Sveriges universitets-
och högskoleförbund
Tryckerigatan 8
111 28 Stockholm

2024-05-23
Dnr SU-850-0029-24
YTTRANDE

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

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

Sveriges universitets- och högskoleförbund (SUHF) har givits möjligheten att yttra sig över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) (NIS2), dnr Fö2024/00496.

Inledning

SUHF önskar i första hand att lärosätena ska undantas från den föreslagna regleringen och en kompletterande utredning beträffande lärosätenas cybersäkerhet tillsätts. Detta då utredningens förslag beträffande lärosäten är ett tydligt exempel på överimplementering av EU-lagstiftning och riskerar att skada svensk forskning och utbildning. SUHF:s synpunkter lämnas således mot bakgrund av att universitet och högskolor är undantagna från NIS2-direktivets tillämpningsområde, att utredningen inte på ett tillfredsställande sätt förhåller sig till den forskning som faktiskt bedrivs på svenska lärosäten, och som en konsekvens lämnar förslag som inte är balanserade beträffande den cybersäkerhet som behöver uppnås och den administration som skapas. De ekonomiska konsekvenserna av ökad administration kommer att minska svenska lärosätens möjligheter att bedriva utbildning och forskning av högsta kvalitet.

Sveriges lärosäten är väl medvetna om att de behöver stärka sin cybersäkerhet. Det är ett prioriterat arbete som bedrivs med kraft och cybersäkerheten höjs genom såväl administrativa åtgärder som genom att sätta av personella och ekonomiska resurser. SUHF välkomnar således en tydlig, kraftfull och stöttande reglering som stödjer detta arbete.

Sammanfattning

Sammanfattningsvis önskar SUHF i första hand att en kompletterande utredning beträffande lärosätenas cybersäkerhet tillsätts. I andra hand lämnar SUHF följande synpunkter:

- Undanta lärosäten med mindre omfattande forskning från cybersäkerhetsregleringen
- Kategorisera lärosätena som viktiga verksamheter och minska därigenom den administrativa bördan
- Det bör vara endast en myndighet som meddelar föreskrifter samt utövar tillsyn över lärosätena
- Implementera NIS2-direktivets riskbaserade förhållningssätt i svensk cybersäkerhetsreglering
- Alla lärosäten ska oavsett huvudman ha samma sanktionsbelopp
- Kompensera lärosätena för de stora ekonomiska kostnader som den nya regleringen kommer att medföra

Utredningens förslag om cybersäkerhetsreglering bör inte omfatta lärosätena och en kompletterande utredning tillsättas

- *SUHF menar att utredningen gjort en stor insats som på kort tid behövt lägga tekniskt komplicerade förslag som täcker många sektorer. SUHF konstaterar dock att förslaget innebär överimplementering av EU-lagstiftning och att utredningens förståelse för lärosätenas verksamhet brister. SUHF anser det avgörande att lärosätena generellt omfattas av en tydlig, kraftfull och stödjande cybersäkerhetsreglering, men en kompletterande utredning bör tillsättas som harmonierar de svenska lärosätenas cybersäkerhetsreglering med den som tas fram i andra medlemsstater.*

NIS2-direktivet syftar till att förbättra den inre marknadens funktion. Det är mot denna bakgrund som utbildningsinstitutioner som universitet och högskolor **inte** omfattas av NIS2-direktivets tillämpningsområde; den inre marknaden kommer inte att fungera bättre för att lärosätena i unionen har en gemensam cybersäkerhetsnivå. Däremot anger NIS2-direktivet att ”Medlemsstaterna får föreskriva att detta direktiv ska tillämpas på … utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet” (Artikel 2.5). Regeringens direktiv till utredningen är också i linje med detta: ”Utredaren ska mot denna bakgrund överväga om universitet och högskolor, eller ett urval av dessa, bör omfattas av den nya regleringen.”

Trots att utredningen konstaterar att den har möjlighet att föreslå ett undantag även för lärosäten med staten som huvudman så föreslår utredningen att lärosätena ska inkluderas i regleringen. Detta innebär en överimplementering av EU-lagstiftning.

