Stockholms universitet

Rektor

BESLUT
2024-05-23 Dnr SU FV-0893-24

Rikard Skårfors
FD, Utbildningsledare
Rektors kansli, Ledningssekretariatet

Regeringskansliet (Försvarsdepartementet)

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

Stockholms universitet har av Regeringskansliet (Försvarsdepartementet) anmodats att inkomma med synpunkter på delbetänkandet av Utredningen om genomförande av NIS2- och CER-direktiven, *Nya regler om cybersäkerhet* (SOU 2024:18). Universitetet har följande att anföra.

Övergripande synpunkter

Stockholms universitet konstaterar att universitet och högskolor är undantagna från NIS2-direktivets tillämpningsområde och menar att lärosätena ska undantas även från den förslagna regleringen. En ny utredning bör tillsättas för att harmoniera de svenska lärosätenas cybersäkerhetsreglering med den som tas fram i andra länder inom EU. Stockholms universitet ställer sig därmed helt bakom det yttrande som Sveriges universitets- och högskoleförbund (SUHF) lämnar över betänkandet. I likhet med SUHF ser universitetet att lärosätena annars befaras ställas inför krav på administrativa och organisatoriska förändringar vars ekonomiska konsekvenser kommer att minska våra möjligheter att bedriva utbildning och forskning av högsta kvalitet.

Om regeringen ändå väljer att gå vidare med utredningens förslag framhåller Stockholms universitet samma synpunkter som SUHF tar upp i sitt yttrande:

- Undanta lärosäten med mindre omfattande forskning från cybersäkerhetsregleringen.
- Kategorisera lärosätena som viktiga verksamheter och minska därigenom den administrativa bördan.
- Det bör endast vara en myndighet som meddelar föreskrifter samt utövar tillsyn över lärosätena.
- Implementera NIS2-direktivets riskbaserade förhållningssätt i svensk cybersäkerhetsreglering.
- Alla lärosäten, oavsett huvudman, ska ha samma sanktionsbelopp.

Stockholms universitet

- Kompensera lärosätena för de stora ekonomiska kostnader som den nya regleringen kommer att medföra.

Specifika synpunkter

Riskanalys

Utredningen anger att ”syftet med en ny lag om cybersäkerhet är att uppnå en högre cybersäkerhet” (sammanfattning, s. 15). Det konstateras vidare att ”verksamhetsutövare ska vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. *Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas*” (s. 18).

Frågan är i vilken utsträckning lagförslaget, som i huvudsak berör administrativa aspekter såsom beskrivning av sektorer, incidentrapportering, allokering av ansvar mellan myndigheter, ingripande och sanktioner, bidrar till att tillgodose detta syfte. Skrivningen om en proportionell riskanalys återkommer i lagförslagets 3 kap 1 § (avsnitt 1.1, s. 41) där ytterligare några relativt självklara aspekter som ska vara föremål för analysen anges (incidenthantering, kontinuitetshantering, säkerhet i leveranskedjan, säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation m.fl.). Regler eller anvisningar om hur proaktiva riskanalyser ska genomföras saknas emellertid och det anges (avsnitt 12.6.1, s. 336) att ”tillsynsmyndigheterna får … meddela föreskrifter om säkerhetsåtgärder avseende riskanalyser, riskhanteringsåtgärder och incidenthantering enligt 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster för sina respektive tillsynsområden.” Paragrafer som likaledes är relativt intetsägande vad avser *riskanalys*.

En konsekvens av förslaget, som i jämförelse med befintlig reglering innebär att antalet myndigheter och aktörer som omfattas av lagen avsevärt utökas, är att regleringen av cybersäkerheten blir mer splittrad och besvärlig att förstå. Rimligen ökar även riskerna för uppkomsten av skilda rutiner mellan olika aktörer och sektorer, verksamheter som allteftersom kan komma att integreras. Frågor måste också ställas om hur pass väl underbyggda en del av förslagen är. Exempelvis motiveras förslaget om att utse länsstyrelserna till tillsynsmyndigheter för *forskning* på följande sätt (avsnitt 8.4.2, s. 224): ”Sektorn har ingen tydlig koppling till någon befintlig sektor eller tillsynsmyndighet i den nuvarande NIS-regleringen. Utredningen föreslår därför att länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län ska vara tillsynsmyndigheter i sektorn.” Samma myndigheter föreslås med liknande outvecklad argumentation som tillsynsmyndigheter för *lärosäten med examinationsrätt*. I vilken utsträckning dessa enheter besitter den kompetens som behövs framgår inte och konsekvensanalys rörande eventuella nödvändiga anpassningar saknas.

Eftersom även personkretsen utvidgas när fler aktörer involveras vill Stockholms universitet framhålla att riskerna för spridning av säkerhetskänslig information ökar – gediget

Stockholms universitet

genomförda riskanalyser utgör även checklistor för hur potenta cyberattacker kan designas. Innefattandet av fler aktörer som måste förhålla sig till regleringen medför samtidigt ett avsevärt pedagogiskt problem.

Lagskrivningsteknik

Utredningen presenterar inledningsvis en förteckning över uttryck och termer (avsnitt 1.1, ss. 33f.). Tanken är god och detta är i vanliga fall ett stöd för den som vill förstå en lagtext. Det aktuella regleringsområdets uppsplittrade natur framgår dock tydligt, nedan några exempel:

”2 § I lagen avses med

1. *allmän dataskyddsförordning:* 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.
2. *allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster:* begreppen har samma innebörd som i lagen (2022:482) om elektronisk kommunikation,
3. *betrodda tjänster:* begreppet har samma innebörd som i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. …”

Stockholms universitet menar att detta är en lagskrivningsteknik som inte bidrar till att underlätta läsningen. Att explicit förklara de begrepp som berörs i en text är ett grundkrav, hänvisningar till ursprungsdokumenten är nödvändiga men inte tillräckliga. Vidare kan formuleringar och uppdelningen av reglerna i olika paragrafer bearbetas för att bättre svara mot rimliga krav på klarspråk och begriplighet. Exempelvis kan paragraferna 12, 13, 14 och 15 i lagförslagets kapitel 5 (ss. 47f.) enkelt sammanföras.

Detta beslut är fattat av rektor, professor Astrid Söderbergh Widding, i närvaro av prorektor, professor Clas Hättestrand, och universitetsdirektör Åsa Borin. Studeranderepresentanter har informerats och haft tillfälle att yttra sig. Ärendet har beretts av Juridiska fakultetsnämnden. Övrig närvarande och föredragande i ärendet har varit Rikard Skårfors, Ledningssekretariatet (protokollförare).