Vår referens: Diarienummer 20-3324

Sammanställning och analys av inkomna remissvar avseende PTS förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster

1. Inledning

Post- och telestyrelsen (PTS) har den 2 mars 2022 skickat ut ett förslag till nya föreskrifter och allmänna råd om säkerhet i nät och tjänster. Remisstiden gick ut den 1 april 2022.

Nedan sammanställs de huvudsakliga synpunkter som framförts i inkomna remissvar, tillsammans med PTS inställning till remissinstansernas synpunkter.

2. Inkomna remissvar

PTS har tagit emot remissvar från 28 remissinstanser.

Följande företag, myndigheter organisationer har lämnat synpunkter på PTS förslag till nya säkerhetsföreskrifter:

1. Allente Sverige AB
2. GlobalConnect
3. Hi3G Access AB (Tre)
4. Kommerskollegium

Post- och telestyrelsen
Postadress: Box 6101
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

5. Myndigheten för samhällsskydd och beredskap (MSB)
6. Netnod Internet Exchange AB (Netnod)
7. Regelrådet
8. Region Värmland
9. Statens energimyndighet
10. Stokab
11. Svenska stadsnätsföreningen (SSNF)
12. Säkerhetspolisen
13. Tele2 Sverige AB (Tele2)
14. Telenor Sverige AB (Telenor)
15. Telia Company AB (Telia)

Följande remissinstanser har inga synpunkter på, inget att invända mot, inget ytterligare att tillägga eller avstår från att lämna synpunkter på PTS förslag till nya föreskrifter.

Försvarets Radioanstalt, Försvarsmakten, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Konkurrensverket, Konsumentverket, Myndigheten för press, radio och tv, Polismyndigheten, Svenska kraftnät, Sveriges Kommuner och Regioner, Teknikföretagen, Trafikverket och Vinnova.

Konkurrensverket framför i sitt yttrande att de noterar att PTS har genomfört en grundlig konsekvensanalys avseende föreskrifternas marknadspåverkan, och i det sammanhanget haft dialog med bredbandsmarknadernas aktörer samt genomfört samråd med berörda myndigheter. Verket har mot den bakgrunden inget att invända mot de föreslagna föreskrifterna.

Framförda synpunkter redovisas i kapitel 3 (Övergripande synpunkter) och i kapitel 4 (Närmare synpunkter på förslaget).

3. Övergripande synpunkter

3.1 Allmänt om de föreslagna föreskrifterna

Telia anför bl.a. följande. Som PTS anger i konsekvensbeskrivningen utgör elektroniska kommunikationsnät och tjänster en grundläggande funktion för att dagens samhälle ska fungera. Sverige är beroende av fungerande elektroniska kommunikationer i såväl normalläge som i kris, höjd beredskap och krig. Det är därför

viktigt att säkerheten upprätthålls och att näten och tjänsterna inte drabbas av störningar och avbrott samt att uppgifter om personer och deras kommunikation behandlas på ett korrekt sätt och skyddas. Telia har därför i allt väsentligt inte några invändningar mot det förslag till nya föreskrifter som PTS nu remitterar.

MSB framför följande. Telekommunikation blir allt viktigare för att kommunicera under vardag och vid samhällsstörningar. Det påverkar såväl enskilda och myndigheter som samhällsviktiga företag m.fl. Driftsäkerhet och robusthet i elektroniska kommunikationer har mycket stor betydelse för samhällets funktionalitet, inte minst för samhällsviktig verksamhet. Den här typen av föreskrifter är därmed av mycket stor vikt för arbetet med att utveckla och stärka det civila försvaret i samhället. De kommer även att ha direkt betydelse för framtidens säkra elektroniska kommunikationstjänster som MSB har i uppdrag att planera och förbereda vidare utveckling och etablering av för dagens Rakelanvändare. MSB ser mot bakgrund av detta ett behov av att justera och förtydliga ett antal av kraven i föreskrifterna.

SSNF har ingen erinran gällande PTS nya säkerhetsföreskrifter. SSNF framför vidare att små aktörer behöver vägledning och stöd och att PTS bör tillhandahålla handfasta vägledningar till sektorns aktörer, till både stora och små, för att säkerställa en så god efterlevnad som möjligt av föreskrifterna.

Stokab välkomnar förslaget till föreskrifter och allmänna råd om säkerhet i nät och tjänster och anser att förslaget utgör ett viktigt komplement till de skyldigheter som följer av nya LEK. Stokab framför att elektroniska kommunikationsnät och tjänster utgör en grundläggande funktion för att dagens samhälle ska fungera. I princip samtliga sektorer i samhället är beroende av säker och pålitlig elektronisk kommunikation då allt fler tjänster och samhällsfunktioner förlitar sig på datatrafik via fungerande nät och tjänster för allt från sjukvård till försörjning av livsmedel och dricksvatten. Elektroniska kommunikationer är dessutom av stor vikt för Sveriges totalförsvarsförmåga.

Samtidigt ger den ökade digitaliseringen i samhället upphov till utmaningar i form av nya och fler risker, hot och sårbarheter. Det rådande försämrade säkerhetspolitiska läget i Europa och Sveriges närområde gör dessutom att riskerna för incidenter till följd av angrepp eller påverkan på elektroniska kommunikationsnät och -tjänster ökar.

Att elektroniska kommunikationsnät och tjänster är säkra, tillförlitliga och robusta blir således allt viktigare, likaså vikten av att tillhandahållare bedriver ett ändamålsenligt och anpassat säkerhetsarbete i syfte att säkerställa detta – såväl utifrån befintliga som nya risker och hot. Detta är desto mer angeläget sett till dels det faktum att telekomsektorns mångfald av aktörer föranleder behov av samordning och resursdelning, dels det intersektoriella beroendet mellan totalförsvarets olika sektorer.

Mot bakgrund av det ovanstående och eftersom säkerhet i nät och tjänster är ett komplext område, som omfattar många olika aspekter, ser Stokab positivt på PTS förslag, som ger vägledning i hur det övergripande säkerhetsarbetet ska bedrivas.

Stokab anser att nya krav som föreslås i förslaget överlag är ändamålsenliga och relevanta samt att det är lämpligt att kraven är utformade som funktionskrav (”vad”-krav), istället för tekniskt detaljerade krav på hur något ska uppnås (”hur”-krav). Mot bakgrund av att de verksamheter som omfattas av föreskrifterna skiljer sig mycket åt och således också har olika risker är det enligt Stokabs uppfattning angeläget att tillhandahållare har flexibilitet att utifrån förskrifternas krav, utforma säkerhetsarbetet och bestämma vilka exakta åtgärder som behöver vidtas utifrån den egna verksamheten.

Tre välkomnar de föreslagna föreskrifterna i stort och framför att det är bra att PTS har kvarhållit struktur och innehåll i stort i förhållande till nuvarande föreskrifter men också försökt begränsa ändringarna i förhållande till nuvarande föreskrifter.

Region Värmland framför att samhällets digitalisering förutsätter tillförlitlig digital infrastruktur och kraven behöver skärpas successivt. Det handlar inte bara om driftsäkerhet och robusthet av fysisk infrastruktur, utan även mjuk infrastruktur såsom rutiner och processer. Det handlar också om att säkerställa redundanta förbindelser på många platser. Det är ett område som tilltar i betydelse, inte minst genom det ökade behovet till följd av pandemin, att alltmer av den offentliga servicen genomförs via digitala tjänster, den snabba ökningen av cyberkriminalitet och nu det oroliga världsläget.

Region Värmland framför att behovet av tillförlitliga och säkra uppkopplingar kan skilja sig beroende på slutanvändarens verksamhet, behov och krav, men inte mellan tätorter och glesbebyggda områden eller om det är en liten eller stor nätägare.

PTS nya föreskrifter och allmänna råd om säkerhet i nät och tjänster bör utgå från slutanvändarens behov samt var i bredbandsnätens topologi som risk för störningar föreligger och var konsekvensen av störningar är stora, snarare än att utgå från nätägarens förmåga att upprätthålla en adekvat driftsäkerhetsnivå. Redundans och reservkraftsystem är de kanske viktigaste åtgärderna för att öka nätens driftsäkerhet och robusthet. Samtidigt är PTS förslag på åtgärder kostsamma för nätägaren och därmed en viss rimlighet i att mindre nät åläggs mindre långtgående skyldigheter. Samtidigt kan inte en enskild kund i ett mindre nät anses bli mindre drabbad av ett avbrott än en i ett större nät. Det blir dessutom än mer ologiskt att en kund som är ansluten via till exempel en fiberförening inte omfattas av säkerhetsföreskrifterna, men att denna situation kan förändras om en större nätägare köper fiberföreningens nät.

Åtgärder för redundans och reservkraft är i princip desamma som de åtgärder som samhället har att stå för gällande det LEK säger om ”Tjänsters tillgänglighet vid extraordinära händelser i fredstid”. Det är därför svårt att bedöma rimligheten i PTS förslag separat. Det kan vara så att staten behöver ta en viss del av ansvaret så att enskilda användarna i alla nät, stora som små, får ta del av likvärdig driftsäkerhet.

Det är sammantaget olyckligt att mindre nätägare, som fiberföreningar och mindre stadsnät, inte omfattas av de viktigaste delarna av PTS ~~s~~äkerhetsföreskrifter, då ett hushåll i ett villaområde i en tätort har samma behov och krav på nätens tillförlitlighet som ett hushåll i en by i ett landsbygdsområde.

PTS kommentar: Av säkerhetsbestämmelserna i nya LEK framgår bl.a. att åtgärder som tillhandahållare ska vidta ska vara proportionerliga. Föreskrifterna innehåller därför bl.a. krav på klassificering av tillgångar, där tillgångar klassas högre ju fler aktiva anslutningar som skulle påverkas om tillgången slutar fungera (se 11 kap. 1 §). Med utgångspunkt från tillgångarnas klassificering ska tillhandahållaren efterleva krav på redundans och reservkraft (11 kap. 3–8 §§). PTS noterar Region Värmlands synpunkt men bedömer att ställda krav är proportionerliga.

Energimyndigheten framför bl.a. följande. Föreskrifterna och konsekvensutredningen bedöms som väl underbyggda och väl avvägda. Energimyndigheten ger förslag på en gemensam beredning och samverkan kring riskanalys för sektorerna, men myndigheten har inga direkta invändningar mot föreskrifterna.

Energisektorn är beroende av säkra elektroniska kommunikationer, vilket innebär att de nu föreslagna föreskrifterna blir normerande för en central del av säkerheten även för energiförsörjningen. PTS och Energimyndigheten har tidigare samverkat kring utformning av säkerhetsåtgärder i föreskrifter för informationssäkerhet inom ramen för NIS (Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster) och LEK. Det kan finnas anledning att stärka det sektorsöverskridande perspektivet mellan elektroniska kommunikationer och energiförsörjning då en avgränsad analys och hantering av risker i svenska samhällsviktiga verksamheter och kritiska infrastrukturer i allt mindre utsträckning speglar faktiska beroenden och risker.

Det finns idag rekommendationer från EU-kommissionen och ENISA[1] för hur en sektorsöverskridande riskanalysprocess för energi- och telekomsektorn skulle kunna genomföras, och exempelvis Österrike genomför årligen en samlad riskanalys för sektorerna.

[1] European Union Agency for Cybersecurity, den europeiska cybersäkerhetsmyndigheten.

PTS kommentar: Med anledning av att ett reviderat NIS-direktiv, det s.k. NIS2, har beslutats (i maj 2022) och ska genomföras i svensk lag inom loppet av 21 månader kommer ett ökat sektorövergripande perspektiv mellan t.ex. telekom- och energisektorn att bli ännu mer angeläget.

3.2 Sammanslagning av flera föreskrifter till en regelsamling

MSB, SSNF, Stokab och Tre ser positivt på att PTS uppdaterar samt sammanför flera föreskrifter till en regelsamling och framför sammanfattningsvis bl.a. följande. Sammanslagningen ger en bättre överblick och struktur samt ökad tydlighet åt bestämmelserna. På detta sätt tydliggörs också på ett bra sätt att säkerhetsarbetet ska omfatta samtliga säkerhetsaspekter. Det bedöms vara både viktigt och nödvändigt för att kunna bedriva ett systematiskt arbete för att tillhandahålla elektroniska kommunikationsnät och -tjänster som är säkra, tillförlitliga och robusta.

GlobalConnect och **Telenor** framför bl.a. följande. Samlingen av reglerna i en regelsamling, som ersätter fem befintliga föreskrifter och allmänna råd, medför risker. Mot denna bakgrund är det viktigt att ändamålet med varje regel, definitioner och uttryckssätt genomgående är tydliga samt vilken aspekt av säkerhet (autenticitet, tillgänglighet, riktighet och konfidentialitet) som respektive regel tar sikte på är tydlig. Det framförs vidare att ju mer omfattande föreskrifterna är desto större är även risken att föreskrifterna kommer att kompletteras med ett stort antal ändringsföreskrifter och på sikt därför bli mer svåröverskådlig än om respektive säkerhetsområde styrdes av egna föreskrifter.