Begreppet överimplementering syftar på att när stater ska genomföra EU-direktiv så utökar staterna sina egna nationella regler i sin iver att följa EU-direktiven. Sverige anses i detta sammanhang ha en tendens att vara bäst i klassen och därmed gå bortom direktivens syfte och skapa alltför tung administration, det vill säga överimplementera. Regeringen är bekymrad och anger därför i vårbudgetpropositionen för 2023 ”Ett implementeringsråd kommer att inrättas med syfte att undvika överimplementering av EU-direktiv och därigenom motverka omotiverade regelbördor.” Regeringen kan redan nu begränsa överimplementeringen av NIS2-direktivet.

Utredningen anför i huvudsak två argument för att lärosäten ska inkluderas i regleringen. Det första är att

Forskning är en egen sektor i NIS2-direktivet som inte innefattar utbildningsinstitutioner. Att relativt liten andel av forskningen i Sverige bedrivs i forskningsinstitut talar enligt utredningen för att inkludera lärosäten i regleringen. Resultatet skulle annars bli att en större del av den forskning som bedrivs i Sverige inte skulle omfattas av NIS2-direktivet. Detta skulle gå emot direktivets syfte.

Utredningen har haft kort tid på sig att lämna ett delbetänkande om regleringar som täcker många sektorer. SUHF bedömer att utredningen utifrån dessa förutsättningar har gjort en stor insats, men konstaterar att det inte heller är konstigt om blivit fel i beskrivningen av olika verksamheter.

”Forskning” urskiljs i NIS2-direktivet som en egen sektor, men avgränsas där till att beröra ”verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning eller experimentell

utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner". Forskning i detta avseende utförs endast i mycket begränsad utsträckning på svenska lärosäten i. Den forskning NIS2-direktivet tar sikte på ingår följaktligen inte i lärosätenas ordinarie verksamhet, varför den argumentation som framförs i betänkandet inte heller är i linje med direktivets avsikt.

Utredningens påstående att lärosätena bör omfattas av cybersäkerhetsregleringen därför att motsatsen skulle gå emot direktivets syfte är uppenbart felaktigt eftersom forskning vid lärosäten inte är ett av NIS2-direktivets tillämpningsområden. Utredningen för i sammanhanget ett resonemang om att det bedrivs omfattande forskning vid Sveriges lärosäten. Detta resonemang förstärker emellertid inte utredningens slutsats att svenska lärosäten bör omfattas av regleringen. Detta då det givetvis bedrivs omfattande forskning även vid andra EU-länders lärosäten; det är universitets själva grundidé. Anledningen till att NIS2-direktivet preciserar sektorn "forskning" som "forskning i kommersiellt syfte", är att den forskning som bedrivs vid lärosätena i unionen endast i mycket begränsad utsträckning har bäring på den inre marknadens funktion.

Utredningens andra argument för att inkludera lärosätena i regleringen tar avstamp i en rapport från Riksrevisionen. Rapportens övergripande slutsats är att lärosätena inte bedriver ett effektivt informationssäkerhetsarbete för att skydda forskningsdata. Lärosätena tar Riksrevisionens rapport på mycket stort allvar och vidtar åtgärder utifrån den. Det ligger dock i sakens natur att det är svårare att på ett universitet med tusentals forskningsprojekt med helt olika typer av information bedriva ett effektivt informationssäkerhetsarbete, än vad det är på myndigheter med mer avgränsade typer av information. Det bör samtidigt också påpekas att det inte finns några indikationer på att lärosäten, trots rimligtvis större svårigheter att bedriva ett effektivt informationssäkerhetsarbete, i relation till andra myndigheter har haft fler läckor av skyddsvärd information eller har varit mindre framgångsrika i att avvärja cyberattacker.

SUHF menar vidare att utredningen förbisett tre viktiga aspekter.

