



Polismyndigheten
Rättsavdelningen

Finansdepartementet
i.remissvar@regeringskansliet.se

Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

Polismyndigheten tillstyrker att förslaget genomförs.

Polismyndigheten lämnar emellertid vissa synpunkter på förslaget.

Polismyndigheten tolkar innehållet i och syftet med den föreslagna förordningen som att myndigheten inte kommer ses som en ekonomisk aktör, exempelvis vid inköp av teknikprodukter från tredje land som uteslutande ska användas inom myndigheten. På samma sätt uppfattar myndigheten att förordningen inte omfattar den situationen att Polismyndigheten utvecklar egen teknik som endast ska användas inom myndigheten. Eftersom Polismyndigheten är slutanvändare av produkter som köps in kan myndigheten inte heller rimligen ses som distributör i den mening som avses i förordningen. Begreppet ”tillhandahållande på marknaden” förutsätter att förfarandet sker inom ramen för kommersiell verksamhet. Samma definitioner återfinns i *New Legislative Framework (NLF)* som förordningsförslaget baseras på.¹ Det är emellertid angeläget att dessa tolkningar verifieras och Polismyndigheten efterfrågar därför ett förtydligande kring förordningens tillämpningsområde.

Om det trots allt är så att Polismyndigheten i något avseende skulle anses omfattas av förordningen så anser myndigheten att det bör införas undantag. Polismyndighetens operativa verksamhet kan t.ex. komma att behöva köpa in ny teknik med kort varsel från tredje land. Ett tidskrävande administrativt förfarande kan då komma att försämra den operativa förmågan.

Den föreslagna förordningen uppställer krav på rapporteringsskyldighet och transparens. Exempelvis ska tillverkare anmäla vissa sårbarheter till EU:s

¹ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG, kapitel R1, artikel R1.

cybersäkerhetsbyrå Enisa som i sin tur ska vidarebefordra information till nationella CSIRT-enheter. Det är för Polismyndigheten viktigt att det säkerställs att inga för myndigheten skyddsvärda metoder och förmågor röjs. Ett exempel är om en produkt tagits fram exklusivt för Polismyndigheten och den visar sig utgöra en betydande cybersäkerhetsrisk. Enligt Polismyndighetens uppfattning torde det då t.ex. inte finnas anledning för marknadskontrollmyndigheten att informera om det publikt. Det kan befaras att artikel 52 som behandlar konfidentialitet inte ger ett tillräckligt skydd mot röjande av känslig information. Samtidigt kan Polismyndigheten ha behov av att kunna ta del av material från marknadskontrollmyndigheten inom ramen för den brottsförebyggande och brottsutredande verksamheten på cyberområdet. Båda dessa intressen bör beaktas.

Enligt artikel 10 punkt 6 ska en tillverkare när en produkt med digitala element släpps ut på marknaden under viss tid säkerställa att produktens sårbarheter hanteras effektivt och i enlighet med de väsentliga krav som fastställs i avsnitt 2 i bilaga I. Det anges inte utifrån vilka kriterier eller av vem denna tidsrymd ska beräknas. Med tanke på att enskilda konsumenterna ofta använder hårdvara, som t.ex. routrar och TV-apparater, betydligt längre tid än fem år kan det ifrågasättas om inte tidsrymden är väl begränsad.

Detta yttrande har beslutats av juristen Tony Back efter föredragning av juristen Emilia Freij.

POLISMYNDIGHETEN

På avdelningschefens vägnar

Tony Back

Emilia Freij

Remissvaret har godkänts digitalt och saknar därför namnunderskrifter.

Kopia till:

Justitiedepartementet (PO)
Arbetslagarorganisationerna
Rikspolischefens kansli