därför att det tydligt anges att även regioner utgör väsentliga verksamhetsutövare.

5.5.5 På motsvarande sätt följer det av den föreslagna bestämmelsen i 2 kap. 1 § p. 3 att verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster utgör väsentliga verksamhetsutövare förutsatt att de uppfyller kravet på att utgöra medelstora företag.

5.5.6 Eftersom sådana verksamheter återfinns i bilagan 1 till NIS 2-direktivet så omfattas de redan av den föreslagna punkten 2, i nämnda bestämmelse.

5.5.7 Advokatfirman Kahn Pedersen förordar därför att 2 kap. 1 § p. 3 stryks, alternativt att det klargörs vilken skillnad som finns mellan de aktuella punkterna och deras inbördes tillämpning.

5.6 Incidentrapportering

5.6.1 Av den föreslagna bestämmelsen i 3 kap. 6 § första stycket följer att en ”*tidigare varning enligt 5 § ska uppdateras*”. Det följer dock inte i vilken mån detta ske, eller i vilket avseende den tidigare varningen ska uppdateras.

5.6.2 Advokatfirman Kahn Pedersen förordar att en mer direktivkonform skrivning ersätter den föreslagna på så sätt att bestämmelsen, i likhet med art. 23.4.b) i NIS 2-direktivet, utformas på så sätt att det anges att ”*Dessutom ska den tidigare information som lämnats inom ramen för en varning enligt 5 § även uppdateras vid behov*”

När ska mottagarrapportering ske?

5.6.3 Enligt art. 23 i NIS 2-direktivet ska en verksamhetsutövare rapportera om betydande incidenter till mottagarna av dess tjänster, förutsatt att det dels är lämpligt, dels att incidenten sannolikt inverkar negativt på tillhandahållandet av tjänsten.

5.6.4 På motsvarande sätt ska mottagarna av tjänsterna underrättas om ett betydande cyberhot som sådant, när så är lämpligt. Mottagarna ska även underrättas om vilka åtgärder som de kan vidta som svar på ett betydande cyberhot.

5.6.5 I jämförelse med den myndighetsrapportering som ska ske så fort en betydande incident har uppstått, så krävs det enligt NIS 2-direktivet alltså något ytterligare för att även mottagare ska underrättas om betydande incidenter respektive cyberhot.

5.6.6 Något sådan avgränsning görs dock inte i Utredningens förslag till 3 kap. 6 § fjärde stycket. Av denna följer istället att en verksamhetsutövare ska rapportera till mottagarna av tjänsterna när en betydande incident inträffat eller ett betydande cyberhot uppstått.

5.6.7 Enligt Advokatfirman Kahn Pedersens mening utgör ett sådant krav en uppenbar överimplementering av NIS 2-direktivets krav. Advokatfirman Kahn Pedersen kan inte heller utläsa varför Utredningen valt en sådan väg.

5.6.8 För att undvika att verksamhetsutövare måste rapportera om betydande incidenter och cyberhot även i de fall där det inte är lämpligt förordar Advokatfirman Kahn Pedersen att den föreslagna bestämmelsen ändras, och får ett mer direktivkonformt innehåll.

Vem är mottagare?

5.6.9 Varken begreppet *mottagare* eller *tjänstemottagare* definieras i NIS 2-direktivet, vilket gör det svårt att avgöra vem som omfattas av begreppet. Det saknas dessutom vägledning om hur begreppen ska tolkas i både skälen och artikel 23 i NIS 2-direktivet.

5.6.10 Vem som är mottagare av en särskild tjänst behöver enligt Advokatfirman Kahn Pedersens mening bedömas i det enskilda fallet och beror på typen av tjänst.

5.6.11 För en tillhandahållare av exempelvis ett system för datakommunikation lär det vara förhållandevis enkelt att avgöra vem som är mottagare av tjänsten, nämligen de enskilda användarna som nyttjar den.

5.6.12 I en sådan situation är det även logiskt att dessa användare skulle ha nytta av att bli underrättade om en betydande incident eller ett cyberhot eftersom de kan vidta åtgärder för att minska påverkan av den eventuella skadan.

5.6.13 För andra typer av tjänster, så som livsmedels- eller läkemedelsförsörjningen där det kan finnas flera olika led i leverantörskedjan, eller kedjan av potentiella mottagare, är det inte lika tydligt vem som är mottagare.

5.6.14 För livsmedel kan det tänkas vara respektive grossist som mottar varorna i första hand från producenten, men det kan även vara de olika återförsäljarna eller i sista hand de enskilda kunderna som är mottagare av tjänsten. Det går enligt Advokatfirman Kahn Pedersens mening nämligen att argumentera för att mottagaren av en tjänst rimligtvis är den som faktiskt konsumerar tjänsten som sådan, och inte den aktör som utgör ett av flera led i ett återförsäljarled.

5.6.15 Vid bedömningen av vem som utgör tjänstemottagare bör enligt Advokatfirman Kahn Pedersens mening dock hänsyn tas till verksamhetsutövarnas faktiska möjlighet att uppfylla den aktuella rapporteringsskyldigheten.

5.6.16 För att verksamhetsutövare ska kunna ha en praktisk möjlighet att mottagarrapportera bör det därför rimligtvis kunna krävas att denne har någon typ av relation till eller i vart fall vetskap om vem mottagaren är.

5.6.17 Advokatfirman Kahn Pedersens förordar därför att det tydliggörs att skyldigheten att rapportera till mottagarna av tjänsten begränsas till sådana direkta mottagare som verksamhetsutövaren känner, eller rimligtvis bör känna, till.