PTS kommentar: PTS har gjort vissa förtydligande justeringar i föreskrifterna med anledning av Telenors och GlocalConnects synpunkter. PTS kan även genom t.ex. tillsyn (och vägledningar) komma att avgöra och ytterligare tydliggöra vissa frågor.

3.3 Kommande NIS-direktiv

Telia framför bl.a. följande. Enligt förslag till nytt NIS-direktiv (NIS 2) ska det nya direktivet ersätta artiklarna 40 och 41 i Kodexen. NIS 2 ska vara infört i medlemsstaterna senast 18 månader efter det att direktivet har trätt ikraft. Redan om ca två år kommer med all sannolikhet säkerhetsbestämmelserna i nya LEK och nu aktuella föreskrifter att ersättas eller kompletteras. Även om NIS 2 ännu inte är antaget hade det varit önskvärt om PTS tagit upp frågan i sin konsekvensutredning.

Telia framför vidare att de föreslagna föreskrifterna innebär krav på riskanalyser och dokumentation av dessa som till viss del inte sker idag. De befintliga riskanalyserna måste kompletteras och dokumenteras. Nya säkerhetsåtgärder kan behöva vidtas. Det är inte rimligt att tvingas införa nya rutiner och vidta åtgärder som när de är införda i stor utsträckning behöver förändras. Enligt Telias uppfattning bör PTS därför

i detta skede endast göra sådana förändringar i nuvarande föreskrifter som oundgängligen är nödvändiga för att genomföra Kodexen i nuvarande lydelse.

PTS kommentar: Föreskrifterna ska överensstämma med överordnad reglering och syftar till att förtydliga bestämmelserna i nya LEK. Med anledning av att nya LEK träder ikraft den 3 juni 2022 har PTS inte haft möjlighet att invänta kommande reglering (NIS 2).

PTS gör bedömningen att den kommande implementeringen av NIS 2 inte påverkar vilka aktörer som berörs av föreskrifterna eller kriterierna för vad som avses med en incident. Eventuella justeringar i PTS föreskrifter kan dock, som Telia påpekar, bli aktuella i ett senare skede men det påverkar inte PTS bedömning om behovet av föreskrifter i nuläget.

3.4 Behov av tydliga regler

Ett antal remissinstanser har uttryckt att det finns ett behov av att förtydliga vissa ordalydelser eller kravformuleringar i föreskrifterna.

MSB ser mot bakgrund av samhällets behov av tillförlitliga och säkra elektroniska kommunikationsnät och tjänster att det finns ett behov av att justera och förtydliga ett antal av kraven i föreskrifterna, bl.a. bestämmelser om riskanalys, åtgärder efter riskbedömning, reservkraftskrav, klassificering av tillgångar och kontinuitetsplanering.

Tre framhåller att det finns några otydligheter i föreskrifterna som kan ge upphov till tolkningsproblem, vilket kan leda till bristande regelefterlevnad. Tre anför vidare att det är viktigt att det står klart vad som förväntas av tillhandahållarna. Det är en förutsättning att reglerna i föreskrifterna är tydliga och förutsägbara eftersom bristande regelefterlevnad av stora delar av kraven kan föranleda sådan sanktionsavgift som införs i 12 kap. nya LEK, vilken har en straffliknande karaktär (se prop. 2021/22: 136 s. 381). PTS måste av rättssäkerhetsskäl ha högsta ambitionsnivå avseende reglernas tydlighet och förutsägbarhet i tillämpningen för tillhandahållarna. Om otydliga regler och skönsmässiga bedömningar läggs till grund för beslut om sanktionsavgift är det mycket problematiskt och rättsosäkert.

Tre framför vidare att PTS avvägning av vilka säkerhetsåtgärder som bedöms som nödvändiga är också viktig, då varje sådan ändring kan vara förenad med stora anpassningskostnader för tillhandahållarna. Detta gäller också tillsynes små justeringar, t.ex. kravet för informationsbehandlingstillgångar att spara varje version av en identifierad tillgång (system, databaser och fysiska resurser) samt dess tillverkare under mycket lång tid. Detta bör därför övervägas noggrant av PTS.

PTS kommentar: PTS har med anledning av synpunkterna justerat vissa delar av föreskrifterna. Vilka närmare justeringar PTS har gjort framgår av efterföljande avsnitt i denna sammanställning.

Telenor framför att en genomgående otydlighet i föreskrifterna är säkerhetsbegreppet. Telenor menar att det i vissa delar avser alla aspekter av säkerhet medan det i andra delar främst verkar ta sikte på driftsäkerhet, exempelvis när PTS gör skillnad på åtgärder som ska förhindra säkerhetsincidenter respektive integritetsincidenter.

PTS kommentar: I 1 kap. 7 § nya LEK definieras säkerhetsincident som en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser. Det vill säga, definitionen omfattar fyra säkerhetsaspekter. En säkerhetsincident kan röra negativ inverkan på en eller flera av de fyra säkerhetsaspekterna.

Integritetsincident definieras i 1 kap 7 § nya LEK som en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster. Definitionen är densamma som i nu gällande LEK (se prop. 2010/11:115 s. 130 f. och 181).

Det finns händelser som enligt definitionerna kan vara både en säkerhetsincident och en integritetsincident. Skyldigheterna är delvis överlappande i och med att samma händelse kan vara rapporteringspliktig enligt båda regelverken. Dock ställs i regelverken olika krav för vilka incidenter som ska rapporteras och vilka regler som gäller för rapporteringen. Det framgår av respektive bestämmelse i föreskrifterna om kraven tar sikte på säkerhetsincidenter eller integritetsincidenter eller både och.

GlobalConnect uppger att det behöver klargöras hur definitionen av säkerhetsincident ska tillämpas. Enligt definitionen i nya LEK innebär en händelse med faktisk negativ inverkan på tillgängligheten en säkerhetsincident. Hur förhåller sig detta till den tillgänglighet som avtalats med kunder? Innebär även en händelse som ligger inom ramarna för den typ av avbrott som avtalats med kunder en säkerhetsincident?

PTS kommentar: Säkerhetsbestämmelserna i nya LEK och PTS föreskrifter utgör grundnivån för de åtgärder som tillhandahållare ska vidta. I kapitel 17 PTS föreskrifter tydliggörs vilka säkerhetsincidenter som bedöms ha betydande påverkan på nät och

tjänster och därmed är rapporteringspliktiga till PTS. I det fall en säkerhetsincident bedöms falla in under kriterierna i kapitel 17 är den rapporteringspliktig till PTS. Tillhandahållare kan inte avtala bort skyldigheter enligt nya LEK.

3.5 Ikraftträdandedatum för föreslagna föreskrifter

GlobalConnect framför att det är kort tid fram till att den nya lagstiftningen träder ikraft och konstaterar att PTS föreslår att föreskriften träder ikraft samtidigt som den nya lagstiftningen. GlobalConnect ser stora utmaningar att hinna vidta eventuella förändringar som föreskrifterna innebär till den 1 augusti 2022. Särskilt om de nya kraven innebär behov av IT-utveckling.

Telia anför att de nya föreskrifterna troligen kommer att antas i slutet av juni 2022 och att de enligt förslaget ska träda ikraft den 1 augusti 2022. Det framstår som uppenbart att det inte finns tillräckligt med tid för att kunna efterleva de nya kraven redan vid ikraftträdandet, om fyra månader från idag. PTS bör därför senarelägga ikraftträdandet av föreskrifterna. Detta är särskilt motiverat mot bakgrund av de möjligheter till sanktionsavgifter som införs i samband med införandet av den nya LEK.

PTS kommentar: Föreskrifterna kompletterar och förtydligar skyldigheter i nya LEK och syftar till att uppnå en enhetlig tillämpning av skyldigheterna så att nät och tjänster är säkra. Detta gör att det är angeläget att nya LEK och de nya föreskrifterna träder i kraft i nära anslutning till varandra. Det är vidare angeläget ur rättssäkerhetssynpunkt att det finns en tydlighet och förutsägbarhet i regleringen. PTS bedömer därför att det är lämpligt att föreskrifterna träder i kraft den 1 augusti 2022. De föreslagna föreskrifterna motsvarar vidare till stor del de nuvarande föreskrifterna.

3.6 Skyldighet att ställa krav på underleverantörer och tjänsteleverantörer i enlighet med gällande bestämmelser om säkerhet i föreskrifter och lag

Allente framför bl.a. följande. Bolaget agerar tjänsteleverantör avseende bredband, TV och telefoni till kunder på den svenska öppna stadnätsmarknaden. Mot bakgrund av att bolaget inte äger eller opererar någon infrastruktur på egen hand behöver det ingå samarbetsavtal med aktörer med dessa tjänster. Tjänsteleverantörsrollen för Allente möjliggörs bl.a. via samarbeten med andra tjänsteleverantörer. För att kunna erbjuda slutkundstjänster har också Allente ingått avtal med ett flertal stadsnät i Sverige där kunder finns anslutna. Med denna bakgrund är det Allentes åsikt att remissen gällande förslag till föreskrifter om säkerhet i nät och tjänster inte påverkar Allente utan ansvaret ligger hos deras samarbetspartners.

PTS kommentar: *PTS vill i detta sammanhang uppmärksamma tillhandahållare på att skyldigheten att vidta säkerhetsåtgärder i de föreslagna föreskrifterna gäller för tillhandahållare oaktat om arbetet utförs i egen regi eller om extern aktör uppdras att utföra arbetet. Det är därmed av vikt att de tillhandahållare som väljer att använda sig av externa aktörer säkerställer att kraven på säkerhet och integritet regleras i avtal samt att tillhandahållare följer upp underleverantörers säkerhetsarbete både innan och under avtalstiden för att säkerställa att kraven efterlevs av underleverantören. Bristande kravställning och kontroll av underleverantörer kan medföra bristande säkerhet. Sådana brister är något tillhandahållare hålls ansvariga för*.

3.7 Regelrådets bedömning

Regelrådet finner att PTS konsekvensutredning uppfyller kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning.

PTS kommentar: PTS noterar detta.

3.8 Beaktande av Sveriges säkerhet vid tillämpning av nya LEK

Säkerhetspolisen har i sitt yttrande anfört bl.a. följande. Säkerhetspolisen och PTS har inom ramen för samrådsprocessen i det aktuella föreskriftsarbetet haft en långtgående dialog om att i föreskrifterna arbeta in de principer och kriterier som återfinns i det s.k. inriktningsdokumentet, vilket utgjort ett bedömningsunderlag vid prövningen av ansökningarna i auktionen av frekvenser tänkta för de svenska 5G-näten. Inriktningsdokumentet har genom PTS beslut den 20 oktober 2020 och den 20 januari 2021 (PTS dnr 18-8496) blivit en del av tillståndsvillkoren för auktionen och tillståndshavarna förutsätts under hela tillståndens giltighetstid iaktta de principer som framgår av inriktningsdokumentet. Att dessa gäller, utöver de nu föreslagna föreskrifterna, bör tydliggöras i konsekvensanalysen. Som Säkerhetspolisen tidigare fört fram till PTS bör samma krav som gäller för 5G-näten ställas även på andra elektroniska kommunikationsnät som är vitala för Sveriges säkerhet. Det är därför en brist att inte samtliga krav återfinns i de nu reviderade föreskrifterna. Vidare bör det förtydligas att säkerhetskänslig verksamhet och sådana tillgångar som utgör skyddsvärden enligt säkerhetsskyddslagen (2018:585) ska identifieras och skyddas enligt den lagstiftningen, varför andra krav kan gälla utöver dessa föreskrifter.

PTS kommentar: PTS har föreslagit nya föreskrifter och allmänna råd om säkerhet i nät och tjänster med utgångspunkt i de rättsliga mandat som ges PTS i 1 kap. 11 § samt 8 kap. 1, 3–6 och 9 §§ nya LEK. PTS har noga analyserat de föreslagna föreskrifterna i förhållande till Säkerhetspolisens inriktningsdokument. PTS har bedömt att många av de mål för Sveriges säkerhet som anges i dokumentet uppfylls genom de föreslagna bestämmelserna eller redan genom lagtexten.

Om verksamhetsutövarna identifierar sin verksamhet, sina nät och tjänster, som säkerhetskänslig verksamhet åligger det dem att förutom säkerhetsföreskrifterna även följa säkerhetsskyddslagen. Det är PTS uppfattning att målen i inriktningsdokumentet så långt möjligt uppfylls genom den basnivå som säkerhetsföreskrifterna utgör, tillsammans med de särskilda villkor som PTS ställt som villkor för innehav av radiofrekvenser i frekvensband avsedda för användning av 5G-teknik och de särskilda bestämmelser som enligt säkerhetsskyddslagen gäller för säkerhetskänslig verksamhet. Sammantaget anser PTS att detta utgör en proportionerlig kravnivå.