Den första aspekten är den framskrivning som sker i såväl NIS2-direktivet som i regeringens direktiv om att medlemsstaterna får föreskriva att detta direktiv ska tillämpas på utbildningsinstitut, *särskilt om de utför* ***kritisk*** *forskningsverksamhet*" (Artikel 2.5). NIS2-direktivet definierar inte "kritisk forskningsverksamhet", men det står klart att även med en vidsträckt definition skulle endast en liten andel av forskningen vid svenska lärosäten bedömas som "kritisk".

Den andra aspekten är att utredningen i sammanhanget helt saknar överväganden beträffande regeringens tydliga direktiv: "Utgångspunkten för utredarens arbete ska dock vara att förslagen utformas så att regelbördan och administrationen för berörda entiteter minimeras."

Den tredje aspekten är att det är oklart i vilken utsträckning som andra medlemsstater låter lärosätena omfattas av NIS2-direktivet. Om Sverige blir ett av få länder som gör det riskerar Sverige att bli mindre attraktivt som samarbetspartner för forskare i andra länder; något som givetvis är direkt skadligt för svensk forskning. SUHF anser det avgörande att lärosätena generellt omfattas av en kraftfull och stödjande cybersäkerhetsreglering, men en kompletterande utredning bör tillsättas som harmonierar de svenska lärosätenas cybersäkerhetsreglering med den som tas fram i andra medlemsstater.

Om regeringen väljer att gå vidare med utredningens övergripande förslag lämnar SUHF nedan specifika förslag som i delar minskar den överimplementering som utredningens förslag skulle innebära.

Undanta lärosäten med mindre omfattande forskning från cybersäkerhetsregleringen

- *SUHF anser att cybersäkerhetsregleringen endast bör omfatta lärosäten som har minst 50 anställda forskare eller vars omsättning eller balansomslutning för forskning eller utbildning på forskarnivå överstiger 10 miljoner euro per år.*

Utredningen föreslår att utöver lärosäten med staten som huvudman så ska regleringen även omfatta icke-statliga lärosäten som uppfyller storlekskravet på minst 50 anställda eller har en omsättning eller balansomslutning som överstiger 10 miljoner euro per år. Anledningen anges vara att det annars blir en omotiverad skillnad mellan lärosäten som bedrivs med staten som huvudman respektive de som inte gör det.

Utredningens resonemang om att alla lärosäten bör omfattas eftersom det annars blir ”en omotiverad skillnad” hade kunnat problematiseras. Anledningen till att staten har avsagt sig huvudmannaskapet för några av de svenska lärosätena är givetvis att det ska finnas skillnader; annars kunde ju staten ha behållit huvudmannaskapet.

Om man likväl accepterar premissen att alla lärosäten – vare sig de har staten som huvudman eller inte – bör omfattas av samma regelverk kan förhållningssättet emellertid vara det omvända. I stället för att utöka antalet lärosäten som omfattas av NIS2-direktivet kan det minskas.

Implementeringen av regleringen kommer att innebära stora kostnader och ökad administrativ börda. Detta kommer i synnerhet bli kännbart på de mindre lärosätena. Stockholms Musikpedagogiska Institut (SMI) är ett konkret exempel på ett lärosäte vars verksamhet är så långt ifrån NIS2-direktivets syfte som tänkas kan. Vid SMI bedrivs inte någon forskning och år 2023 redovisade SMI 174 studenter (70 helårsstudenter). Det statliga bidraget uppgår till 17,6 Mkr. SMI har dock ett stort antal inriktningar vilket gör att det engageras 64 lärare där den överväldigande majoriteten arbetar deltid, motsvarande 16 helårsverken. Men trots verksamhetens mycket blygsamma omfattning så föreslår alltså utredningen att SMI ska omfattas av regleringen.

Utredningens förslag om att lärosäten med minst 50 anställda ska omfattas av regleringen bottnar sannolikt utifrån en uppfattning om att det vid alla lärosäten bedrivs en omfattande forskning (med kommersiellt syfte).

