Förvaltningsutskottet

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet)

Till kommunikationsutskottet

INLEDNING

Remiss

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet) (RP 57/2024 rd): Ärendet har remitterats till förvaltningsutskottet för utlåtande till kommunikationsutskottet.

Sakkunniga

Utskottet har hört
- specialsakkunnig Marko Priiki, kommunikationsministeriet
- lagstiftningsråd Eeva Lantto, finansministeriet
- polisinspektör Kimmo Ulkuniemi, Polisstyrelsen
- specialsakkunnig Hanna Menna, Välfärdsområdesbolaget Hyvil Ab
- specialsakkunnig Martti Setälä, Finlands Kommunförbund.

Skriftligt yttrande har lämnats av
- inrikesministeriet
- dataombudsmannens byrå
- skyddspolisen
- Helsingfors stad
- Västra Nylands välfärdsområde
- Vanda och Kervo välfärdsområde
- Ålands landskapsregering.

UTSKOTTETS ÖVERVÄGANDEN

Propositionens utgångspunkter

I propositionen föreslår regeringen att det stiftas en cybersäkerhetslag. Dessutom ska flera andra lagar ändras, såsom lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen). Lagen föreslås bli kompletterad med bestämmelser

om sektorn offentlig förvaltning. Genom de föreslagna lagarna genomförs EU-direktivet om cybersäkerhet[1], som syftar till att stärka EU:s gemensamma och medlemsstaternas nationella cybersäkerhetsnivå med avseende på sektorer som är viktiga för samhällsverksamheten.

Förvaltningsutskottet förordar det tillvägagångssätt som valts i propositionen, där det nationella handlingsutrymmet har använts så att genomförandet av direktivet föreslås ske på det sätt som miniminivån förutsätter i fråga om både tillämpningsområde och skyldigheter.

Förvaltningsutskottet välkomnar genomförandet av och syftena med cybersäkerhetsdirektivet och konstaterar att de samordnade skyldigheterna i fråga om riskhanteringen inom cybersäkerheten och anmälan om betydande incidenter förtydligar och främjar cybersäkerhetsåtgärderna i de olika organisationerna.

Sektorspecifik tillsyn

Inom förvaltningsutskottets fackområde framträder informationshanteringslagen som den viktigaste lagen i fråga om välfärdsområdenas verksamhet. Lagen innehåller bestämmelser om skyldigheterna inom den offentliga förvaltningen och tillsynen över att skyldigheterna iakttas. Å andra sidan kan en myndighet som omfattas av informationshanteringslagens tillämpningsområde i vissa situationer, såsom välfärdsområdena i fråga om hälsovårdssektorn, också omfattas av cybersäkerhetslagens tillämpningsområde. Välfärdsområdena är verksamhetsmässigt uppdelade i social- och hälsovård och räddningsväsende.

Förvaltningsutskottet konstaterar att tillsynsuppgifterna inom välfärdsområdena som sagt är sektorsvis uppdelade på många myndigheter. Enligt informationshanteringslagen får Transport- och kommunikationsverket utfärda närmare föreskrifter och anvisningar för aktörerna. Med stöd av speciallagstiftningen meddelar också olika myndigheter, såsom Valvira och Fimea, närmare anvisningar och föreskrifter om välfärdsområdena och utövar tillsyn över dem. Förvaltningsutskottet konstaterar att detta är förenat med en risk för att myndigheterna utfärdar överlappande och motstridiga föreskrifter.

Utskottet betonar att välfärdsområdena och tillsynsmyndigheterna bör vara införstådda med hur den sektorspecifika tillsynen riktas i fråga om välfärdsområdenas funktioner. Det är viktigt att myndighetstillsynen över välfärdsområdena och andra aktörer i alla situationer är jämförbar och att tolkningarna av fullgörandet av skyldigheterna är tydliga och enhetliga också när det finns flera tillsynsmyndigheter. Särskild uppmärksamhet bör fästas vid att myndighetstillsynen ska vara enhetlig och jämförbar och att tillsynsmyndigheterna ska samarbeta.

Anmälningar till tillsynsmyndigheterna

Som det konstateras ovan föreslås det i propositionen nya tillsynsuppgifter sektorsvis för flera myndigheter. I propositionen föreslås det att de aktörer som omfattas av lagens tillämpningsom-

1 Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

råde ska lämna sina uppgifter till tillsynsmyndigheten, som i sin tur ska lämna uppgifterna till en gemensam kontaktpunkt. Kontaktpunkten anmäler uppgifterna vidare bland annat till Europeiska unionens cybersäkerhetsbyrå.