3.9 Kommerskollegiums bedömning

Kommerskollegium ser inte anledning att ifrågasätta PTS bedömning om att de bestämmelser som har sitt ursprung i e-dataskyddsdirektivet kan betraktas som anmälningspliktiga enligt förordningen (1994:2029) om tekniska regler. Kollegiet bedömer vidare att de tjänster som regleras i förslaget inte omfattas av tjänstedirektivet och därmed uteblir en anmälan enligt förordning (2009:1078) om tjänster på den inre marknaden.

PTS kommentar: PTS har anmält relevanta delar av föreskrifterna i enlighet med förordningen (1994:2029) om tekniska regler.

3.10 Synpunkter om alternativ som inte har föreslagits

Tre framför att det i prop. 2021/22:183[2] avseende registrering av kontantkort uppkommit en utökad reglering avseende uppgift som omfattas av ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken. En komplettering till berörda avsnitt behöver göras om de avsnitten även ska omfatta bevarandet av viss lagrad uppgift.

PTS kommentar: I 9 kap. 25 § nya LEK anges att 8 kap. 5 § ska tillämpas på motsvarande sätt avseende den uppgift som ska bevaras. PTS har, med stöd av 8 kap. 5 § andra stycket, tagit fram föreskrifter om de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. 8 kap. 5 § nya LEK ska tillämpas på det sätt som framgår av PTS föreskrifter. PTS kommer att se över behovet av förtydliganden i säkerhetsföreskrifterna med anledning av förslagen i prop. 2021/11:183. PTS kan även komma att förtydliga tillämpningen av 8 kap. 5 § i kommande tillsyn.

[2] Regeringens proposition 2021/22:183 Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter.

Energimyndigheten framför att det för aktörernas konsekvensplanering vore önskvärt om det fanns möjlighet att ta hänsyn till en prioritering av kunder eller anslutningar, både för kraven på redundans och för en återstart.

PTS kommentar: PTS noterar Energimyndighetens önskemål. Förslaget till föreskrifter utgör en grundläggande nivå på säkerhet i nät och tjänster. Idag finns, som Energimyndigheten påpekat, ingen skyldighet för tillhandahållare att prioritera vissa kunders behov av tillgång till fungerande elektroniska kommunikationer. I de fall enskilda kunder önskar en högre nivå av säkerhet än den nivå som föreskrifterna stadgar kan kunderna avtala och köpa detta av tillhandahållare utifrån verksamhetens behov.

3.11 Användning av uttrycken riskanalys, riskhantering och åtgärder efter riskbedömning (se även avsnitt 4.4.1, 4.4.3 och 4.5.3)

För att undvika missförstånd föreslår **MSB** att användningen av begreppen riskanalys och riskbedömning justeras på så sätt att de överensstämmer med hur begreppen används i ISO 27000-serien.

PTS kommentar: *PTS ändrar inte användningen av begreppen i enlighet med MSB:s förslag i denna version av föreskrifter. Av det allmänna rådet till 3 kap. 1 § föreskrifterna framgår att tillhandahållare, till stöd för säkerhetsarbetet, bör utgå från etablerad standard på området., SS-ISO/IEC 27000-serien eller motsvarande. För att undvika missförstånd tar PTS bort referensen till ISO27000-serien.*

4. Närmare synpunkter på förslaget

Vissa remissinstanser har haft synpunkter på ordval osv. i förslaget till föreskrifter. PTS har genomfört vissa justeringar i föreskriftstexten mot bakgrund av dessa men redovisar inte samtliga dessa justeringar i sammanställningen nedan.

4.1 Ord och uttryck (2 kap.)

4.1.1 Avsaknad av definitioner

SSNF framför att det i 2 kap. saknas några definitioner, exempelvis allmänt elektroniska kommunikationsnät, allmänt elektronisk kommunikationstjänst samt interpersonell kommunikationstjänst. SSNF efterfrågar förtydliganden och gärna exempel då såväl stora som små aktörer ska ta del av föreskrifterna.

PTS kommentar: Med anledning av att uttrycken elektroniskt kommunikationsnät, allmänt elektronisk kommunikationstjänst samt interpersonell kommunikationstjänst definieras i nya LEK har PTS inte definierat begreppen i föreskrifterna. Begreppen har samma innebörd i föreskrifterna som i nya LEK, se 2 kap. 1 § föreskrifterna.

Säkerhetspolisen framför att de definitioner som används i föreskrifterna kan leda till otydlighet om vilka tillhandahållare som omfattas av de aktuella föreskrifterna och vilka krav som gäller för respektive åtgärd. Exempelvis anges att med begreppet *kommunikationstjänst* avses (genom en hänvisning till 1 kap. 7 § nya LEK) ”en tjänst som (….) är en interpersonell kommunikationstjänst”. När det däremot gäller definitionen av begreppet *aktiv anslutning*, avses en ”anslutning till kommunikationstjänst, som inte är en nummeroberoende interpersonell kommunikationstjänst” (s.k. NI-ICS). Detta kan leda till förvirring och det saknas en närmare analys av varför de s.k. NI-ICS undantas från den sistnämnda definitionen.

PTS kommentar: Anledningen till att s.k. NI-ICS:ar inte omfattas av definitionen ”aktiv anslutning” är att de enbart tillhandahåller slutkundstjänster, till skillnad mot sådana tillhandahållare som erbjuder tjänster både till slutkunder och till andra tjänsteleverantörer.

Telenor framför att det är oklart hur aktiva anslutningar ska beräknas när den aktuella tillgången eller förbindelsen används som insatsvara för andra tillhandahållare, se PTS förslag till allmänt råd till 17 kap. 3 §. Som underleverantör är det oftast inte möjligt att veta hur många slutkunder som kan nyttja tjänsten i nästa led. Definitionen bör därför avse ”*omedelbar användning av kommunikationstjänster av en slutanvändare som är abonnent hos den som äger eller kontrollerar tillgången*”.

PTS kommentar: I det fall en tillhandahållare hyr ut kapacitet till en eller flera andra tillhandahållare, t.ex. en s.k. kommunikationsoperatör, kan den som hyr kapacitet i många fall enkelt ta reda på hur många användare eller aktiva anslutningar som deras tillgångar betjänar. Tillhandahållaren bör därmed relativt enkelt kunna få den uppgiften från den som hyr kapacitet.

Säkerhetspolisen framför att i definitionen av *”kritisk komponent”* bör uttryck som ”sända och motta” ersättas med ”genererar och behandlar” då de är mer ändamålsenliga begrepp som används i lagtexten.

PTS kommentar: Definitionen av kritisk komponent är densamma som i tidigare föreskrifter (PTSFS 2015:2). Begreppet är känt av tillhandahållarna och PTS har i denna översyn av föreskrifterna valt att inte ändra definitionen..

Telenor framför att de förstår definitionen av ”tillgång” som att den utesluter underliggande infrastruktur och tillhörande funktioner, såsom kanalisation, teknikutrymmen, master, torn, kraft, kyla samt sensorer, givare, prober och liknande som inte har någon direkt funktion i tjänsteleveransen.

PTS kommentar: Begreppet ”tillgång” används i föreskrifterna för att beteckna en funktion som är nödvändig för att tillhandahålla kommunikationsnätet eller kommunikationstjänsten och som utgör en avgränsad del av nätet eller tjänsten som är avsedd att användas för att sända, motta, bearbeta eller lagra information. En tillgång utgör således en aktiv del av nätet eller tjänsten. Tillhandahållare bedömer vilka funktioner i deras nät och tjänster som utgör tillgångar. Vid bedömningen är det dock viktigt att beakta att tillgången måste vara nödvändig för att tillhandahålla tjänsten vilket gör att en tillgång t.ex. åtminstone behöver vara av viss omfattning eller betydelse.

4.2 Övergripande säkerhetsarbete (3 kap.)

4.2.1 Långsiktigt, kontinuerligt och systematiskt säkerhetsarbete (3 kap. 1 §)

Telenor framför att de är certifierade enligt ISO 27001 och välkomnar referenserna till detta ledningssystem. Telenor uppger vidare att ISO 27001 tar sikte på informationssäkerhet, inte driftsäkerhet.

PTS kommentar: Skyldigheterna enligt 1 kap, 8 kap. och 9 kap. i nya LEK har ett vidare omfång och har ett vidare ändamål än ISO 27000-serien.

Att tillhandahållare bör tillämpa processer som utgår från etablerad standard syftar till att ge tillhandahållare ett stöd i arbetet. Viktigt att poängtera är dock att etablerade standarder innehållsmässigt fokuserar på risker för tillhandahållares verksamhet i sig medan kraven i föreskrifterna istället fokuserar på risker utifrån ett användar- och samhällsperspektiv. PTS ställer inte krav på att tillhandahållaren ska utgå från ISO-27000-serien specifikt och ser därför att tillhandahållare kan använda den eller motsvarande standarder som stöd i syfte att kunna bedriva ett säkerhetsarbete i enlighet med gällande föreskrifter. PTS har förtydligat detta genom en justering i det allmänna rådet så att hänvisningen till en specifik standard har tagits bort.

4.3 Identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare (4 kap.)

4.3.1 Identifiering och dokumentation av tillgångar, informationsbehandlingstillgångar, förbindelser och uppdragstagare (4 kap. 1 §).

Telenor framför att det i samband med att kravet i 4 kap. på olika förteckningar slås ihop i samma föreskrifter uppstår frågan om det är önskvärt att samtliga beståndsdelar införs i samma förteckning eller om PTS hellre ser en åtskillnad så att det finns en separat förteckning över tillgångar, informationsbehandlingstillgångar och förbindelser. Telenor uppger att om förteckningen görs gemensamt uppstår frågan om hur en tillgång som också är en informationsbehandlingstillgång ska betecknas. Enligt GDPR finns därtill liknande krav på dokumentation och riskanalys (privacy impact analysis), men som utgår från behandlingen snarare än den tillgång som behandlar informationen. I praktiken kan dock dessa förteckningar och riskanalyser vara delvis överlappande.

PTS kommentar: Det ställs inte några krav på huruvida dokumentationen av tillgångar och förbindelser ska vara samlad eller inte eller vilken form dokumentationen ska ha. Det är upp till tillhandahållaren. Men tillhandahållaren ska åtminstone dokumentera en unik beteckning, funktion samt en hänvisning till aktuell riskanalys, geografisk placering om sådan finns och tillverkare för tillgångar, informationstillgångar och förbindelser. Dokumentationen syftar bl.a. till att effektivisera genomförandet av riskanalyser, underlätta upptäckt av tillgångar som fysiskt gått sönder och behöver repareras m.m. Av 3 kap. föreskrifterna framgår att tillhandahållarens identifiering, dokumentation och bevarande ska ske på ett systematiskt och långsiktigt sätt.

GlobalConnect framför att det är oklart vad PTS anser som en fastställd version av en databas i kontexten av 4 kap. 1 §. Det är vidare inte rimligt att varje förändring av databasen är en ny version som ska lagras under fem år. PTS kostnadsuppskattning relaterat till detta krav är ytterst blygsam och om kravet innebär att det efter varje förändring uppstår en ny version av en databas som ska sparas i fem år är uppskattningen helt orealistisk.

Telia framför att dokumentationen för Telias nät ändras vid tusentals tillfällen per år, vilket innebär att mer än tusen versioner varje år behöver sparas och det i fem år för var och en av dessa versioner. Telia uppger vidare att kravet därigenom medför att det blir en enorm mängd data som sparas, vilket kan bli svårhanterligt, oöverskådligt och kostsamt. Telia framför därtill att PTS inte angett något egentligt skäl till att alla versioner ska sparas och bevaras i fem år samt att Telia i tidigare samråd påpekat

detta, men inte heller då fått något gehör eller något klargörande från PTS avseende den frågan.

Tre framför att det nya kravet på dokumentation av informationstillgångar så långt tillbaka i tiden saknar angivna skäl eller avgränsning för vad som är nödvändigt har svårt att förstå varför PTS anser att detta ska vara nödvändigt. Tre anger vidare att det inte synes finnas någon konsekvensanalys om innebörden av denna förändring, även i förhållande till de av PTS uppskattade kostnaderna som denna lagring medför och som Tre anser är grovt underskattade. Tre bedömer att kravet på lagring och versionshantering som helhet blir en stor administrativ börda för verksamheten som inte står i proportion till vad bestämmelsen ska uppnå.

Tre har vidare svårt att se hur föreskrifterna i denna del på ett konsekvent sätt ska kunna tillämpas på ett ”system” eller en ”databas”. Det finns en otydlighet i vad som avses med ett system i förhållande till ”geografisk placering” och ”tillverkare”. Tre förstår inte relevansen av att behöva dokumentera geografisk placering av system och databaser, såsom t.ex. CRM-system. Informationstillgångar bör vidare inte omfattas av krav på dokumentation av geografisk placering och tillverkare i 1 § andra stycket 3 och 5 samt krav på bevarande av varje uppdaterad version av dokumentation i 1 § tredje stycket.

PTS kommentar: Kravet på identifiering, dokumentation samt bevarande av uppgifter i fem år är inte nytt och har i tidigare föreskriftsarbeten konsekvensutretts av PTS. Bestämmelsen är inte avsedd att innebära en ändring i sak jämfört med 4 § i PTSFS 2020:1. Däremot omfattas fler tillhandahållare av de nya bestämmelserna jämfört med tidigare.