Av de 49 lärosäten som har examenstillstånd är det emellertid inte bara SMI som inte har någon eller mycket begränsad forskning. I nedanstående tabell anges de 18 lärosäten som har lägre intäkter än 10 miljoner euro per år för forskning och utbildning på forskarnivå.

Lärosäte	Intäkter forskning och utbildning på forskarnivå, tusentals kronor
Skandinaviens Akademi för Psykoterapiutveckling*	
Svenska institutet för kognitiv psykoterapi*	
Beckmans designhögskola	0

Ericastiftelsen	0
Gammelkroppa skogsskola	0
Johannelunds teologiska högskola	0
Newmaninstitutet	0
Stockholms Musikpedagogiska Institut	0
Örebro teologiska högskola	1890
Enskilda Högskolan Stockholm	8949
Röda Korsets högskola	15063
Kungl. Konsthögskolan	20507
Konstfack	26958
Sophiahemmet högskola	30197
Kungl. Musikhögskolan i Stockholm	32573
Marie Cederschiöld högskola	41964
Stockholms konstnärliga högskola	60979
Gymnastik- och idrottshögskolan	68019

Källa: Högskolan i siffror https://www.uka.se/vara-resultat/statistik/hogskolan-i-siffror
För lärosäten markerade med * saknas uppgifter om intäkter, men forskningen är mycket begränsad. Observera att i dessa intäkter ingår OH samt infrastruktur

Förutom att de 18 lärosätena inte bedriver någon forskning eller endast gör det i mindre utsträckning kan det konstateras att det knappast är något av dem som bedriver en ”kritisk forskningsverksamhet”.

Kategorisera lärosätena som viktiga verksamheter och minska därigenom viss administration

- *SUHF menar att lärosätena bör definieras som viktiga verksamheter och därmed kan den administrativa bördan minskas.*

NIS2-direktivet gör en distinktion mellan ”väsentliga” och ”viktiga” verksamheter. Utredningens förslag följer denna distinktion vilken innebär att medan väsentliga verksamheter måste vidta mer omfattande tillsynsåtgärder, behöver viktiga verksamhetsutövare endast vidta tillsynsåtgärder när tillsynsmyndigheten har befogad anledning att anta att regelverket inte följs. Observera att oavsett om en verksamhet är viktig eller väsentlig så ska verksamheterna vidta samma cybersäkerhetsåtgärder. Direktivets distinktion mellan väsentliga och viktiga verksamheter

speglar i vilken mån de är av kritisk betydelse med avseende på sektor eller de typer av tjänster de tillhandahåller samt deras storlek. … Tillsyns- och efterlevnadskontrollsystemen för dessa båda kategorier av entiteter bör differentieras för att säkerställa en rättvis balans mellan riskbaserade krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av efterlevnaden å den andra (skäl nr 15).

Mot bakgrund av NIS2-direktivets tydliga resonemang om att distinktionen ska spegla om en verksamhet är av kritisk betydelse är det anmärkningsvärt att utredningen föreslår att lärosätena ska betraktas som väsentliga.

Det bör vara bara en myndighet som meddelar föreskrifter samt utöver tillsyn över lärosätena

- *SUHF menar i första hand att det bör vara endast en myndighet som ges rätt att utöva tillsyn över lärosätena. Detta oaktat vilken verksamhet de bedriver inom ramen för forskning och utbildning samt tillhörande stödfunktioner. Vidare bör det endast vara en myndighet som ges rätt att meddela föreskrifter för riskhanteringsåtgärder för denna verksamhet.*
- *SUHF menar i andra hand att förordningen bör göras tydligare beträffande hur lärosäten och tillsynsmyndigheter ska avgöra vilka delar av verksamheten som ska underställas tillsyn från vilken myndighet, särskilt med avseende på verksamhet som kan omfattas av tillsyn från flera myndigheter, samt hur oförenliga krav från olika tillsynsmyndigheter ska hanteras.*

Flera av de stora lärosätena bedriver bred verksamhet och kan därför komma att underställas flera tillsynsmyndigheter. Majoriteten av lärosätena tillhandahåller studenthälsa och detta öppnar upp för tillsyn från Inspektionen för vård och omsorg. De som bedriver läkemedelsforskning enligt direktivets definition kan komma att underställas tillsyn från Läkemedelsverket. Några tillhandahåller molntjänster för forskning och skulle därmed kunna underställas tillsyn från Post- och telestyrelsen. Samtliga lärosäten ska även underställas tillsyn från någon av fyra länsstyrelser.

