

Webbinarium angående cybersäkerhetslagens tillämpningsområde

Sektor: hälso- och sjukvård (vårdgivare)

Entiteter	Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 2022/2371 Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2 Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123
Vid lärosätena	Studenthälsan, psykologmottagningar, tandläkarmottagningar, ögonmottagningar, m.m.



En sektor som de flesta lärosäten kan påverkas av är hälso- och sjukvård. De flesta har egen studenthälsovård och i vissa bedriver någon form av mottagning bemannad av studenter, till exempel en psykologmottagning eller tandläkarmottagning, och eventuellt kan ses som vårdgivare. Det finns även lärosäten som bedriver forskning och utveckling avseende läkemedel.

Varje lärosäte behöver själv bedöma om man har verksamhet passar in i direktivets olika definitioner. Det är helt förväntat att olika lärosäten kommer att bedöma exempelvis sin studenthälsa på olika sätt eftersom man har olika tjänster och bemanning. Det är alltså inte riktigt lika viktigt att sektorn är enig i sina slutsatser kring hälso- och sjukvård som kring offentlig förvaltning, men viss enlighet i övergripande angreppssätt vore fördelaktigt.

Sektor: hälso- och sjukvård (vårdgivare)

Definition¹

Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU

vårdgivare: varje fysisk eller juridisk person eller varje annan entitet som lagligen bedriver hälso- och sjukvård på en medlemsstats territorium.

hälso- och sjukvård: hälso- och sjukvårdstjänster som hälso- och sjukvårdspersonal tillhandahåller patienter i syfte att bedöma, bibehålla eller återställa deras hälsotillstånd, inbegripet förskrivning, utlämning och tillhandahållande av läkemedel och medicinska hjälpmedel.

patient: varje fysisk person som ansöker om eller får hälso- och sjukvård i en medlemsstat.

hälso- och sjukvårdspersonal: läkare, sjuksköterska med ansvar för allmän hälso- och sjukvård, tandläkare, barnmorska eller farmaceut i den mening som avses i direktiv 2005/36/EG eller annan person som utövar yrkesverksamhet inom hälso- och sjukvård som är begränsad till ett reglerat yrke enligt definitionen i artikel 3.1 a i direktiv 2005/36/EG, eller en person som anses som hälso- och sjukvårdspersonal enligt den behandlande medlemsstatens lagstiftning.

Det är viktigt att alltid ha i åtanke att det är NIS 2-direktivets definition av "vårdgivare" som ska användas, inte exempelvis patientsäkerhetslagens. Definitionerna skiljer sig lite åt, och de är fullt möjligt att vara vårdgivare enligt patientsäkerhetslagen men inte enligt NIS 2-direktivet och vice versa.

Definitionen av vårdgivare återfinns i artikel 3 i direktiv 2011/24/EU och för att uttolka den får man kombinera flera olika definitioner. Antar man att alla lärosäten är att betrakta som juridiska personer och att eventuell vård bedrivs lagligen, och att de som vårdas är att betrakta som patienter så kvarstår två saker för att avgöra om en verksamhet är att betrakta som vårgivare:

- Tillhandahåller man hälso- och sjukvårdstjänster *enligt definitionen i EU-regleringen?*
- Tillhandahålls tjänsterna av hälso- och sjukvårdspersonal *enligt definitionen i EU-regleringen?*

Bedömningarna kommer att skifta från verksamhet till verksamhet. Det vore dock fördelaktigt att de lärosäten som anser att de erbjuder hälso- och sjukvårdstjänster inte grundar sin bedömning enbart på exempelvis föreläsningar om hälsa, eller enklare enskilt coaching eller samtalsstöd, utan även identifierar annan verksamhet som ännu tydligare är hälso- och sjukvård. Det råder olika syn på den typen av tjänster inom sektorn, och det underlättar för övriga lärosäten om flexibiliteten att bedöma dem på olika sätt kvarstår.

Sektor: hälso- och sjukvård (vårdgivare – studenthälsa)

Bedömning	Hälso- och sjukvårdstjänster och tillhandahålls av utpekad personal
Tjänster	Är tjänsterna som tillhandahålls hälso- och sjukvårdstjänster? • Vilka tjänster som tillhandahålls varierar mellan lärosäten!
Personal	Tillhandahålls tjänsterna av utpekad personal? • Läkare, sjuksköterska med ansvar för allmän hälso- och sjukvård, tandläkare, barnmorska eller farmaceut i den mening som avses i direktiv 2005/36/EG? • Annan person som utövar yrkesverksamhet inom hälso- och sjukvård som är begränsad till ett reglerat yrke enligt definitionen i artikel 3.1 a i direktiv 2005/36/EG? • En person som anses som hälso- och sjukvårdspersonal enligt Svensk lagstiftning?