Att ha en aktuell och samlad bild över samtliga tillgångar, informations-behandlingstillgångar, förbindelser och uppdragstagare är enligt PTS en förutsättning för att ha god kontroll över verksamheten och fastställa vad som omfattas av säkerhetsarbetet. Identifieringen och dokumentationen är utgångspunkten för arbetet med riskanalyser och vidtagandet av säkerhetsåtgärder. Utan detta är det inte möjligt att genomföra en korrekt riskanalys eller avgöra vilka åtgärder som behöver vidtas för att hantera eventuella risker. Dokumentationen är vidare en viktig del för att kunna följa upp och kontrollera säkerhetsarbetet, t.ex. ta reda på vilka säkerhetsåtgärder som har vidtagits för en viss tillgång eller vilka uppdragstagare som har utfört ett visst uppdrag även sedan en viss tid förflutit. Om en tillgång, informationsbehandlingstillgång eller förbindelse inte identifieras och dokumenteras finns det en risk att denna faller utanför det systematiska säkerhetsarbetet och över tid löper risk att bli exponerad för de risker som bristande säkerhetsarbete innebär. Sparade versioner av dokumentation är dessutom ett viktigt redskap i PTS tillsyn.

4.4 Riskanalys (5 kap.)

Säkerhetspolisen påpekar att en riskanalys ska göras av relevanta hot och att det är oklart vad som anses vara ett relevant hot och vem som avgör detta. Det förutsätter också att den som gör bedömningen har förmågan att avgöra vad som är ett relevant hot. Det finns i detta sammanhang skäl att framhålla att när det gäller vissa hot har regeringen uttalat att det bara är Säkerhetspolisen och Försvarsmakten som har helhetsbilden (se prop. 2019/20:153 s. 35, Samråd om tillståndsärenden). Vidare framför Säkerhetspolisen att fråga uppstår om detta medför att ett hot som inte anses vara relevant inte ska konsekvensbedömas. Rimligen borde även skyddsvärden beaktas när en riskanalys görs.

PTS kommentar: Enligt 5 kap. 1 § föreskrifterna ska tillhandahållare genomföra riskanalyser. Som en del av detta ska de identifiera relevanta hot (se 5 kap. 3 §). Det är dock naturligt att det är Säkerhetspolisen och Försvarsmakten som har helhetsbilden när det gäller vissa typer av hot. Detta har tagits om hand i föreskrifterna i 5 kap. 2 §. Enligt bestämmelsen ska riskanalyser bl.a. genomföras efter att tidigare okända hot som är relevanta för riskanalysen identifierats. Information om sådana hot kan förmedlas av Post- och telestyrelsen. På så sätt finns en möjlighet för samrådsmyndigheterna att, via PTS, nå ut till tillhandahållarna och medverka till att vissa typer av hot analyseras.

MSB framför att uttrycket "likvärdiga tillgångar" i 5 kap. 1 § behöver förtydligas.

Tre anför att det är oklart vad PTS menar med ”likvärdiga tillgångar” i det allmänna rådet till 5 kap. 1 §. Om med likvärdiga tillgångar avses den funktion som tillgångarna realiserar och som bedöms ha gemensamma eller likvärdiga risker så bör rådet tydliggöras. Om det endast gäller en kategorisering av tillgångar där varje kategori (t.ex. basstationer, hubbar, osv.) kan omfattas av en riskanalys så är det allmänna rådet begripligt. PTS bör klargöra vad som avses här.

Telenor framför att de sammanslagna bestämmelserna om riskanalyser leder till frågan om PTS nu ser framför sig att tillhandahållarna gör en gemensam riskanalys för tillgångar eller grupper av tillgångar som också är informationsbehandlingstillgångar eller grupper av sådana, eller om PTS hellre ser att tillhandahållarna håller dessa riskanalyser åtskilda.

PTS kommentar: Av 5 kap. 1 § framgår bl.a. att riskanalyser ska göras för varje tillgång, informationsbehandlingstillgång och förbindelse. Det allmänna rådet till 1 § är en möjlighet för tillhandahållare att förenkla arbetet med riskanalyserna genom att det ger utrymme för gemensamma riskanalyser för likvärdiga tillgångar,

[3] Skydd av Sveriges säkerhet vid radioanvändning (riksdagen.se)

informationsbehandlingstillgångar och förbindelser. Det är dock tillhandahållaren som får bedöma i vilka fall gemensamma riskanalyser är lämpliga och vid genomförande av riskanalyser för ”likvärdiga tillgångar” beakta de eventuella unika förutsättningar och hot som finns för respektive tillgång, informationsbehandlingstillgång och förbindelse.

MSB framför att det är otydligt om 5 kap. 2 § innebär att en helt ny riskanalys alltid ska göras vid inträffad incident eller om den befintliga kan uppdateras.

PTS kommentar: Av 5 kap. 2 § framgår att en riskanalys bl.a. ska genomföras vid en inträffad säkerhetsincident som är rapporteringspliktig enligt 17 kap. Tillhandahållaren får bedöma huruvida den uppdaterar en befintlig riskanalys eller om den upprättar en ny riskanalys.

MSB framför att uttrycket "planerade förändringar" behöver tydliggöras och undrar om ”planerade förändringar” gäller samtliga förändringar eller om det endast rör sig om väsentliga förändringar.

PTS kommentar: Samtliga planerade förändringar ska omfattas av en relevant riskanalys.

MSB framför vidare att PTS användning av "riskanalys" och "riskbedömning" bör justeras så att de överensstämmer med hur begreppen används i ISO27000-serien. I 5 kap. 3 § 4 beskrivs riskbedömningen som en del av riskanalysen. Vid användandet av en sådan terminologi bör besluten baseras på hela riskanalysen och inte bara riskbedömningen såsom den beskrivs i föreskrifterna. Jämför 14 kap. där tillhandahållaren ska upprätta kontinuitetsplaner utifrån konsekvensanalysen.

PTS kommentar: Av PTS föreskrifter framgår att den av leverantören valda riskanalysmetoden ska utgå från etablerad standard. PTS har inte ställt krav på att leverantören ska utgå från ISO-27000-serien specifikt och ser därför inte att begreppen riskanalys och riskbedömning är missvisande. Det allmänna rådet har justerats för att förtydliga detta.

Telenor framför följande. Riskanalyser ska enligt föreskrifterna bl.a. göras inför ”upphandlingar”. Telenor vet inte varför begreppet ”upphandlingar” har valts och vad som skiljer begreppet från ”anskaffning” eller ”inköp”. Upphandling för tankarna till en process med konkurrensutsättning och anbudsutvärdering.

PTS kommentar: PTS har justerat föreskrifterna på så sätt att begreppet ”upphandlingar” har ersatts av ”inför anskaffning av tillgångar, informationsbehandlingstillgångar, förbindelser och anlitande av uppdragstagare”.

Telenor framför att när det gäller för tillhandahållaren okända hot som anges av PTS och som ska beaktas i riskanalysen, är det viktigt att hotet kan beskrivas så konkret som möjligt. Generell information, exempelvis ett påstående om en allmänt ökad risk för cyberangrepp, kan inte anses som ett tillräckligt specifikt hot i detta avseende.

PTS kommentar: *PTS kan inte på förhand uttala sig om vilken slags information som kan komma att lämnas till myndigheten av säkerhetsmyndigheterna. Det är dock även PTS uppfattning att upplysningar om tidigare okända hot bör vara så konkreta som möjligt, så att lämpliga skyddsåtgärder kan vidtas.*

Tre anför att det inte framgår av 5 kap. 1 § att riskanalyser ska genomföras för uppdragstagare, däremot anges detta i 2 § tredje strecksatsen. Det framgår inte heller av 3 § hur riskanalyser ska genomföras för uppdragstagare. Det kanske finns en avsikt med det men det skapar ändå en otydlighet i förhållande till om riskanalyser för uppdragstagare förutsätts omfatta hotbeskrivning och de olika bedömningskriterierna i 3 §. Jämfört med 3 § sista stycket så preciseras kravet beträffande riskanalyser som ska utföras vid planerade förändringar. Vilka kriterier gäller och är relevanta beträffande uppdragstagare? PTS bör således precisera kravet på vad riskanalyser för uppdragstagare ska innefatta.

PTS kommentar: Även vid anlitande av uppdragstagare ska risken för att tillgångar, informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av säkerhets- eller integritetsincidenter analyseras. Det är tillhandahållaren som slutligen har ansvaret för säkerheten i sina egna nät och tjänster, oavsett om någon annan har anlitats för att utföra ett visst uppdrag. Kraven för genomförande av riskanalyser som framgår av 5 kap. 3 §, med tillhörande allmänt råd, är till exempel relevanta även vid anlitande av uppdragstagare.

Tre framför vidare att i 5 kap. 2 § första stycket sista strecksatsen anges att vissa hot som är relevanta för riskanalysen kan förmedlas av PTS. Ordet ”förmedling” är ett förhållandevis vagt ord och kan komma att förväxlas med av PTS uppmärksammade händelser eller kartläggning om hot på ett mer allmänt oadresserat plan. I stället föreslår Tre att ”PTS kan meddela tillhandahållaren om sådana hot som avses i första stycket.”

PTS kommentar: PTS justerar inte formuleringen i det aktuella förslaget. Av bestämmelsen framgår att information om sådana hot kan förmedlas av PTS. PTS ser att det kan finnas eller uppstå hot mot säkerheten som myndigheten – men inte nödvändigtvis tillhandahållare – får kännedom om. För att säkerställa att dessa hot beaktas av tillhandahållare anges därmed i bestämmelsen att även denna typ av okända hot ska analyseras. På vilket sätt sådan information förmedlas till tillhandahållare regleras inte utan får avgöras i det enskilda fallet.

Telenor uppger att PTS, i samband med hantering av planerade förändringar anger säkerhetsaspekterna tillgänglighet, konfidentialitet, autenticitet och riktighet som nya, utan att ge närmare vägledning till vad de förväntas tillföra i riskanalyserna.

Telenor påpekar vidare att det finns uttalanden i konsekvensutredningen som skapar osäkerhet om vad som egentligen är nytt. PTS anger på sid. 73 i konsekvensutredningen att det förändrade kravet på riskanalys innebär att tillhandahållarna behöver beakta fler säkerhetsaspekter utöver tillgänglighet, nämligen därtill konfidentialitet, autenticitet och riktighet. I det följande stycket anger dock PTS att kravet inte ändras i sak och kommer därför inte innebära några ytterligare kostnader.

PTS kommentar: Med anledning av det nya säkerhetsbegreppet i nya LEK behöver tillhandahållarna beakta fler säkerhetsaspekter i sin riskanalys. Utöver tillgänglighet måste även aspekterna konfidentialitet, autenticitet och riktighet beaktas. Detta är ingen direkt konsekvens av PTS föreskrifter då det utvidgade säkerhetsbegreppet har sitt ursprung i nya LEK. Det är alltså inte PTS föreskrifter i sig som föranleder ytterligare kostnader, eftersom de eventuella ytterligare tekniska och organisatoriska åtgärder tillhandahållaren kan behöva vidta har sin grund i det utvidgade säkerhetsbegreppet i nya LEK.

4.5 Riskhantering och åtgärder efter riskbedömning (6 kap.)

4.5.1 Riskhantering (6 kap. 1 §)

MSB anser att PTS mandat att vidta åtgärder när en tillhandahållare accepterar allt för många risker bör förtydligas. Just nu står det att en tillhandahållare alltid bör eftersträva att reducera risker framför att acceptera riskerna och att tillhandahållare endast bör acceptera risker om säkerheten i nät och tjänster i stort kan upprätthållas trots att hotet förverkligas eller incidenten inträffar. MSB anser att det bör finnas ett tydligare mandat i föreskrifterna för PTS att kunna styra leverantörernas riskhantering via tillsyn.

PTS kommentar: Av bestämmelsen framgår tydligt att tillhandahållarens beslut att undvika, reducera eller acceptera en risk ska ske med utgångspunkt i riskbedömningen. PTS kan inte se att det saknas mandat för PTS att granska och göra bedömningar avseende tillhandahållarens riskhantering.

Telenor anser att det, för att underlätta förståelsen och tillämpningen av PTS föreskrifter, hade varit ändamålsenligt att i föreskrifterna närmare förklara innebörden av de nya säkerhetsaspekterna konfidentialitet, autenticitet och riktighet, vilka är nya åtminstone till sin lydelse och i de sammanhang de är relevanta.

PTS kommentar: Det nya säkerhetsbegreppet och de olika säkerhetsaspekternas innebörd återfinns i nya LEK och beskrivs i dess förarbeten. I PTS föreskrifter aktualiseras de olika säkerhetsaspekterna genom att bestämmelser tar sikte på säkerhetsincidenter, vilket i sin tur definieras i nya LEK.