Utredningen tar fasta på att tillsyn av samma verksamhet från flera tillsynsmyndigheter är kostnadsdrivande och medför risk för oförenliga krav och sanktioner och föreslår att "om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde".

Förslaget klargör dock inte vilken myndighet som ska utöva tillsyn när hela verksamheten anges som en myndighets tillsynsområde och delar av den anges därutöver som en eller flera andra myndigheters tillsynsområden.

För lärosätena anges hela verksamheten som länsstyrelsernas tillsynsområde, medan integrerade verksamhetsområden, t.ex. studenthälsan, kan bli tillsynsområde för en annan myndighet, och delade funktioner som IT, HR, ekonomi, lokaler, ledningssystem, policys, och processer torde ingå i samtliga tillsynsmyndigheters tillsynsområden.

Situationen kompliceras ytterligare av att samtliga tillsynsmyndigheter (undantaget länsstyrelserna) samt Myndigheten för samhällsskydd och beredskap har rätt att meddela föreskrifter för verksamheten, och den rätten begränsas inte till delar av verksamheten. Även om det finns en målsättning att tillsynsmyndigheterna ska samordna sitt arbete är risken för oförenliga krav ändå mycket hög.

Implementera NIS2-direktivets riskbaserade förhållningssätt i all svensk cybersäkerhetsreglering

- *SUHF menar att NIS2-direktivets tydlighet kring proportionalitet och allriskansats tydligt bör skrivas in i de delar av Cybersäkerhetsregleringen som ger myndigheter rätt att meddela föreskrifter.*

NIS2-direktivets artikel 21 anger att medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga åtgärder för att hantera risker och understryker att åtgärderna ska baseras på en **allriskansats** och säkerställa en nivå på säkerheten som är lämplig i förhållande till den föreliggande risken – att de är proportionerliga mot riskexponering, konsekvenser, och sannolikhet för att incidenter inträffar.

För att riskhanteringsåtgärder ska vara effektiva, ändamålsenliga, och proportionerliga måste de utformas utifrån verksamhetens art, dess organisation, dess riskexponering, dess sårbarheter, och konsekvenserna av incidenter i verksamheten. Utformas riskhanteringsåtgärder utan denna hänsyn riskerar de bli otillräckliga, oproportionerliga, eller ej ändamålsenliga.

Som diskuterat är utredningens förslag ett tydligt exempel på så kallad överimplementering av EU-lagstiftning. Mycket talar för att generellt fortplantas sådan överimplementering, det vill säga att i nästa steg utfärdar myndigheter föreskrifter som går längre än EU-lagstiftningens syfte och i steget därefter går de berörda myndigheterna än längre i utfärdandet av interna styrdokument.

SUHF anser att det är viktigt att en ny cybersäkerhetsförordning tydligt tar fasta på risken för fortsatt överimplementering, det vill säga risken för föreskrifter som inte är proportionerliga eller ändamålsenliga med hänsyn till verksamhetens art. Direktivets tydlighet kring proportionalitet och allriskansats bör skrivas in i den förordningstext som ger myndigheterna rätt att meddela föreskrifter.

Alla lärosäten ska oavsett huvudman ha samma sanktionsbelopp

- *SUHF menar att om enskilda lärosäten med examenstillstånd ska omfattas av regleringen bör deras bötesbelopp vara i storlek med de lärosäten som har staten som huvudman*

Utredningen konstaterar att sanktionerna ska vara effektiva, proportionella och avskräckande. Den allvarligaste formen av ingripande kommer att kunna bestå av en kombination av förelägganden, förbud och sanktionsavgift. Av tabellen nedan framgår sanktionsbelopp för olika verksamhetsutövare.