Studenthälsan är den verksamhet som har diskuterats mest i detta sammanhang eftersom det berör alla lärosäten.

Det första steget i bedömningen av studenthälsan är att se till vem som tillhandahåller tjänsterna. Många lärosäten driver studenthälsa i egen regi, men det finns även lärosäten som köper in den som tjänst eller lutar sig mot ett annat lärosätes studenthälsa. Dessa lärosäten kan inte betraktas som vårdgivare på grund av studenthälsan eftersom det är någon annan som tillhandahåller tjänsterna.

För de som driver studenthälsan i egen regi finns som nämnts två aspekter att bedöma: är tjänsterna som tillhandahålls att betrakta som hälso- och sjukvårdstjänster och tillhandahålls dem av hälso- och sjukvårdspersonal – *så som begreppen definieras i EU-regleringen*.

Hälso- och sjukvårdstjänster definieras inte på ett entydigt sätt i EU-lagstiftningen, men definitionen av hälso- och sjukvård anger att *syftet ska vara att "bedöma, bibehålla eller återställa deras hälsotillstånd, inbegripet förskrivning, utlämning och tillhandahållande av läkemedel och medicinska hjälpmedel"*. Det saknas även en definition av "hälsotillstånd", så där kan det också finnas visst utrymme för tolkning eller för att hänvisa till nationell lagstiftning.

Direktivet definierar hälso- och sjukvårdspersonal som någon av följande:

- Läkare, sjuksköterska, och andra roller med ansvar för allmän hälso- och sjukvård.
- Tandläkare, barnmorska eller farmaceut i den mening som avses i direktiv 2005/36/EG.

- Annan person som utövar yrkesverksamhet inom hälso- och sjukvård som är begränsad till ett reglerat yrke enligt en annan definition.
- Personer som anses som hälso- och sjukvårdspersonal enligt nationell lagstiftning.

Återigen måste varje lärosäte göra en egen bedömning, men om tjänsterna tillhandahålls av personal som inte ingår i någon av ovanstående kategorier, så uppfylls inte kriterierna för vårdgivare.

Förutom studenthälsan har flera lärosäten olika typer av mottagningar där studenter tillhandahåller exempelvis tandvård eller synundersökningar under överinsyn av kvalificerade handledare. Även här kan förutsättningarna skilja mellan olika lärosäten.

Sektor: hälso- och sjukvård (läkemedelsforskning)

Definition¹ Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG.

läkemedel: varje substans eller kombination av substanser som tillhandahålls för att behandla eller förebygga sjukdom hos människor, varje substans eller kombination av substanser som är avsedd att tillföras människor i syfte att ställa diagnos eller att återställa, korrigera eller modifiera fysiologiska funktioner.

Vid lärosätena: Beroende på forskningsområden.

Ytterligare en typ av verksamhet som ingår i hälso- och sjukvårdssektorn är forskning och utveckling avseende läkemedel.

Flera lärosäten bedriver forskning kring läkemedel, men direktivet anger forskning **och** utveckling avseende läkemedel, inte enbart forskning. Dessvärre finns ingen tydlig definition av "utveckling" i direktivet, men utveckling förstås i många sammanhang handla om att förädla ett resultat i syfte att möjliggöra kommersiell produktion. Bland de lärosäten som bedriver forskning kring läkemedel är det sannolikt bara en del som även bedriver utveckling avseende läkemedel. Var och en måste göra en bedömning utifrån sin egen verksamhet.

Sektor: digital infrastruktur

Definition	Leverantörer av internetknutpunkter Leverantörer av DNS-tjänster, med undantag för operatörer av rotnamnsservrar Registreringsenheter för toppdomäner Leverantörer av molntjänster Leverantörer av datacentraltjänster Leverantörer av nätverk för leverans av innehåll Tillhandahållare av betrodda tjänster Tillhandahållare av allmänna elektroniska kommunikationsnät Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster
Vid lärosätena	Förekommer vid enstaka lärosäten, främst: • Leverantörer av molntjänster • Leverantörer av datacentraltjänster

Några lärosäten kan beröras av sektorn digital infrastruktur, troligast som leverantörer av molntjänster eller datacentraltjänster.