Netnod uppger bl.a. följande. Övergripande för riskhantering säger föreskrifterna: ”*Tillhandahållaren ska utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras. Sådana beslut ska dokumenteras. Beslut om att acceptera en risk ska även motiveras*.” Dock gör föreskrifterna avsteg från denna logik när redundans förordas som den enda lösningen under rubriken ”*Åtgärder efter klassificering av tillgångar*”.

Netnod uppger vidare att det inte är god föreskriftssed att förordna både analys och specifikt val av lösning. Antingen bör analys förordnas där aktörer hålls till svars för att genomföra en sund analys och hantera uppkomna risker, eller så bör föreskrifterna förordna specifika lösningar, inte både analys och lösning.

PTS kommentar: I föreskrifterna finns krav som närmare anger hur tillhandahållare ska hantera risker som hotar säkerheten i nät och tjänster och skydda uppgifter som behandlas i samband med tillhandahållandet av nät och tjänster. Ett av målen med föreskrifterna är att minimera antalet säkerhets- och integritetsincidenter och dess konsekvenser.

Riskanalyser utgör ett viktigt underlag för att tillhandahållaren ska kunna besluta hur risker ska hanteras och vilka säkerhetsåtgärder som ska vidtas och ska därför genomföras för samtliga tillgångar, informationsbehandlingstillgångar eller förbindelser.

Tillhandahållaren ska vidta de säkerhetsåtgärder som behövs mot bakgrund av vad som framkommit i riskanalysen. Säkerhetsåtgärder ska vidtas när riskanalysen visar på risker som ska undvikas eller reduceras. Risker i tillhandahållares verksamheter kan variera stort och det finns därför stor möjlighet för tillhandahållaren att själv välja lösning för att hantera olika risker. Åtgärder ska vidtas på en nivå som är anpassad till den aktuella risken, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.

I föreskrifterna finns dock också krav på att vissa säkerhetsåtgärder inom vissa särskilt angivna områden ska vidtas, oaktat resultatet av riskanalysen. Ett exempel är att tillhandahållare ska ha redundans för tillgångar, förbindelser och kritiska komponenter. Syftet med bestämmelsen är att minska risken för säkerhetsincidenter i form av störningar eller avbrott, till följd av att tillgångar eller förbindelser upphör att fungera. Åtgärder kring exempelvis redundans ska alltså alltid vidtas, under förutsättning att förutsättningarna i bestämmelserna i övrigt är uppfyllda. Att PTS valt

att ställa krav om säkerhetsåtgärder för vissa områden har sin grund i vad PTS genom t.ex. tillsyn, inrapporterade incidenter, risk- och sårbarhetsanalys för sektorn, samråd och annan utredning, har funnit är särskilt viktigt för att säkerställa säkerhet i nät och tjänster och skydd av behandlade uppgifter. I dessa bestämmelser anges vad som måste uppnås med en skyddsåtgärd (redundans) men inte hur detta ska åstadkommas. Redundans kan vara två eller flera identiska eller olika sätt att oberoende av varandra fylla samma funktion. Det är då upp till tillhandahållaren att själv avgöra vilka åtgärder som behövs för att säkerställa att bestämmelsen efterlevs.

Säkerhetspolisen uppger följande. Enligt 6 kap. 1 § ska tillhandahållaren utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om risker ska undvikas, reduceras eller accepteras. Detta innebär att för det fall risken är okänd för tillhandahållaren behöver denne inte vidta några åtgärder för att skydda skyddsvärda uppgifter. I likhet med de krav som ställts upp i inriktningsdokumentet borde som utgångspunkt det skyddsvärda skyddas oavsett om det finns ett känt hot eller känd risk.

PTS kommentar: Tillhandahållaren ska utifrån riskbedömningen besluta hur respektive risk ska hanteras. I föreskrifterna ställs dock krav på tillhandahållaren att alltid vidta säkerhetsåtgärder inom vissa särskilt angivna områden, exempelvis vad gäller åtkomst och behörighet, säkerhetskopiering, loggning och redundans. Åtgärder inom vissa av PTS utpekade områden ska därmed vidtas även om tillhandahållaren inte är medveten om samtliga eventuella risker kopplade till den aktuella tillgången, informationsbehandlingstillgången eller förbindelsen, under förutsättning att förutsättningarna i bestämmelserna i övrigt är uppfyllda.

Vidare framgår av 5 kap. 2 § att tillhandahållaren ska genomföra en riskanalys om denne identifierar nya hot, som tidigare inte varit kända för tillhandahållaren och att information om sådana hot kan förmedlas av PTS.

Tillhandahållare som omfattas av nya LEK kan i vissa fall även bedriva säkerhetskänslig verksamhet och omfattas i dessa delar av säkerhetsskyddslagen (2018:585).

4.6 Åtkomst och behörighet (7 kap.)

4.6.1 Åtkomst och behörighet (7 kap. 1 §)

MSB föreslår att bestämmelsen ändras så att tilldelade behörigheter ska tas bort efter utfört uppdrag, istället för att det i det allmänna rådet står att de bör tas bort.

PTS kommentar: PTS noterar detta, men bedömer att det är mest ändamålsenligt att ge rekommendation om borttagande av tilldelade behörigheter i form av ett allmänt råd.

Säkerhetspolisen uppger att enligt 7 kap. 1 § första meningen ska tillhandahållaren medge åtkomst till tillgångar och behandlade uppgifter. Enligt Säkerhetspolisens uppfattning bör motsvarande krav även finnas för informationssystem.

PTS kommentar: Uttrycket ”Informationssystem” återfinns varken i nya LEK eller i PTS föreskrifter. Däremot definieras ”informationsbehandlingstillgångar” i förslaget till föreskrifter såsom system, databaser och fysiska resurser som används för informationsbehandling. PTS bedömer att ett ändamålsenligt skydd uppnås genom att koppla kravet till tillgångar och behandlade uppgifter.

Säkerhetspolisen uppger att av 7 kap. 1 § tredje meningen framgår att tillhandahållaren ska ha system för hantering och kontroll av identiteter och behörigheter. Det är oklart vad för system som avses (behörighetskontrollsystem?) och detta bör tydliggöras.

PTS kommentar: Det finns inget krav på hur bestämmelsen ska efterlevas. Det är upp till tillhandahållare att avgöra vilket eller vilka system som behövs för att säkerställa att bestämmelsen efterlevs. Systemet ska dock säkerställa att åtkomst endast medges i enlighet med tilldelade behörigheter och omfattar bl.a. att unika identiteter skapas, behörigheter tilldelas administrativt, användare loggar in och enbart kan göra det som behörigheterna tillåter i systemet. En tillhandahållare kan uppfylla regleringen genom ett ensamt system eller med flera olika system som samverkar kring hantering av identiteter, hantering av behörigheter, kontroll av inloggningsuppgifter och kontroll (enforcement) av behörigheterna.

Säkerhetspolisen uppger vidare att det av det allmänna rådet till 7 kap. 1 § framgår att den som kommer i kontakt med behandlade uppgifter *bör* få viss utbildning. Enligt Säkerhetspolisens uppfattning ska detta både vara ett krav och något som det förutsätts att vederbörande har fått innan denne kommer i kontakt med uppgifterna.

PTS kommentar: Av föreskrifterna framgår att tillhandahållaren måste säkerställa att endast den som har upplysts om tystnadsplikten ges åtkomst till behandlade uppgifter. Vad gäller utbildning för den som kommer i kontakt med behandlade uppgifter bedömer PTS att det är mest ändamålsenligt att ge rekommendationer om utbildning och information som ett allmänt råd.

4.7 Säkerhetskopiering m.m. (8 kap.)

4.7.1 Skydd mot oavsiktlig eller otillåten utplåning eller förlust (8. kap 1 §)

Telenor ser inte att ändringen i ordalydelse (s. 83 i konsekvensutredningen) jämfört med PTS 2014:1 är motiverad, eftersom definitionen av integritetsincident i nya LEK inte har ändrats på motsvarande sätt.

PTS kommentar: PTS noterar, i likhet med Telenor, att den ordalydelse som anges i konsekvensutredningen inte har införts i föreskrifterna. Den korrekta definitionen framgår dock av 8 kap. 1 § föreskrifterna.

4.7.2 Skydd mot oavsiktlig eller otillåten utplåning samt oavsiktlig förlust eller ändring av uppgifter som lagras för brottsbekämpande ändamål (8 kap. 2 §)

Säkerhetspolisen anser, angående det allmänna rådet till 2 §, att det behöver tydliggöras att samma skyddsåtgärder gäller för redundant lagring som för lagrade uppgifter eftersom de redundanta lagringarna annars kan manipuleras.

PTS kommentar: PTS bedömer att det faktum att uppgifter ska lagras redundant inte innebär att den ena eller andra upplagan av uppgifterna ska ha ett lägre skydd än vad som i övrigt anges. Av 2 § tredje stycket framgår vidare att ”Säkerhetskopior eller motsvarande ska omfattas av samma skydd […] som de uppgifter som lagras för brottsbekämpande ändamål”, vilket betonar att alla kopior av dessa uppgifter ska ha samma skydd.

4.8 Loggning (9 kap.)

Säkerhetspolisen anger att det i kapitlet ställs krav på loggning av vissa aktiviteter, men det är oklart om detta även ska tolkas så att det ställs krav på behörighet till informationssystem och lokaler där informationssystem förvaras.

PTS kommentar: Krav på åtkomst och behörighet till tillgångar och behandlade uppgifter finns i kapitel 7 i föreskrifterna. För loggning avseende behandlade uppgifter finns inga särskilda krav på behörighet till informationssystem och lokaler där informationssystem förvaras.

Säkerhetspolisen framför att det är oklart vad som avses med systematisk kontroll och i vilket syfte den ska utföras.

PTS kommentar: Vad som är systematisk kontroll anges inte särskilt, men att arbeta systematiskt innebär att tillhandahållaren arbetar på ett ordnat sätt. Det kan t.ex. innebära att tillhandahållaren följer en etablerad plan, dvs. ett på förhand etablerat arbetssätt, för sin loggkontroll.

Telenor upplever att bestämmelsen innebär ett utvidgat krav på loggning, och att det blir intressant att se hur balansen gentemot GDPR ska hållas i de fall det är personuppgifter som loggas och uppger att det hade varit önskvärt att PTS gav bättre ledning i hur denna avvägning ska ske i praktiken.

PTS kommentar: Som anges i konsekvensutredningen har kraven på loggning i allmänhet utökats något. Loggning av all läsning, kopiering, ändring och utplåning av behandlade uppgifter innebär normalt inte att de behandlade uppgifterna själva ska loggas, även om det ibland blir oundvikligt (i vissa fall exempelvis kundnummer eller handläggar-id). I den mån en loggningsåtgärd i sig innebär en personuppgiftsbehandling behöver den följa GDPR[4].

4.8.1 Loggning av läsning, kopiering, ändring och utplåning och åtkomst till system (9 kap. 1 §)

Tre påpekar att det inte framgår vad ”återkommande” i det sista stycket i 9 kap. 1 § om ”Kontroller av loggar ska ske systematiskt och återkommande” innebär. Tre önskar även att en minsta lagringstid för loggar ska framgå av reglerna.

PTS kommentar: Loggning kan göras på olika sätt, och uppföljning och kontroll kan göras på olika sätt. Hur detta görs i detalj för att efterleva kravet lämnar PTS till tillhandahållaren att avgöra. I de fall loggningen innebär en personuppgiftsbehandling måste tillhandahållaren även följa reglerna i GDPR. Formuleringen om ”återkommande kontroller” har samma lydelse som PFSFS 2014:1 och innebär ingen ändring i sak.

4.8.2 Loggning av systemhändelser för att utreda säkerhetsincidenter (9 kap. 2 §)

Tre anser att det vore lämpligt att ange exempel på vilka systemhändelser som bör loggas i ett allmänt råd till paragrafen, istället för att ge exempel i konsekvensutredningen på vad som kan utgöra systemhändelser som kan loggas.

PTS kommentar: Föreskrifterna riktar sig till en bred skara tillhandahållare som har många olika nät, tjänster och övriga it-system, och det är därför inte lämpligt att ge specifika exempel. PTS lämnar därför till tillhandahållaren att avgöra vilka systemhändelser som är relevanta för att kunna uppfylla syftet, dvs. för att kunna utreda säkerhetsincidenter.

[4] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

4.9 Kryptering (10 kap.)

4.9.1 Kryptering av behandlade uppgifter (10 kap. 1 §)

Telenor uppfattar bestämmelsen som att det är innehållet som ska krypteras och inte att överföringen som sådan ska vara krypterad.

PTS kommentar: Bestämmelsen anger att behandlade uppgifter som överförs via internet ska skyddas genom kryptering. PTS har inte angivit tillvägagångssätt, protokoll eller metoder.

GlobalConnect anser att förslaget om kryptering behöver förtydligas och att konsekvensutredningen exemplifierar avtal och fakturor via e-post som lämpliga att kryptera. Globalconnect anser vidare att sådana regler hör hemma i annan reglering och att det är svårt att hitta tekniska lösningar för exemplen ovan.