Verksamhetsutövare	**Högst**	**Lägst**
Väsentlig	Det högsta av 2 procent av den utövarens globala årsomsättning föregående räkenskapsår, eller 10 000 000 euro	5 000 kr
Viktig	Det högsta av 1,4 procent av utövarens globala årsomsättning föregående räkenskapsår, eller 7 000 000 euro	5 000 kr
Offentlig	10 000 000 kr	5 000 kr

Av utredningen framgår att ett lärosäte med staten som huvudman ska bedömas som offentlig verksamhet och dessa kan därmed få en högsta sanktionsavgift om 10 miljoner kronor. Utredningens föreslår att lärosäten med examenstillstånd som inte har staten som huvudman och som har minst 50 anställda eller har en omsättning eller balansomslutning som överstiger 10 miljoner euro per år också ska omfattas av regleringen. Ett sådant lärosäte

kan emellertid knappast ses som offentlig verksamhetsutövare och kan därmed få ett avsevärt högre sanktionsbelopp än ett lärosäte med staten som huvudman. Utredningens resonemang om att det inte ska finnas omotiverade skillnader mellan lärosäten bör även omfatta sanktionsbeloppen.

Utredningen har ej tagit tillräcklig hänsyn till de ekonomiska konsekvenserna.

- *SUHF konstaterar att den nya regleringen kommer att medföra stora ekonomiska kostnader som lärosätena bör kompenseras för*

Utredningen föreslår att de ekonomiska konsekvenserna för införandet av NIS2-direktivet ska finansieras inom verksamhetsutövarens befintliga budgetram. Detta görs med hänvisning till att utredningen anser att förslagen medför besparingar för hela den offentliga sektorn. SUHF konstaterar att eventuella besparingar för hela den offentliga sektorn inte innebär att enskilda verksamhetsutövare kan realisera besparingar, och för lärosätena ser inte SUHF några troliga besparingar. Den enda konkreta besparing som utredningen pekar på är minskade kostnader genom att incidenter förhindras eller begränsas, men kostnaden för incidenter i sektorn är redan i dag mycket låg.

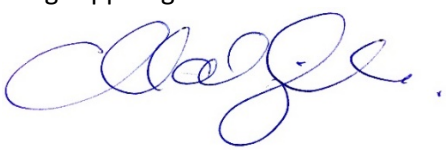
EU-kommissionens har gjort mer substantiella konsekvensbedömningar och dessa pekar på kraftigt ökade kostnader. För enskilda aktörer bedömer man att verksamheter kommer öka sina IKT-kostnader i genomsnitt med 22-25%, potentiellt öka sina kostnader för cybersäkerhet med 10-15%, odefinierade kostnader för tillsyn och granskningar, samt behöva i genomsnitt ytterligare 6-8 heltidsekvivalenter (incidentrapportering undantaget eftersom resurser till detta redan finns). (Källa: SWD(2020) 345 final del 2/3 sidan 63 och framåt).

SUHF bedömer dessa kostnader som i stort sett realistiska. Även om lärosätena sedan tidigare omfattas av krav på exempelvis systematiskt informationssäkerhetsarbete (MSBFS 2020:6) och riskhanteringsåtgärder (MSBFS 2020:7) har införandet av dessa åtgärder aldrig åtföljts av finansiering, och konsekvensbedömningarna som gjorts underskattar i vissa fall kostnaderna med flera storleksordningar. SUHF anser därmed att man inte kan hänvisa till dessa tidigare krav som skäl att inte finansiera införandet av NIS2-direktivet.

Sammantaget innebär det att om kraven i NIS2-direktivet ska införas inom befintliga budgetramar kommer det innebära att förhållandevis stora medel måste tas från forskning och undervisning, vilket undergräver Sveriges utveckling som ledande innovations- och kunskapsnation.

Yttrandet har beretts av en särskild arbetsgrupp utsedd av Expertgruppen för fastighets- och säkerhetsfrågor.

Enligt uppdrag



Marita Hilliges
generalsekreterare