Vid bedömningen av dessa tjänster bör man ta hänsyn till att EU i NIS 2-direktivet beskriver sådana leverantörer och tjänster som gränsöverskridande (exempelvis i skäl 84) och därför ser ett behov av harmoniserade regelverk. Hade man haft leverantörer med en begränsad lokal kundkrets, exempelvis det egna holdingbolaget, några få samarbetspartners, eller några andra lärosäten i åtanke så funnes ingen anledning att "uppnå en hög nivå av harmonisering på unionsnivå". Det finns alltså goda skäl att vara försiktig innan man bedömer att man är leverantör av molntjänster i NIS 2-direktivets mening.

Sektor: digital infrastruktur (molntjänster)

Definition ¹	En digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma beräkningstjänster, inbegripet när sådana resurser är distribuerade på flera platser. Beräkningsresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster.
Förtydligande	Tjänstemodellerna för molntjänster omfattar bland annat infrastruktur som en tjänst, plattform som en tjänst, program som en tjänst och nätverk som en tjänst. Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. Molntjänste- och distribueringsmodellerna har samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014. <i>(De centrala delarna av skäl 33 i NIS 2-direktivet)</i>

Molntjänster definieras ganska tydligt i NIS 2-direktivet, och utöver själva definitionen nämns de vanliga tjänste- och distributionsmodellerna för molntjänster.

För att betraktas som en molntjänst ska alla kriterier vara uppfyllda. Om någon inte är det, så är det inte att betrakta som molntjänst. Det innebär att exempelvis Ladok eller e-posttjänster inte är molntjänster i direktivets mening, och därmed inte heller många av de tjänster som flera lärosäten erbjuder holdingbolag eller föreningar.

Sektor: digital infrastruktur (molntjänster)

Beräkningsresurser	Resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster.
Beställtjänster	Molnanvändarens kapacitet att ensidigt, självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster, kan beskrivas som beställtjänster.
Bred fjärråtkomst	Molnkapaciteten tillhandahålls över nätet och nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar, däribland mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer.
Skalbar	Beräkningsresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan.
Elastisk pool	Beräkningsresurser som tillhandahålls och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna ökas och minskas i takt med arbetsbördan.
Delbar	Beräkningsresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning.

Molntjänster ska ha sex olika egenskaper.

Beräkningsresurser har en bred definition som passar in på väldigt mycket.

Beställtjänster innefattar att användaren ska kunna tillhandahålla kapacitet själv, utan inblandning från leverantören. Om det exempelvis krävs ett manuellt godkännande eller en manuell konfiguration, är det inte en beställtjänst. **Bred fjärråtkomst** innebär att tjänsten ska nås genom mekanismer som *främjar* (inte bara möjliggör) åtkomst av heterogena klientplattformar. Tjänster som är utformade på ett sätt som försvårar användning av exempelvis mobiltelefoner kan knappast sägas *främja* åtkomst från dessa, och därför erbjuder inte tjänsten bred fjärråtkomst. På motsvarande sätt kan man bedöma egenskaperna skalbar, elastisk pool, och delbar.

Även om ett lärosäte erbjuder en molntjänst så bör man också ta ställning till om den har en gränsöverskridande karaktär, eftersom direktivet så tydligt framhäver detta som en egenskap hos molntjänster. Om den saknar en gränsöverskridande karaktär kan det ifrågasättas om lärosätet är en *leverantör* av molntjänster i direktivets mening.

För att räknas som molntjänst ska tjänsten ha alla ovanstående egenskaper. Faller en, så är det inte en molntjänst enligt direktivets definition! Utöver de strikta kriterierna i definitionen av en molntjänst så diskuterar man tjänste- och distribueringsmodeller för molntjänster, så man kan nog hänvisa även till dessa: att om en tjänst inte passar in på någon av dessa modeller, så är det nog inte en molntjänst.

Kring den här sektorn finns nog inget större behov av samordning i sektorn eftersom varje tjänst är unik, men det vore olyckligt om man bestämde sig för att en tjänst som ladok vore en molntjänst, kanske för att man vill vara på den säkra sidan. Och för den som inte vill att en tjänst de erbjuder ska vara en molntjänst, lägg in ett manuellt steg i beställningen av resurser så det inte blir en beställtjänst.