PTS kommentar: Exemplen i konsekvensutredningen är avsedda att visa vid vilka situationer som uppgifter riskerar att spridas och komma på avvägar. I sådana fall kan risken för en säkerhets- eller integritetsincident minskas genom att t.ex. använda en säkrare lösning än e-post eller att undvika att skicka sådana uppgifter som inte är nödvändiga. Regeln gäller sådana uppgifter som behandlas i samband med tillhandahållande av en allmänt tillgänglig kommunikationstjänst.

MSB anför att bedömningsnivån ”låg” inte är definierad och att om inte modellen för riskanalys är definierad riskerar detta att bli en allt för subjektiv bedömning.

PTS kommentar: PTS har formulerat om bestämmelsen i 10 kap. 1 §. Det anges nu tydligare att uppgifter inte behöver skyddas genom kryptering om det med hänsyn till uppgifternas art och sammanhang är osannolikt att överföring utan kryptering kan leda till en säkerhets- eller integritetsincident.

MSB anser vidare att koder, lösenord och sammanställningar av uppgifter som rör en användare eller abonnent ska krypteras vid överföring via internet, istället för att ange att de ”bör” krypteras i tillhörande allmänt råd.

PTS kommentar: PTS har valt att använda ett allmänt råd för att medge flexibilitet. En alternativ lösning måste fortfarande ge samma nivå av skydd.

Tre anser att den föreslagna formuleringen av 1 § är inkonsekvent och föreslår istället formuleringen ”Behandlade uppgifter som överförs via internet ska skyddas genom kryptering, om inte risken för säkerheten i nät och tjänster och för behandlade uppgifter bedöms vara låg”, dvs att ta bort referensen till riskanalys i författningstexten.

PTS kommentar: PTS delar bedömningen att referensen till riskanalys bör tas bort och har därför justerat författningstexten.

4.10 Redundans och reservkraft (11 kap.)

Säkerhetspolisen anför att det framstår som oklart hur många mobila nät i Sverige som faller in under klass A, dvs. 200 000 eller fler aktiva anslutningar. Säkerhetspolisen anser också att under alla förhållanden är den föreslagna indelningen i klasser inte ändamålsenlig för att säkerställa krav på tillgänglighet i elektroniska kommunikationsnät som är vitala för Sveriges säkerhet. Detta medför att det kan finnas skäl att ställa höga krav på redundans och reservkraftsystem även på tillgångar i de lägre klasserna.

PTS kommentar: Klassificeringen följer en modell där antalet aktiva anslutningar, eller i förekommande fall användare, avgör hur betydelsefull en tillgång är, främst ur tillgänglighetsperspektiv. Kravet för respektive klass är satt efter en proportionalitetsbedömning baserad på bl.a. avbrottsstatistik. Som ett resultat är kraven högre för tillgångar som påverkar många aktiva anslutningar eller användare, vilket indirekt har en betydelse för Sveriges säkerhet. Utöver klassningen finns särskilda regler för reservkraftsystem för mobila nät och tjänster (11 kap. 9 § föreskrifterna).

PTS vill i detta sammanhang påpeka att tillhandahållare som bedriver säkerhetskänslig verksamhet även omfattas av säkerhetsskyddslagen (2018:585).

4.10.1 Klassificering av tillgångar - tillhandahållande av kommunikationsnät eller kommunikationstjänster som inte är nummeroberoende interpersonella kommunikationstjänster (11 kap. 1 §)

MSB konstaterar att relativt många aktiva utrustningar hamnar i kategori E. I och med utrullningen av 5G kommer dessa bli ännu fler. Detta kommer att innebära att relativt stora delar av samhällsviktig verksamhet blir allt mer beroende av aktiva anslutningar i kategori E. Denna utveckling borde återspeglas i krav även på dessa tillgångar.

PTS kommentar: I 11 kap. 9 § finns krav på reservkraft som träffar även tillhandahållare i kategori E i händelse av fel i extern elförsörjning. PTS har bedömt att denna kravnivå är proportionerlig i förhållande till tillhandahållare med ett lågt antal aktiva anslutningar.

Säkerhetspolisen framför att antalet aktiva anslutningar i mobila accessnät enligt det allmänna rådet till 11 kap. 1 § definieras som antalet samtidigt möjliga aktiva anslutningar till basstationen, det vill säga det maximala antalet samtidiga användare av respektive basstation. Säpo framför vidare att det av PTS konsekvensutredning framgår att det faktum att en aktiv anslutning möjliggör omedelbar anslutning, inte

innebär att anslutningen måste vara påslagen och i bruk. Det är svårt att avgöra vad som egentligen omfattas av begreppet aktiv anslutning.

Telia framför att det i konsekvensutredningen ges två olika beskrivningar av hur antalet användare ska beräknas. Dels att ”Den ska istället göras utifrån det antal aktiva anslutningar som normalt sett är beroende av tillgången för en fungerande uppkoppling”. Dels görs en hänvisning till det allmänna rådet där ”det maximala antalet” ska beaktas. Telia anser att dessa två beskrivningar, att antingen utgå ifrån ”normalt sett” eller ”maximala antalet” står i konflikt med varandra.

Telia och **Telenor** uppger att antalet aktiva anslutningar för mobilbasstationer inte kan beräknas som ”maximalt antal samtidiga användare” utan att medföra en orimligt hög klassning.

PTS kommentar: PTS har gjort ett förtydligande i det allmänna rådet till 11 kap. 1 § på så sätt att det tydligare framgår att antalet aktiva anslutningar beräknas utifrån det antal aktiva anslutningar som tillhandahållaren har dimensionerat tillgången för. Beräkningen bör även omfatta förutsägbara belastningstoppar.

4.10.2 Säkerställande av tillgångar i klass D (11 kap. 5 §)

MSB anser att 8 respektive 12 timmar bör kunna krävas istället för föreslagna 12 respektive 18 timmar vad gäller avbrott orsakade av att kritiska komponenter upphör att fungera.

PTS kommentar: PTS har i tidigare konsekvensutredning bedömt att kraven är ändamålsenliga och proportionerliga. PTS har inte funnit skäl att ändra tidsfristerna i denna översyn.

4.10.3 Redundans av förbindelser mellan tillgångar i klasserna A, B och C (11 kap. 6 §)

Telenor påpekar att när det gäller geografisk redundans står det inte alltid klart hur denna realiseras när förbindelser hyrs från annan aktör, t.ex. ett stadsnät. Av både säkerhets- och konkurrensskäl kan leverantören ofta hålla den exakta dragningen hemlig. Som köpare blir det svårt att helt säkerställa att förbindelsen inte i någon enda del går i samma kanalisation eller passerar samma nod.

PTS kommentar: PTS känner till problematiken, men understryker att ansvaret för att kraven uppfylls ligger hos tillhandahållaren, som bör ha förutsättningar att kunna försäkra sig om att kraven uppfylls utan att för den skull känna till den exakta dragningen för förbindelsen.

4.10.4 Säkerställande av förbindelser mellan en tillgång i klass D och tillgångar i klasserna A, B och C (11 kap. 7 §)

MSB anser att 8 respektive 12 timmar bör kunna krävas istället för föreslagna 12 respektive 18 timmar vad gäller avbrott orsakade av att förbindelser upphör att fungera.

PTS kommentar: PTS har i tidigare konsekvensutredning bedömt att kraven är ändamålsenliga och proportionerliga. PTS har inte funnit skäl att ändra tidsfristerna i denna översyn.

4.10.5 Reservkraftsystem avseende tillgångar i klasserna A, B, C och D (11 kap. 8 §)

MSB anser att kraven bör skärpas och anför att tillgångar i klass C och D i tätort med fler än 8000 invånare bör ha reservkraft under åtminstone 24 timmar, och att ett sådant krav skulle harmonisera med funktionskraven på elnät.

PTS kommentar: PTS har i tidigare konsekvensutredning bedömt att kraven är ändamålsenliga och proportionerliga. PTS har inte funnit skäl att ändra tidsfristerna i denna översyn.

4.10.6 Reservkraftsystem avseende mobila kommunikationsnät och kommunikationstjänster (11 kap. 9 §)

Telenor anför följande. En nyhet i förhållande till de befintliga föreskrifterna är att vid strömavbrott på mobila kommunikationsnät och kommunikationstjänster, ska det inte längre vara tillåtet att prioritera viss tjänst för att minska tillgångarnas elförbrukning. Enligt konsekvensutredningen är detta en följd av att alla tjänster i 4G och 5G går över data och att det därför inte får några konsekvenser för mobiloperatörerna om denna möjlighet tas bort. Det anges inte hur befintliga 3G-nät ska hantera strömavbrott, men då PTS är tydliga med att förändringen inte får några konsekvenser utgår Telenor från att det fortfarande i praktiken ska vara möjligt att prioritera viss tjänst vid strömavbrott på 3G-site, trots att föreskrifterna inte medger detta. Om PTS i stället menar att möjligheten att ansöka om undantag ska användas för basstationer där tjänst eller viss täckningsgrad dras ner för att spara ström, borde detta ha angetts i konsekvensutredningen. Det riskerar annars blir en mycket stor och omfattande undantagshantering om samtliga sådana siter ska behöva omfattas av undantag per den 1 augusti 2022.

PTS kommentar: 11 kap. 9 § föreskrifterna motsvarar i stort 22 § i PTSFS 2015:2, med den materiella ändringen att tillhandahållaren inte längre kan prioritera bland tjänster. Föreskrifterna är tilltänkta att vara teknikneutrala, så att reglerna kan tillämpas oavsett generation av mobilteknologi. Tjänster (t.ex. tal, data och meddelandetjänst) ska

tillhandahållas under den föreskrivna tiden, trots strömavbrott inom ett visst område. PTS ställer inte krav på att en specifik mobilnätsgeneration ska användas för att realisera en viss tjänst. Om detta uppfylls med 3G eller några andra mobilnätsgenerationer anges inte. PTS föreskrifter ger dock tillhandahållare möjlighet att ansöka om undantag för bl.a. sådana tillgångar som omfattas av beslut om avveckling.

Telia framför att PTS beskrivning i sin konsekvensutredning av den pågående avvecklingen av 2G- och 3G-näten och den pågående utbyggnaden av 5G stämmer väl överens med den stora modernisering av Telias mobilnät som just nu pågår. Telia instämmer i att möjligheten till prioritering mellan samtalstjänst, meddelandetjänst och datakommunikationstjänst bör utgå. Telia instämmer dock inte i att förändringen i kravet inte skulle medföra några ytterligare kostnader eller att den ens skulle vara genomförbar till den 1 augusti 2022, utan föreslår att PTS hanterar införandet av nya krav på reservkraft för mobilnätet på ett liknande sätt som vid införandet av PTSFS 2015:2. Telia föreslår att det nya kravet på reservkraft för mobilnät gäller från den 1 augusti 2022 för basstationer som från och med detta datum moderniseras med 5G, eller nyetableras, samt från den 1 augusti 2025 för nätet i sin helhet.

PTS kommentar: PTS har strävat efter att hålla föreskrifterna teknikneutrala så att reglerna kan tillämpas oavsett generation av mobilteknologi. Således ska tjänster, t.ex. tal, data och meddelandetjänst, tillhandahållas under den föreskrivna tiden trots strömavbrott inom ett visst område. Om detta uppfylls med 2G, 4G eller några andra mobilnätsgenerationer anges inte. I 11 kap. 10 § föreskrifterna finns möjlighet att ansöka om undantag från kravet om tillämpningen av bestämmelsen skulle få konsekvenser som är oproportionerliga i förhållande till kostnaderna, olämpliga med hänsyn till tillgänglig teknik, olämpliga med hänsyn till annan reglering eller oproportionerliga med hänsyn till att berörda tillgångar eller förbindelser omfattas av beslut om avveckling.

MSB stödjer ändringen att det inte längre är möjligt eller lämpligt att skilja på samtals-, meddelande- och datakommunikationstjänster.

4.11 Åtgärder avseende övervakning och beredskap (12 kap.)

4.11.1 Åtgärder avseende övervakning och beredskap (12 kap. 1 §)

Telenor uppger att en nyhet jämfört med tidigare är, enligt PTS, att övervakningen och beredskapen inte bara ska syfta till att förebygga, upptäcka och åtgärda störningar eller avbrott, utan ska även ta sikte på övriga typer av säkerhetsincidenter. Telenor förstår detta som att övervakning och beredskap därmed även ska omfatta aspekterna autenticitet, riktighet och konfidentialitet. Bestämmelsen tar enligt ordalydelsen sikte på säkerhetsincidenter, vilket definitionsmässigt utesluter

integritetsincidenter. Det står därmed inte klart för Telenor vilken omfattning övervakning och beredskap i praktiken ska ha. Precis som i övriga delar av föreskrifterna där hänvisning finns till samtliga aspekter av säkerhet, hade regelverket blivit tydligare om PTS närmare beskrivit hur aspekterna förhåller sig till de olika kraven och inte minst på vilket sätt de är kopplade även till arbetet med att förebygga integritetsincidenter.