Enligt förslaget ska aktören också underrätta tillsynsmyndigheterna om betydande incidenter inom 24 timmar från det att incidenten upptäcktes. EU:s allmänna dataskyddsförordning (EU) 2016/679[2] har redan tidigare ålagt personuppgiftsansvariga en skyldighet att inom 72 timmar rapportera till dataombudsmannen om personuppgiftsincidenter som de har upptäckt. Anmälningsskyldigheter som gäller aktörsfältet finns också i stor utsträckning till exempel i den nyligen genomförda förordningen om artificiell intelligens (EU) 2024/1689[3] och i lagen om skydd för personer som rapporterar om överträdelser av EU-rätten och den nationella lagstiftningen (1171/2022).

Förvaltningsutskottet påpekar för kommunikationsutskottet att praxis och metoder för anmälan för närvarande skiljer sig från varandra för varje tillsynsmyndighet och att samma incident kan utlösa flera anmälningsskyldigheter samtidigt.

Utskottet lyfter i detta sammanhang fram att anmälningar om olika nya tekniker, säkerhet och dataskydd kunde centraliseras till en enda datasäker rapporteringskanal. Då minskar de rapporteringsskyldiga aktörernas administrativa börda och kostnaderna för att ha flera parallella datasäkra rapporteringskanaler. Samtidigt främjas också informationsutbytet mellan myndigheterna och en faktisk samordning mellan tillsynsmyndigheterna.

Förvaltningsutskottet påpekar vidare att enligt 17 § 3 mom. i den föreslagna cybersäkerhetslagen ska tillsynsmyndigheten underrätta polisen om att en betydande incident upptäckts, om det på grundval av aktörens anmälan finns skäl att misstänka ett brott för vilket det föreskrivna maximistraffet är fängelse i minst tre år. Utskottet anser att den föreslagna anmälningsskyldigheten är en bra ändring. En stor del av de uppsåtliga gärningarna i cybermiljön är cyberbrott, och det är därför naturligt att tillsynsmyndigheten är skyldig att anmäla grova informations- och kommunikationsbrott till polisen. Tröskeln för skyldigheten att anmäla misstänkta brott är på rätt nivå. Däremot bör den formulering som lyder ”skäl att misstänka ett brott” och som ligger till grund för anmälningsskyldigheten övervägas i syfte att det inte ska krävas att den som handlägger anmälan ska göra en rättslig prövning av om tröskeln för ”skäl att misstänka ett brott” överskrids eller inte.

Samtidigt konstaterar utskottet dock att motsvarande formulering används också i 316 § i lagen om tjänster inom elektronisk kommunikation (917/2014), där det föreskrivs om Transport- och kommunikationsverkets rätt att få uppgifter om kommunikation. Om bestämmelsen ändras kan en alternativ formulering vara ”det kan antas att ett brott har skett”. Samma uttryck används också i den föreslagna 16 §, så det bör övervägas om även den paragrafen behöver ändras. Enligt ut-

2 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)

3 Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordningen om artificiell intelligens)

redning till utskottet har det i diskussionerna mellan polisen och andra aktörer befarats att aktörerna inom den offentliga förvaltningen och den privata sektorn kan ha svårt att bedöma vad som avses med uttrycket ”skäl att misstänka” och hur man ska ställa sig till det i förhållande till den upptäckta händelsen.

Tillsynsmyndigheternas samarbete och resurser

Av propositionen framgår det att det inte kommer att anvisas tilläggsresurser för samarbetet mellan myndigheterna, utan samarbetet ses i den föreslagna lagstiftningen som en angelägenhet som kan skötas med nuvarande resurser trots att tillsynsverksamhet nu också ska bedrivas av nya myndigheter som inte har erfarenhet av tillämpningen av de gällande lagarna om cybersäkerhet. Förvaltningsutskottet anser det viktigt att samordningen, informationsutbytet och samarbetet mellan tillsynsmyndigheterna ordnas och tilldelas resurser på riksnivå så att tillsynen är av samma kvalitet inom de olika sektorerna.

FÖRSLAG TILL BESLUT

Förvaltningsutskottet föreslår

att kommunikationsutskottet beaktar det som sägs ovan.

Helsingfors 19.9.2024

I den avgörande behandlingen deltog

ordförande Mauri Peltokangas saf
vice ordförande Pihla Keto-Huovinen saml
medlem Alviina Alametsä gröna
medlem Petri Honkonen cent
medlem Juha Hänninen saml
medlem Christoffer Ingo sv
medlem Mari Kaunistola saml
medlem Anna Kontula vänst
medlem Rami Lehtinen saf
medlem Mira Nieminen saf
medlem Saku Nikkanen sd
medlem Eemeli Peltonen sd
medlem Paula Werning sd
medlem Ben Zyskowicz saml
ersättare Jari Ronkainen saf.

Sekreterare var

plenarråd Sanna Helopuro.