Sektor: digital infrastruktur (datacentraltjänster)

Definition	En tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.
Förtydligande	Vid tillämpningen av detta direktiv bör termen datacentraltjänst omfatta strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Termen datacentraltjänst bör inte vara tillämplig på interna datacentraler som ägs och drivs av den berörda entiteten för egen räkning.

(De centrala delarna av skäl 35 i NIS 2-direktivet)

Flera lärosäten inhyser utrustning för andras räkning i sina datacentraler, och frågan om det innebär att man är leverantör av datacentraltjänster har dryftats.

Direktivets definition av en datacentraltjänst utesluter tydligt interna datacentraler som man äger och driver för egen räkning och sätter i stället fokus på anläggningar (strukturer eller grupper av strukturer) som är *avsedda* för *centraliserad inkvartering*. De allra flesta datacentraler vid lärosätena ägs och drivs av lärosätet för egen räkning, och är inte avsedda för inkvartering. Eventuell inkvartering, även om den görs mot betalning, är oftast ett sammanträffande, en snabb och smidig lösning på ett problem som lärosätet och en samarbetspart ställts inför.

Även om lärosätet bedömer att man erbjuder datacentraltjänster så är det motiverat att överväga om tjänsten har en gränsöverskridande karaktär, något som i skälen till direktivet framhävs som en egenskap hos datacentraltjänster.

Sektor: forskning

Definition [Forskningsorganisationer är entiteter] 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.

Förtydligande Forskningsorganisationer bör anses inbegripa entiteter som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i "Frascatimanualen 2015: Riktlinjer för insamling och rapportering av uppgifter om forskning och experimentell utveckling" från Organisationen för ekonomiskt samarbete och utveckling, i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållande av en tjänst, eller marknadsföring därav.

(De centrala delarna av skäl 36 i NIS 2-direktivet)

Forskningssektorn ser till namnet ut att vara tillämpligt på de flesta lärosäten, men direktivet är tydligt med att man här avser tillämpad eller experimentell forskning – inte grundforskning – som bedrivs med kommersiellt syfte. Man skriver också explicit att sektorn inte inbegriper utbildningsinstitutioner. Direktivet anger också att medlemsstaterna själva får föreskriva att direktivet får tillämpas på utbildningsinstitut, vilket ytterligare understryker att universitet och högskolor inte förväntas ingå i sektorn "forskning".

Avslutande kommentarer

Cybersäkerhet är viktigt och något som sektorn i stort behöver satsa på

Det handlar inte om att undvika att arbeta med cybersäkerhet – utan att göra det på rätt sätt

Regelverk kan vara till hjälp, men fel regelverk kan orsaka stora svårigheter i arbetet

Försiktighet i bedömningarna undviker överimplementering och skapar handlingsutrymme



Cybersäkerhetslagen i sig är väl avvägd för sitt syfte. Den identifierar sektorer där det är av särskild vikt att upprätthålla en god cybersäkerhet, och ger berörda verksamhetsutövare ett ramverk inom vilket de kan arbeta på det sätt som ger bäst utfall. Cybersäkerhetsförordningen fortsätter den trenden, även om den inför vissa utmaningar för de verksamhetsutövare som har verksamhet i flera olika sektorer. Den mer omfattande reglering som väntas i föreskrifter från främst Myndigheten för Civilt Försvar (MCF) riskerar dock medföra betydande svårigheter eftersom de föreskriver i detalj hur stora delar av cybersäkerhetsarbetet ska bedrivas, och därmed riskerar leda till en kraftigt ökad administrativ börda, och att uppmärksamhet och resurser avleds till att följa regelverket snarare än att upprätthålla en lämplig cybersäkerhetsnivå. Härvidlag skiljer sig de föreslagna föreskrifterna fundamentalt från såväl NIS 2-direktivet som cybersäkerhetslagen, och från standarder som ISO 27000 – som alla poängterar vikten av att utforma arbetet med cybersäkerhet utifrån verksamhetens risk och lämnar eventuell detaljstyrning till vägledning.

Med det perspektivet finns det anledning att undvika extensiva i bedömningarna av vilken verksamhet som omfattas av NIS 2-direktivets och därmed cybersäkerhetslagens kriterier. Genom att vara återhållsam skapas ett handlingsutrymme där lärosätet kan välja inriktning: att arbeta med cybersäkerhet utifrån ett givet regelverk, eller att arbeta med cybersäkerhet utifrån sina egna behov och förutsättningar.

Men att arbeta med cybersäkerhet – det är något alla måste göra.

Linköpings universitet

www.liu.se