PTS kommentar: Kravet om övervakning och beredskap omfattar även aspekterna autenticitet, riktighet och konfidentialitet. PTS lämnar åt tillhandahållaren att utforma detaljerna kring sin övervakning och beredskap eftersom verksamheten och riskerna skiljer sig åt mellan olika tillhandahållare.

Tre anser att ordet ”förebygga” bör strykas i bestämmelsen, och om formuleringen trots detta behövs enligt PTS, måste föreskrifterna förklara vad denna aktivitet i övervakningsfunktionen ska avse, eftersom det varken är logiskt eller tydligt.

PTS kommentar: Valet av ordet ”förebygga” är i detta fall avsett att innebära en förmåga att kunna upptäcka avvikelser ”i tid” och därefter åtgärda feltillstånd som annars kunde ha lett till en säkerhetsincident, dvs. stoppa förloppet innan en faktisk säkerhetsincident enligt definitionen uppstår, snarare än att enbart upptäcka den och åtgärda den efter att den inträffat.

Säkerhetspolisen anser att bestämmelsen i 1 § som innehåller övervakningskrav beträffande säkerhetsincidenter bör innehålla motsvarande krav även för integritetsincidenter.

PTS kommentar: PTS fäster stor vikt vid tillhandahållares förmåga att kunna upptäcka integritetsincidenter. Denna bestämmelse syftar främst på en förmåga att hantera betydande situationer, som har potential att falla in under definitionen på en säkerhetsincident enligt nya LEK. En integritetsincident å andra sidan kan vara en felskriven e-postadress som drabbar en enstaka individ. PTS har ansett det för långtgående att kräva sådan övervakning (och beredskap) för den typen av incidenter. Dock finns det en viss överlappning, så en situation som kan innebära både en säkerhetsincident och en integritetsincident kommer att omfattas av kravet på övervakning och beredskap.

4.12 Intern incidenthantering (13 kap.)

4.12.1 Intern hantering av säkerhets- och integritetsincidenter (13 kap. 1 §)

Tele2 uppger bl.a. följande. Enligt förslaget till föreskrifter ska en tillhandahållare säkerställa att inträffade säkerhets- eller integritetsincidenter rapporteras internt. I konsekvensutredningen uppmärksammar PTS att en materiell förändring har skett i

jämförelse med nuvarande regler i fråga om denna bestämmelse; även ”integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål omfattas av bestämmelserna”.

Denna förändring framgår emellertid inte av föreskrifterna, prop. 2021/22:136 Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation (”Propositionen”) eller av Kodexen. Tele2 noterar särskilt att bestämmelserna om skydd av trafikuppgifter m.m. som lagras eller på annat sätt behandlas för brottsbekämpande ändamål regleras i 8 kap. 5 § nya LEK, under rubriken ”Skyddsåtgärder vid lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande ändamål”, medan bestämmelserna om skydd av uppgifter vid tillhandahållande av tjänster, liksom bestämmelserna om rapportering av integritetsincidenter, regleras i 8 kap. 6 och 8 §§ nya LEK, under rubriken ”Skydd av uppgifter vid tillhandahållande av tjänster”. I Propositionen görs således skillnad på skyddet av uppgifter som lagras för brottsbekämpande ändamål och skyddet av uppgifter vid tillhandahållandet av tjänst. Begreppet ”integritetsincident” är i propositionen knutet till det senare fallet.

Den enda källan till att 13 kap. 1 § 1 föreskrifterna innehåller en materiell förändring i jämförelse med nuvarande regler är PTS:s konsekvensutredning. För det fall PTS vill inkludera integritetsintrång avseende uppgifter som lagras för brottsbekämpande ändamål i bestämmelserna om intern incidentrapportering bör detta därför framgå direkt i föreskriftstexten.

PTS kommentar: PTS avser inte att komplettera formuleringarna i 13 kap. 1 § föreskrifterna eftersom PTS bedömning är att uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK kan vara föremål för både säkerhets- och integritetsincidenter. Enligt 13 kap. 1 § föreskrifterna ska tillhandahållare vidta ett antal åtgärder vid inträffade säkerhets- eller integritetsincidenter. Därvid behöver tillhandahållare vidta föreskrivna åtgärder enligt 13 kap. föreskrifterna även för uppgifter som lagras för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK i de fall uppgifterna har omfattats av en säkerhets- eller en integritetsincident.

4.13 Kontinuitetsplanering (14 kap.)

MSB anser att begreppet kontinuitetshantering bättre återspeglar vad som regleras i kapitlet.

PTS kommentar: PTS noterar MSB:s synpunkt, men gör ingen justering av författningstexten i samband med denna föreskriftsöversyn.

4.14 Fredstida planering för totalförsvarets behov av elektroniska kommunikationer (15 kap.)

4.14.1 Kontinuitetsplaner för höjd beredskap och krig (15 kap. 1 §)

Energimyndigheten för fram följande. Det är svårt för tillhandahållarna och andra myndigheter att bedöma relevansen av generella krav på åtgärder för främst höjd beredskap och krig. Ett sätt att underlätta förståelsen och analysarbetet är att jobba med scenarion som PTS skulle kunna besluta om, och distribuera, årligen. Scenarion som analysmetod skulle kunna utvecklas tillsammans med andra relevanta myndigheter såsom exempelvis MSB och Energimyndigheten. Ett följdproblem med ospecifika krav på åtgärder för höjd beredskap och krig, blir att konsekvensanalysen till föreskrifterna för detta kapitel samtidigt blir mindre användbar eftersom subjekten svårligen kan säga var eller vilka kostnader som uppstår.

PTS kommentar: PTS genomför löpande utbildnings- och övningsverksamhet, vilka bl.a. omfattar scenarion, tillsammans med de aktörer som omfattas av bestämmelserna.

4.14.2 Revidering av kontinuitetsplaner vid information från PTS (15 kap. 2 §)

MSB anser att vilka verksamhetsdelar och resurser som är kritiska för totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap och krig och vad kontinuitetsplanerna ska innehålla för att tillgodose totalförsvarets behov av elektroniska kommunikationer vid höjd beredskap eller krig bör beslutas efter dialog med fler aktörer, bl.a. MSB.

PTS kommentar: Avsikten är att det fortsatta arbetet utifrån föreskrifterna ska göras i dialog med relevanta aktörer inom totalförsvaret, däribland MSB. PTS har inte funnit skäl att ändra bestämmelsen utifrån MSB:s synpunkter.

Telia anger att den föreslagna ordningen där PTS ska informera om vilka verksamhetsdelar som är kritiska och närmare krav i kontinuitetsplanerna väcker frågor. Bolaget anger att förslaget inte ger någon vägledning för planering, förberedelse eller krigsplacering och att förändringar måste aviseras i god tid då verksamheten har långa ledtider och PTS information påverkar ingångna kommersiella avtal.

PTS kommentar: *PTS noterar Telias synpunkt. Avsikten är att eventuell ytterligare information, där det är möjligt, kommer att tas fram i samverkan med berörda aktörer och att såväl innehåll som implementeringstider utformas på ett sådant sätt att de inte innebär omotiverade olägenheter för de aktörer som har att förhålla sig till dem.*

4.14.3 Planering för samverkan med PTS (15 kap. 3 §)

Tre framför att enligt 3 § ska tillhandahållaren planera för att vid höjd beredskap ställa personal till förfogande för samverkan med PTS i den omfattning som krävs. Det är visserligen en äldre skrivning från föreskriften 1995:1, men det framstår ändå som otydligt att tillhandahållaren ska planera för personalresurser ”som krävs”. Det är önskvärt att det av bestämmelsen, eller i ett allmänt råd till bestämmelsen, framgår vilken/vilka personalkategori(er) som bör ställas till förfogande, eftersom utsedd personal ska följa av tillhandahållarens planering.

PTS kommentar: PTS har i det allmänna rådet till 15 kap. 3 § gjort ett förtydligande om personella resurser. Det har inte bedömts som ändamålsenligt att ställa uttryckliga krav på personalresurser. PTS anser att aktörerna själva är bäst lämpade att bedöma vilken personal som behöver ställas till förfogande. Med utbildning och övning är avsikten att PTS och berörda aktörer ska ha en samsyn i frågan om vilka resurser som kan krävas.

Telenor har synpunkter på det föreslagna kravet att ställa personal till förfogande och anser att det är tillräckligt att det uppställs ett krav på en fungerande samverkansfunktion. Att ställa personal till myndighetens ”förfogande” leder tankarna till att personalen ska vara fysiskt tillgänglig, vilket kan komma i konflikt med krigsplacering eller tjänsteplikt.

PTS kommentar: PTS inför, mot bakgrund av Telenors synpunkt, ett allmänt råd till 15 kap. 3 § som förtydligar att det är en samverkansfunktion som avses.

4.15 Information till användare om konkret och betydande hot om en säkerhetsincident (16 kap.)

4.15.1 Information till användare om konkret och betydande hot om en säkerhetsincident

GlobalConnect uppger att kravet på information till användare behöver omvärderas och förtydligas för att skyldigheten enligt nya LEK inte ska få allvarliga konsekvenser och uppger att begreppet ”konkreta och betydande hot om en säkerhetsincident” är svårt att tyda.

Telenor uppger att i texten tycks ordet hot och risk emellanåt användas som synonymer, vilket inte bidrar till ökad förståelse. Rubriken och föreskriftens första led är olyckligt formulerad och skapar onödig otydlighet. Vad avses med ett ”hot om en säkerhetsincident”? Lagtexten är något tydligare som anger att det ska vara ett ”hot om att en säkerhetsincident kan inträffa”. Det framgår inte varför PTS väljer att uttrycka skyldigheten på det aktuella sättet och om någon saklig skillnad jämfört med lagtexten är avsedd.

Vidare uppger Telenor att föreskriftens andra led också skiljer sig från lagtexten och även här har PTS förslag blivit svårare att förstå. En läsning ger vid handen att PTS har ändrat innebörden men motiven för detta framgår inte. Skillnaderna mellan lagtexten och föreskrifterna är betydliga och det är anmärkningsvärt att dessa inte kommenteras närmare i konsekvensutredningen.

Mot bakgrund av att bestämmelsen är ny och dessutom sanktionerad enl. 12 kap. 1 § nya LEK är det särskilt viktigt att den både är tydlig och proportionerlig. Telenor anser att PTS måste arbeta om föreskrifterna i denna del så att otydligheterna försvinner och skillnaderna mot 8 kap. 4 § nya LEK (och art. 40.3 i direktivet) antingen tas bort eller motiveras ingående.

PTS kommentar: Med anledning av inkomna remissvar har PTS gjort vissa språkliga förtydliganden i bestämmelsen samt justerat rubriken.

GlobalConnect uppger att det ofta är kontraproduktivt att informera om säkerhetshot. Om operatörer ska informera användare om säkerhetshot måste man utgå från att även de som vill utnyttja säkerhetsbristerna för att orsaka skada får kunskap om detta. Att sprida kunskap om säkerhetshot som kan ligga till grund för underrättelseinhämtning av främmande makt eller brottslig verksamhet är direkt olämpligt. Att informera användare i en sådan situation ökar risken för att säkerhetsincidenter inträffar. Samtidigt kan det förekomma situationer där information ökar möjligheterna för användare att vidta lämpliga åtgärder som skyddar mot hot. Det är dock i mycket specifika situationer.

GlobalConnect anser att skyldigheten bara ska tillämpas restriktivt när det är tydligt att risken för säkerhetsincidenter inte ökar genom åtgärden.

Telenor anser att de konkreta hot som upptäcks och som riskerar leda till säkerhetincidenter hos tillhandahållaren i majoriteten av fall inte är lämpliga eller nödvändiga att kommuniceras med användaren. Det är i stället den förhöjda risken för störningar och avbrott i tjänsten som är av intresse för användaren att känna till och förbereda eventuella åtgärder inför. Endast i undantagsfall torde själva orsaken till den förhöjda risken för säkerhetsincidenter vara relevant för användaren att känna till. Dessutom kan säkerheten motverkas om information om vissa hot sprids i en vidare krets. Lagtextens sista led, ”om det är lämpligt, om själva hotet” är därför att föredra. Uppgift om själva hotet ska bara lämnas om det efter en sammantagen bedömning kan anses lämpligt.

PTS kommentar: Av 8 kap. 4 § nya LEK framgår att information om själva hotet ska ges till användare om det är lämpligt. Av propositionen till nya LEK framgår att vid bedömningen av om det är lämpligt att informera om själva hotet, bör det t.ex. beaktas om spridning av uppgifter om vad en upptäckt säkerhetsbrist består i kan

väntas förvärra hotet. PTS har justerat 16 kap. 1 § föreskrifterna så att det tydligare framgår att det är information om de skydds- eller motåtgärder som tillhandahållaren rekommenderar som ska lämnas, inte information om själva hotet. Av det allmänna rådet till 16 kap. 1 § i föreskrifterna framgår vidare att informationen bör lämnas på ett säkert sätt så att inte informationen i sig ger upphov till nya säkerhetsincidenter. PTS anser att det i många fall går att informera om förhöjda risker på ett sådant sätt att inte informationen i sig ger upphov till nya risker.