5.7 Utförande av säkerhetsrevisioner

5.7.1 Advokatfirman Kahn Pedersen tillstyrker den föreslagna bestämmelsen i 4 kap. 8 § om att det bör finnas särskilda skäl för att en tillsynsmyndighet ska kunna ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision.

5.7.2 Enligt Advokatfirman Kahn Pedersens mening får det anses främmande för svensk förvaltningsmodell att på detta sätt i det närmaste överlåta tillsynsmyndighetens ansvar på ett utomstående organ.

5.7.3 Advokatfirman Kahn Pedersen förordar dock att det i sammanhanget anges vad som ska anses utgöra sådana skäl som kan motivera att ett oberoende organ utför en riktad revision.

5.7.4 Advokatfirman Kahn Pedersen förordar därtill att det särskilt föreskrivs tydliga och effektiva sätt för ett tillsynsobjekt att begränsa sådana revisioner till att enbart avse den del av verksamheten som är absolut nödvändig att granska. Annars är risken att den utomstående parten gör mer omfattande revisioner än vad som kan anses vara motiverat i det enskilda fallet, givet att kostnaden för den ska tas av den enskilda verksamhetsutövaren.

5.7.5 Advokatfirman Kahn Pedersen förordar därför att det i lag eller annan författning tydligt regleras att tillsynsmyndigheten på ett detaljerat sätt måste ange både villkoren för och omfattningen av en säkerhetsrevision, om den ska utföras av ett utomstående organ.

5.8 Möjligheten att meddela förelägganden

5.8.1 Av den föreslagna bestämmelsen i 5 kap. 6 § har tillsynsmyndigheten möjligheten att meddela förelägganden. Av 7 § samma kapitel följer att sådana förelägganden bland annat får avse möjligheterna att offentliggöra information, samt att informera mottagarna av tjänsterna.

5.8.2 Advokatfirman Kahn Pedersen ställer sig tvekande till behovet av att i lag uttryckligen ange vilka slags förelägganden som tillsynsmyndigheterna kan meddela. Detta behov framstår i nuvarande fall dessutom som överflödigt eftersom den allmänna bestämmelsen om möjligheterna att meddela förelägganden i 5 kap. 6 § rymmer även de situationer som därefter särregleras i 7 §.

5.8.3 Advokatfirman Kahn Pedersen förordar därför att den föreslagna bestämmelsen i 5 kap. 7 § stryks i sin helhet, och att det av förarbetena till lagen istället nämns vilka slags förelägganden som kan bli aktuella att meddela vid olika slags överträdelser.

5.9 Förbudet mot att utöva ledningsfunktion

5.9.1 Advokatfirman Kahn Pedersen tillstyrker den föreslagna bestämmelsen i 5 kap. 8 § om att införa möjligheten att meddela förbud om att utöva ledningsfunktion, och förslaget om att den personkategori som kan omfattas av denna form av förbud kopplas till bestämmelserna i lagen om näringsförbud.

5.9.2 Enligt Utredningens förslag ska dock ett beslut om förbud kunna meddelas i de fall när den överträdelse som det bakomliggande föreläggandet avser är allvarlig. Även om det inte uttryckligen framgår av lagtexten som sådan så bör frågan om en överträdelse är allvarlig rimligen bedömas utifrån vad som enligt lagen ska anses utgöra en sådan.

5.9.3 Enligt den föreslagna bestämmelsen i 6 kap. 5 § är en överträdelse allvarlig om verksamhetsutövaren exempelvis inte har följt ett föreläggande från tillsynsmyndigheten (jfr Utredningens avsnitt 9.4.2).

5.9.4 Eftersom ett förbud mot att utöva ledningsfunktion enbart ska kunna komma ifråga om ett föreläggande inte följts, innebär det rimligen att en sådan överträdelse alltid är allvarlig.

5.9.5 Enligt Advokatfirman Kahn Pedersens mening innebär en sådan ordning att kravet på överträdelsens allvarlighet riskerar att förlora sin betydelse. Advokatfirman Kahn Pedersen förordar därför att det tydliggörs vad som ska betraktas som en allvarlig överträdelse i situationer som rör förbud att utöva ledningsfunktion.

5.9.6 Advokatfirman Kahn Pedersen delar därutöver Utredningens bedömning om att det får anses synnerligen ovanligt att denna typ av sanktion behöver tillgripas av en tillsynsmyndighet. Denna omständighet bör dock särskilt förtydligas i förarbetena till lagen.

5.10 Sanktionsavgifter

5.10.1 Advokatfirman Kahn Pedersen delar Utredningens bedömning att tillsynsmyndigheten ska ha möjlighet att besluta om att en sanktionsavgift ska tas ut.

5.10.2 På grund av sanktionsavgifters straffrättsliga karaktär, förordar Advokatfirman Kahn Pedersen dock att det bör tydliggöras att det är tillsynsmyndigheten som har bevisbördan dels för att en överträdelse har skett och dels i förhållande till dess allvar och övriga omständigheter som ska beaktas i fråga om sanktionsavgiftens storlek.

5.10.3 Givet de mycket höga belopp som sanktionsavgifterna kan komma att uppgå till förordar Advokatfirman Kahn Pedersen att det dessutom lagregleras vilket beviskrav som tillsynsmyndigheterna ska nå upp till för att en sanktionsavgift ska kunna tas ut.

5.10.4 Advokatfirman Kahn Pedersen förordar därutöver att det tydliggörs att sanktionsavgifter i den övre halvan av det föreslagna beloppsintervallet endast bör komma i fråga för mycket allvarliga överträdelser.