GlobalConnect uppger att regeringen påpekar att PTS föreskriftsrätt inte bara är verkställighetsföreskrifter utan bl.a. behövs för att ge operatörer vägledning vid bedömningen av om det finns ett konkret och betydande hot om att en säkerhetsincident ska inträffa och identifiering av lämpliga skydds- eller motåtgärder. GlobalConnect anser inte att förslaget till föreskrifter ger vägledning utan behöver förtydligas.

Telenor uppger följande. Det är inte tydligt om kravet på information när det föreligger en förhöjd risk för säkerhetsincidenter inom ett visst område, skulle kunna innefatta en skyldighet att förse användare med omvärldsanalys om hot som eventuellt kan leda till säkerhetsincidenter hos tillhandahållaren. Det förhållande att tillhandahållaren har ”upptäckt” hotet kan möjligtvis inte anses omfatta sådant som framgår av generell omvärldsanalys.

Tre uppger följande. Det är viktigt att kunder och andra användare inte får information som är meningslös och/eller förvirrande, utan den måste var väl avvägd. Dessutom kan en för frekvent information leda till minskad uppmärksamhet från kunderna.

Det vore vidare lämpligt att PTS avgränsar bestämmelsens omfattning, och tydligt exkluderar fall när skyldigheten att informera användare typiskt sett inte är nödvändigt, istället för att överlåta till tillhandahållaren att avgöra dessa gränsdragningar. Tre uppger även att det i det allmänna rådet till 1 § anges att informationen till användarna bör lämnas på ”ett säkert sätt”. Det vore lämpligt att PTS ger exempel på säkra och trovärdiga metoder som bör användas i det allmänna rådet.

PTS kommentar: I propositionen till nya LEK anges att det ska finnas ett konkret hot som kan drabba användare på ett ingående sätt, t.ex. genom att användare kan drabbas av avbrott i tjänster eller att känsliga uppgifter om användare riskerar att spridas. Vidare framgår att informationen ska ange vilka skydds- eller motåtgärder som användarna kan vidta och att det t.ex. kan röra sig om användning av kryptering, byte av lösenord eller uppgradering av programvara[5]. Att regeringen gett PTS

[5] Prop. 2021/22:136 s. 497.

föreskriftsrätt innebär en möjlighet för PTS att meddela föreskrifter om informationsskyldigheten. I föreskrifterna ger PTS ytterligare vägledning kring vilken skyndsamhet som gäller vid information till användare, hur informationen bör lämnas samt vad informationen bör innehålla. Viss ytterligare vägledning kring informationsskyldigheten finns även i ENISA:s rapport CyberThreat Consumer Outreach.[6] ENISA konstaterar att det redan idag är branschpraxis att informera användare i händelse av hot om säkerhetsincidenter och i rapporten ges exempel på sådana händelser där användare har informerats. I rapporten föreslår ENISA en checklista som stöd i bedömningen av om användare bör informeras samt på vilket sätt information bör ges. ENISA:s rapport är inget rättsligt bindande dokument utan en ögonblicksbild av ENISA:s tolkning och syn på när och på vilket sätt tillhandahållare bör informera användare.

GlobalConnect uppger att skyldigheten inte heller ska användas om det inte är säkert att användaren kan vidta åtgärder för att öka sitt skydd för att undvika konsekvenserna av en säkerhetsincident.

Telenor anför att det kan vara svårt i det enskilda fallet för tillhandahållaren att rekommendera vilka skydds- eller motåtgärder som är ändamålsenliga utifrån användarens behov. Ett strikt krav på att informera om vad användaren kan göra för att skydda sig mot säkerhetsincidentens konsekvenser är inte påkallat. Lagtexten förefaller i denna del aningen striktare än direktivstexten som stadgar att sådan information omfattar ”möjliga” skyddsåtgärder (possible measures).

Tre uppger att i många fall kan hot om en säkerhetsincident röra fysiska hot, t.ex. väderrelaterade hot som kan leda till störningar eller avbrott (som mycket väl kan vara konkreta, betydande och som riskerar leda till avbrott i tjänsterna). Dessa väderrelaterade händelser är normalt inte något som användaren kan vidta skyddsåtgärder mot.

PTS kommentar: Informationsskyldigheten till användare är ett krav som har sin grund i 8 kap. 4 § nya LEK. PTS bedömer att det i de allra flesta fall finns åtminstone någon skydds- eller motåtgärd som användaren kan vidta.

GlobalConnect föreslår att skyldigheten bara ska tillämpas efter samråd med PTS när det finns ett konkret hot och en betydande säkerhetsincident.

PTS kommentar: PTS noterar GlobalConnects förslag. Det är emellertid upp till tillhandahållarna att bedöma om informationsskyldigheten aktualiseras. Det finns

[6] Cyber threats outreach in telecom, Guidelines for national Authorities and telecom providers on outreach to users about cyber threats, March 10, 2022.

emellertid inget som hindrar att tillhandahållaren även informerar PTS om det exempelvis är lämpligt för att koordinera insatser med ytterligare tillhandahållare.

Telenor uppger att det inte framstår som tydligt i vilken utsträckning tillhandahållaren ska ha insikter i hur ingående en användare kan drabbas av säkerhetsincidenter hos tillhandahållaren, eller hur upptäckta hot har bäring på de motåtgärder användaren kan behöva vidta.

PTS kommentar: Av förarbeten till nya LEK framgår att det ”ska finnas ett konkret hot som kan drabba användare på ett ingående sätt, t.ex. genom att användare kan drabbas av avbrott i tjänster eller att känsliga uppgifter om användare riskerar att spridas.”[7] Det måste i första hand vara tillhandahållaren som bäst kan bedöma vilka effekter ett visst hot kan få och vilka motåtgärder som i det enskilda fallet är mest lämpliga.

Tre uppger följande. Hur snabbt eller vid vilken tidpunkt på dygnet som informationen ska ges framgår inte av 1 § annat än att det ska ske ”så snart som möjligt efter upptäckt” för att användaren ”så snart som möjligt ska kunna vidta de skydds-, eller motåtgärder som rekommenderas…”. I det allmänna rådet föreslås att tillhandahållarna bör beskriva risken som hotet innebär samt vad konsekvenserna kan bli om inte användarna vidtar rekommenderade åtgärder. För att förstå vilka åtgärder som kan komma att krävas i det enskilda fallet kan det bli nödvändigt att analysera hotet för att förstå riskerna och hur dessa risker kan hanteras. Det medför att innebörden av ”informera användare…så snart som möjligt efter att hotet har upptäckts” också bör ta hänsyn till den utredning och analys och riskbedömning som tillhandahållaren behöver göra för att lämna korrekt information till användarna.

Tre föreslår att 1 § kompletteras med en skrivning enligt följande.

Tillhandahållaren ska informera användare som kan komma att påverkas av ett konkret och betydande hot om en säkerhetsincident så snart som möjligt efter att hotet har upptäckts, och vid behov har analyserats, för att användarna så snart som möjligt ska kunna vidta de skydds- eller motåtgärder som rekommenderas av tillhandahållaren.

PTS kommentar: PTS har justerat bestämmelsens lydelse så att det anges att tillhandahållarna så snart som möjligt ska informera om de skydds- eller motåtgärder som tillhandahållaren rekommenderar.

[7] Prop. 2021/22:136 s. 497.

4.16 Rapportering av säkerhetsincidenter till Post- och telestyrelsen (17 kap.)

4.16.1 Rapportering av säkerhetsincidenter till PTS (17 kap. 1 - 2 §§)

Telenor föreslår att för att uppnå en ökad tydlighet om vad som gäller för rapportering av integritetsincidenter att rubriken ändras till att även inkludera integritetsincidenter och att en paragraf tillförs som hänvisar till den aktuella EU-förordningen om rapportering av integritetsincidenter.

PTS kommentar: PTS har infört en ytterligare bestämmelse i 17 kap. som hänvisar till den aktuella EU-förordningen. PTS har även förtydligat rubriken.

Energimyndigheten uppger att krav på incidentrapportering är bra och den styrande regleringen från EU har många likheter med exempelvis NIS, så även föreskrifterna. Men på sikt borde kanske målsättningen vara att incidentrapporteringen ska samordnas med MSB, i form och/eller kanal. Detta då vissa av subjekten riskerar att hamna under parallella och kanske överlappande krav på rapportering för samma incident, men även för att minska bördan generellt.

PTS kommentar: PTS har genom bestämmelserna i LEK fått i uppdrag att hantera rapportering av säkerhets- och integritetsincidenter. Det är sannolikt att behovet av samverkan mellan olika myndigheter kommer öka ytterligare. Det är dock inte en fråga som kan lösas inom detta föreskriftsarbete.

4.16.2 Tröskelvärden för rapportering av säkerhetsincidenter (17 kap. 5 §)

Region Värmland anser att tröskelvärden för rapportering av säkerhetsincident är för höga enligt förslaget och att det bör vara möjligt med ett inrapporteringssystem även för mindre nätägare och mindre omfattande incidenter. Ett högt tröskelvärde för rapportering riskerar att, precis som idag, ge en för avgränsad verklighetsbild.

PTS kommentar: Av 8 kap. 3 § nya LEK framgår att det är säkerhetsincidenter som haft betydande påverkan på nät och tjänster som ska rapporteras. Omständigheter som särskilt har betydelse för bedömningen av om en säkerhetsincident har haft en betydande påverkan är t.ex. antalet drabbade användare, storleken på det drabbade geografiska området och hur länge säkerhetsincidenten varar. PTS noterar Region Värmlands synpunkt men bedömer att tröskelvärdena är väl avvägda och ändamålsenliga.

4.16.3 Rapporteringsplikt vid betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället (17 kap 6 §)

Tre uppger följande. I 6 § introduceras en ny bestämmelse som ska omfatta andra rapporteringspliktiga säkerhetsincidenter med betydande påverkan på nätet eller tjänstens funktion. Bestämmelsen innehåller inte några trösklar för vad som är betydande påverkan och saknar även en närmare förklaring vad som avses med

nätets eller tjänstens ”funktion”. Det som torde kunna uteslutas är sådana säkerhetsincidenter som också kan utgöra integritetsincidenter, eftersom med nätets och tjänstens funktion torde PTS avse något annat än sådan påverkan som rör uppgifternas konfidentialitet. Dessa händelser ska istället rapporteras enligt 8 kap 8 § nya LEK. PTS behöver dock tydliggöra vad som avses med ”nätets och tjänstens funktion”; om det avser något annat än tillgängligheten (dvs störning och avbrott) men också vad PTS menar med ”betydande påverkan på funktion*er* i samhället”. Vad är ”funktioner i samhället”? Den sistnämnda indikerar att incidenten ska påverka flera funktioner i samhället för att vara rapporteringspliktig, men det är oklart om det är PTS avsikt.

I första ledet förutsätts en bedömning av säkerhetsincident och i andra ledet en bedömning av om händelsen har haft en betydande påverkan på tjänstens funktion eller ytterst om händelsen påverkat några samhällsfunktioner och om påverkan har varit betydande. När bestämmelsen har en så vag utformning och kan tolkas på flera olika sätt, vilket riskerar att leda till olika tolkningar hos tillhandahållarna, blir det svårt att tillämpa den i praktiken. Att bestämmelsen sedan kan ligga till grund för sanktionsavgift i händelse av att incidenten inte rapporteras framstår då både som högst olämpligt och oproportionerligt.

Bestämmelsen bör strykas. Om formuleringen trots detta behövs enligt PTS, måste den förtydligas med en beskrivning av vad PTS menar är en ”betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället.”

Tre avstyrker förslaget i 6 §.

Tele2 uppger bl.a. följande. Säkerhetsincidenter, enligt 17 kap. 6 §, ska rapporteras om de har haft ”betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället”. Vad PTS avser med detta framgår inte, vare sig av Förslaget eller konsekvensutredningen. Detta trots att PTS i konsekvensutredningen anför att det ska ”anges under vilka förutsättningar detta ska ske”.

Eftersom ett elektroniskt kommunikationsnät såväl som en elektronisk kommunikationstjänst har till huvudsaklig – om inte enda – uppgift i samhället att just tillhandahålla elektroniska kommunikationstjänster, är det enligt Tele2 svårt att se framför sig vilka andra säkerhetsincidenter än större störningar eller avbrott som skulle ha ”betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället”. För att säkerställa rätt tillämpning av 17 kap. § 6 Förslaget bör PTS därför konkretisera, eller minst exemplifiera, vilka incidenter – och då andra incidenter än störningar och avbrott – som har en ”betydande påverkan på nätets eller tjänstens funktion eller funktioner i samhället”.

PTS kommentar: PTS har förtydligat formuleringen i 17 kap. 6 §. Vägledning finns också i ENISA:s vägledning om rapportering av incidenter under Kodexen.[8]

5. Avslutning

PTS vill tacka samtliga remissinstanser för inkomna synpunkter.

[8] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu)