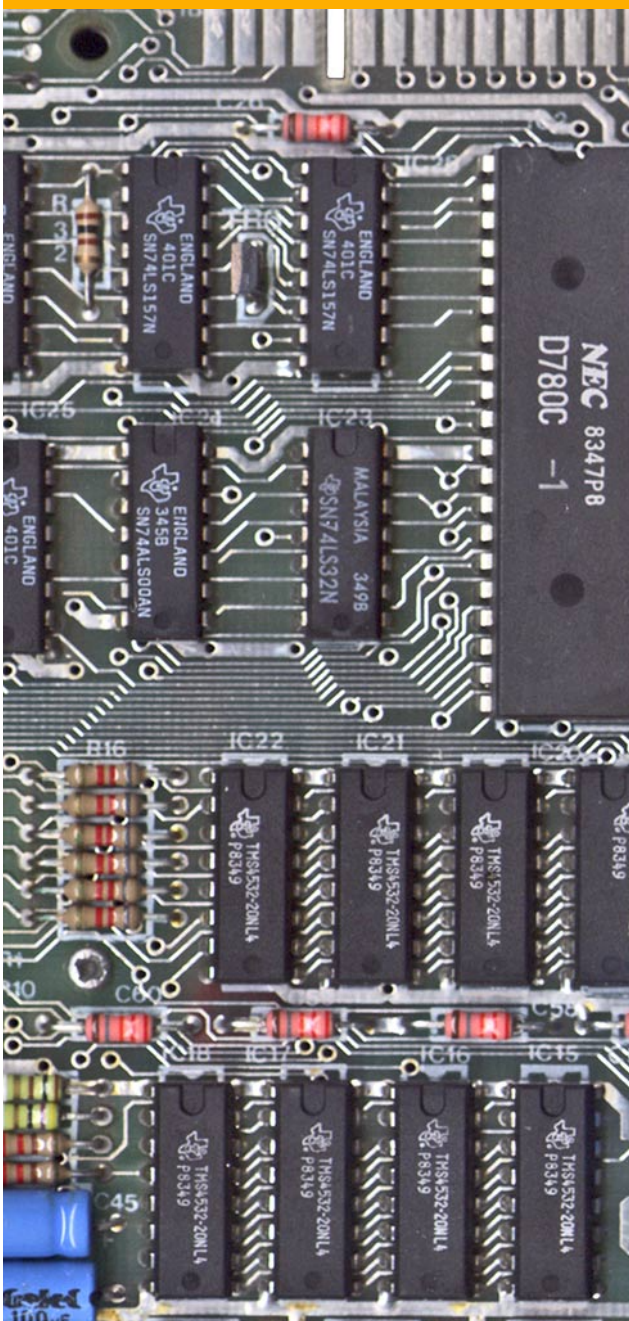
Swedish Edtech Industry

Digital suveränitet i utbildningssektorn

Beroenden, beredskap och handlingsfrihet



Medlemsundersökning om digital suveränitet i utbildningssektorn

Swedish Edtech Industry 2026

Förord

Digital suveränitet och beredskap

Den här rapporten lyfter en fråga som hamnat allt högre upp på agendan: frågor om molnval och digital infrastruktur handlar inte längre bara teknik, konkurrenskraft eller juridik, de har blivit strategiska och kopplade till säkerhetsfrågan. Hur beroende är vi av andra och vad händer om någon stänger av tillgången? Efter återkommande utspel från USA:s politiska ledning, läs Donald Trump, har debatten om vårt beroende av amerikanska molntjänster tagit ny fart i Europa, men också hemma i Sverige. Den diskuteras inom såväl näringslivet som offentlig sektor och frågan ställs allt oftare direkt till politiker, även på EU-nivå.

Samtidigt är det en komplex och svår fråga, utan enkla svar. Beroendet av ett fåtal dominerande leverantörer hänger ihop med hur marknaden har utvecklats: stora tredjelandsaktörer har byggt ett betydande tekniskt försprång, skalfördelar och ekosystem som präglar både innovationstakt och prisbild. Därför handlar diskussionen inte bara om risker och beredskap, utan också om Europas konkurrenskraft och om hur vi kan kombinera säkerhet, funktionalitet, kostnadseffektivitet och innovationsförmåga.

För skola och utbildning är frågan extra viktig. Skolan och utbildningssystemet är samhällsbärande funktioner. Coronapandemin visade hur snabbt undervisning blir beroende av digitala verktyg när samhället behöver ställa om. Och när fysisk skolgång hotas kan distansundervisning vara avgörande för att utbildning ska kunna fortsätta. I det perspektivet blir "digital suveränitet" i den här rapporten inte en abstrakt princip, utan en praktisk fråga om kontroll, kontinuitet och förmågan att agera: att veta var data finns, vilka regler som gäller, vilka underleverantörer som ingår och att kunna byta eller avveckla en tjänst utan att verksamheten stannar. Har vi beredskap om något händer?

Digital suveränitet är inte en helt enkel fråga och den kan förstås på olika sätt. För vissa handlar den främst om kontroll över data, infrastruktur och beroenden. För andra handlar den om vår förmåga att utveckla tjänster och lösningar för det svenska utbildningsväsendet utifrån europeiska behov, nationella särdrag och värderingar. I det perspektivet blir det också en fråga om hur vi skapar förutsättningar för en europeisk marknad och för företag att utveckla lösningar som möter behov.

För att komma vidare i samtalet behövs mer kunskap om hur frågan uppfattas och vilka erfarenheter som finns hos de aktörer som utvecklar och levererar digitala tjänster till utbildningssektorn. Därför presenterar vi en rapport som bygger på en medlemsundersökning från februari 2026. Undersökningen ska läsas som en temperaturmätare, inte som en heltäckande bild av hur det ser ut i hela utbildningssektorn. Den ger indikationer på hur våra medlemmar uppfattar frågor om beroenden, risker, krav och beredskap, liksom vilka frågor som möter dem i dialogen med kunder. Med rapporten vill vi uppmärksamma ett område som behöver diskuteras med större precision än idag. Rapporten är deskriptiv och syftar till att bidra med ett underlag för fortsatt samtal, fördjupad analys och välgrundade beslut.

Jannie Jeppesen

Vd Swedish Edtech Industry

Innehåll

Bakgrund
Varför denna rapport?

Debatten om Sveriges och Europas beroende av framför allt amerikanska molntjänster har tagit fart igen. Världsläget är mer osäkert och USA:s politik upplevs som mer svår att förutsäga. Vår medlemsundersökning genomfördes i början av februari 2026, innan Israel och USA anföll Iran. När konflikter och handelsspänningar ökar hamnar digital infrastruktur i centrum. Det som tidigare sågs som en teknisk fråga blir istället en fråga om trygghet och beredskap.

Ett växande "molnberoende" i Europa

Marknadsdata över användningen av amerikanska molntjänster i hela Europa visar att beroendet är stort. Enligt Synergy Research Group har europeiska molnleverantörer visserligen mer än tredubblat sina lokala intäkter mellan 2017 och 2024, men marknaden har vuxit ännu snabbare. År 2024 var den europeiska molnmarknaden värd cirka 61 miljarder euro. Europeiska leverantörers marknadsandel ligger runt 15 %, medan Amazon, Microsoft och Google tillsammans står för omkring 70 %.

Marknadsandelar i Europa

Europeiska molnleverantörer: ca **15 %**
Amazon, Microsoft och Google tillsammans: ca **70 %**
Europeisk molnmarknad: ca **61 miljarder euro**

Källa: Synergy Research Group (2024)

Det betyder att även när europeiska alternativ växer, fortsätter beroendet av de största amerikanska leverantörerna att vara mycket stort i både offentlig sektor och i det privata näringslivet. Här finns också en alternativkostnad att ta i beaktande: ledande företrädare från det svenska och europeiska näringslivet[1] lyfter perspektivet att om vi lämnar de stora teknikplattformarna kommer det att minska företagens produktivitet och konkurrenskraft.

I korthet
Molntjänster

En **molntjänst** innebär att lagring, beräkningskapacitet och programvara tillhandahålls via internet istället för att drivas lokalt på egna servrar. Organisationer hyr kapacitet efter behov istället för att själva äga infrastrukturen.

Med amerikanska molntjänster avses molnbaserade tjänster som ägs eller drivs av företag med huvudkontor i USA, till exempel Amazon Web Services (AWS), Microsoft och Google. De erbjuder både grundläggande infrastruktur (servrar, databaser, lagring) och mer undervisningsnära tjänster, AI och analysverktyg.

Även när data lagras i europeiska datacenter kan leverantören omfattas av amerikansk lagstiftning, vilket är en del av den juridiska diskussion som förs kring digital suveränitet.

Hyperscalers

Begreppet **hyperscalers** används för att beskriva mycket stora globala molnleverantörer med kapacitet att skala upp drift i mycket stor omfattning. Exempel är AWS, Microsoft Azure och Google Cloud. Många digitala tjänster i Europa, även sådana som utvecklas av europeiska bolag, körs på infrastruktur från någon av dessa aktörer. Därför får hyperscalers en central roll i frågor om beroenden, digital suveränitet och beredskap.

[1]ComputerSweden 13/3-26:Europeiska företag varnar EU – minskat beroende av USA-teknik slår mot lönsamheten

Digital suveränitet – vad menar vi?

I den här rapporten använder vi "digital suveränitet" i en praktisk betydelse, dvs fokuserar på var data lagras och vilken lag som gäller, insyn i leverantörskedjan och underleverantörer, möjlighet att byta leverantör utan stora avbrott, tydliga exitplaner och planer för kontinuitet om en tjänst slutar fungera.

I korthet

Vad menas med digital suveränitet?

Digital suveränitet handlar i grunden om att ha kontroll över sina egna digitala system, sin data och sin tekniska infrastruktur. Enkelt förklarat betyder det att bestämma över vår information, var den lagras, vem som har tillgång till den och vilka regler som gäller. Det handlar också om att inte vara ensidigt beroende av enskilda företag eller andra länder för att samhällets digitala funktioner ska fungera.

För svensk utbildningssektor är frågan särskilt relevant eftersom vi idag har ett stort beroende av digitala tjänster till vardags. Elevregister, betygssystem, lärplattformar, digitala provverktyg och läromedel samt i allt högre grad olika AI-lösningar är centrala för den dagliga verksamheten. En del av denna teknik tillhandahålls av stora globala företag, ofta med huvudkontor och lagstiftning utanför EU.

Digital suveränitet i utbildningssektorn handlar därför om mer än bara it-drift. Det rör skyddet av elevers och studenters personuppgifter, forskningsdata och känslig information. Sen handlar det om att säkerställa att undervisning, examination och administration kan fortsätta även om en tjänst ligger nere, om ett avtal förändras eller om det uppstår en geopolitisk konflikt som påverkar tillgången till ett digitalt verktyg. Det handlar också om att undvika ett för ensidigt beroende av enskilda leverantörer, så att skolhuvudmän och lärosäten har handlingsutrymme.

Digitala tjänster består sällan av en enda leverantör. Bakom en lärplattform, ett provsystem eller en AI-tjänst kan det finnas flera led: molninfrastruktur, driftpartners, säkerhetstjänster och supportfunktioner. Dessa kan i sin tur ha egna underleverantörer.

I korthet

Vad är en leverantörskedja?

En **leverantörskedja** är alla de aktörer som tillsammans gör en digital tjänst möjlig. Inom edtech handlar det inte bara om företaget som säljer en lärplattform eller ett digitalt läromedel, utan också om deras molnleverantörer, driftpartners, underleverantörer av kod, AI-modeller och supporttjänster.

En tjänst kan vara utvecklad av ett europeiskt bolag men drivas på en global molninfrastruktur. Support kan utföras från ett annat land och vissa tekniska komponenter kan levereras av ytterligare aktörer. Leverantörskedjan blir därmed internationell, även när kunden tecknar avtal med en enda part. Ju fler led i kedjan, desto större krav ställs på transparens, riskbedömning och uppföljning.

Beredskap, en central del av suveränitet

Beredskap handlar i grunden om att ha kontroll och handlingsförmåga när förutsättningarna förändras. Den blir därför en central del av digital suveränitet. Att ha beredskap betyder att, i den mån det är möjligt, vara förberedd *innan* något händer. I ett osäkrare säkerhetsläge, med ökande cyberhot och större geopolitiska spänningar, är utbildningssektorn en samhällsviktig funktion. Om skolornas digitala system slås ut påverkar det elevers rätt till utbildning, betygssättning, antagning till vidare studier och i förlängningen hela samhällets kompetensförsörjning. Om universitetens system drabbas kan forskning försenas eller gå förlorad.

En viktig del av beredskapen är samspelet mellan juridik och informationssäkerhet. Dataskyddsjuridiken (GDPR, dataskyddslagen, offentlighets- och sekretesslagen, arkivlagen) sätter ramarna för hur personuppgifter och information får hanteras. Informationssäkerheten handlar om de tekniska och organisatoriska åtgärder som krävs utifrån hur skyddsvärd informationen är, exempelvis kryptering, behörighetsstyrning och incidenthantering.

Tillsammans utgör de grunden för att bygga robusta och resilienta digitala system. En lösning behöver vara både juridiskt hållbar och tekniskt säker över tid. Samtidigt kräver beredskap mer än regelefterlevnad. Efterlevnad (compliance) innebär att organisationen vet vilka regler som gäller, kan visa hur de följs och löpande följer upp risker. Det minskar sårbarheten vid exempelvis lagändringar, rättspraxis eller förändringar i leverantörskedjan.

Centrala delar av beredskap

Exitplan: en plan för hur data och drift kan flyttas om en tjänst inte längre kan användas
Dataportabilitet: möjlighet att exportera och återanvända data i andra system
Kontinuitetsplanering: hur verksamheten fortsätter arbeta vid avbrott
Undvika inlåsning: tekniska och avtalsmässiga val som möjliggör leverantörsbyte

Beredskap handlar ytterst om att kunna agera. Att ha konkreta planer för hur data och tjänster kan flyttas, ersättas eller drivas vidare vid störningar.

Att stärka beredskapen inom utbildning handlar om att bygga motståndskraft. Det innebär att ha överblick över var data finns och vem som har tillgång till den, att ställa genomtänkta krav i upphandlingar, minska sårbara beroenden och att utveckla egen kompetens.

Skolan är en samhällsbärande funktion

För utbildningssektorn är frågan extra viktig. Skolan är en samhällsbärande verksamhet. Coronapandemin visade hur snabbt undervisning och administration blir beroende av digitala verktyg när samhället behöver ställa om. Utbildningssektorn i Sverige omfattar i runda slängar 2,5 miljoner barn, elever och studenter. Kriget i Ukraina visar också hur viktigt det är att ha beredskap: när fysisk skolgång hotas blir hel eller delvis distansundervisning avgörande för att utbildning ska kunna fortsätta.

Utbildningssverige behöver ha beredskap, dvs handlingsförmåga, för att säkerställa att svensk skola och högre utbildning kan fungera stabilt och säkert även när omvärlden är orolig.

Hur ser det ut i utbildningssektorn - vad visar vår undersökning?

För att förstå vad vi behöver göra framåt, behöver vi först få en tydligare bild av hur det ser ut med beroendet och beredskapen i utbildningssektorn. Ett sätt är att ta hjälp av de som levererar tjänster, dvs våra medlemmar. I vår medlemsundersökning, som ligger till grund för den här rapporten, har vi ställt frågor dels om hur deras leverantörskedja ser ut, hur deras möjlighet att vid behov, byta ut delar av kedjan och dels hur deras kunder kravställer och vilka utmaningar det finns framåt.

Svaren på undersökningen synliggör problematiken med de olika tolkningarna av rådande lagrum som finns, hur risken med beroenden till amerikanska molntjänster uppfattas och hur väl de tekniska åtgärderna kan skydda data som hanteras. Några betonar de kvarstående juridiska och strukturella beroendena i amerikanska molntjänster, medan andra menar att riskerna i stor utsträckning kan hanteras genom rätt teknisk och organisatorisk uppsättning. Det här gäller såväl våra medlemmar som deras kunder där våra medlemmar är avhängiga sina kunders tolkning och i det behöver göra olika anpassningar. Många vittnar om kundernas hängslen- och byxremtänk, dvs att för säkerhets skull ställa ibland irrelevanta krav på efterlevnad och inte utgå från tjänsten som sådan och vilken data den hanterar.

> **För hög eller låg "sense of urgency". Sällan rimlig nivå.”**
>
> citat från medlemsundersökning 2026

”Två skolor”

Ansvaret att säkerställa beredskap ligger inte enbart hos den ena eller den andra parten. Det är ett samarbete som regleras av flera olika faktorer: kravställning, hur det digitala ekosystemet av tjänster ser ut och fungerar hos kund (vilka integrationer som finns mellan de olika tjänsterna, hur data flödar och vad som då händer om en tjänst inte längre är tillgänglig), hur supportavtal och andra avtal ser ut.

Vår medlemsundersökning visar på två “skolor”, både när det gäller företagen själva, men även deras kunder. De som å ena sidan betonar de kvarstående juridiska och strukturella beroenden i amerikanska molntjänster respektive de som å andra sidan menar att riskerna i stor utsträckning kan hanteras genom rätt teknisk och juridisk uppsättning.

Amerikanska vs europeiska molntjänster - vad tycker våra medlemmar?

I korthet

Vad menas med EU/EES baserade eller ägda lösningar?

Med **EU/EES-baserade** eller EU/EES-ägda lösningar avses digitala tjänster där både ägandet och den huvudsakliga driften finns inom EU eller EES. Det innebär att företaget har sitt huvudkontor inom EU/EES, lyder under EU:s lagstiftning och att data i normalfallet lagras och behandlas inom området.

Amerikanska molntjänster: Å ena sidan har vi medlemmar som menar att beslutsfattare underskattar att amerikanska molntjänster lyder under amerikansk lag, trots lagring i EU och kryptering, vilket gör att amerikanska myndigheter kan begära ut data och att IP-trafik och användare är synliga. Å andra sidan har vi medlemmar som menar att man kan isolera drift i Sverige/EES med rätt uppsättning och juridiska avtal. Vissa menar att stark kryptering och kompletterande skyddsåtgärder gör det möjligt att uppfylla kraven även med

globala leverantörer. Andra menar att tredjelandslagstiftning innebär en kvarstående osäkerhet som inte fullt ut kan avtalas bort.

***Lokala alternativ vs hyperscalers*:** I vår undersökning frågade vi om alternativ till de stora globala molnleverantörerna, där några svarar att beslutsfattare har för hög tilltro till att det finns likvärdiga europeiska alternativ, men det motsatta anges också, att beslutsfattare inte vet att det finns andra alternativ att kravställa.

Vanliga missuppfattningar: "Suveränitet är inte detsamma som säkerhet"

Vi frågade också våra medlemmar om vilka de menar är de största missuppfattningarna hos beslutsfattare om digital suveränitet. Här ger fritextsvaren en splittrad bild.

Komplexitet och omfattning av digital suveränitet: Det är en missuppfattning att frågan om digital suveränitet är enkel att lösa: enligt svaren i vår undersökning underskattar beslutsfattare hur svårt det är att uppnå fullständig suveränitet utanför befintliga ekosystem (läs Google/Microsoft). Man pekar bland annat på låg kunskap generellt om digital suveränitet, data governance och hela kedjan av underleverantörer, där fokus ofta ligger på hosting snarare än hela kedjan. Inom skolan anmärks det bland annat att man ser en inkonsekvens för leverantörer: samtidigt som stora amerikanska leverantörer upphandlas och används i bred skala kan mindre leverantörer granskas striktare gällande amerikansk-ägd tredjepart.

I korthet

Data governance

Data governance kallas på svenska oftast datastyrning och handlar om de regler, processer och ansvar som säkerställer att en organisation hanterar data korrekt, säkert och i enlighet med lagar och mål.

> **"Att i stort sett alla svenska huvudmän använder antingen Google eller Microsoft som productivity suites och att det då går att försvara utifrån ett GDPR perspektiv, men att mindre leverantörer förväntas att absolut inte leverera sina tjänster överhuvudtaget där det finns någon amerikansk-ägd tredjepart i något led."**
>
> citat från medlemsundersökning 2026

Suveränitet är inte samma sak som säkerhet. Ett återkommande tema i fritextsvaren är sammanblandningen av begrepp: att suveränitet likställs med informationssäkerhet eller att hög säkerhet antas innebära suveränitet. I praktiken överlappar frågorna, men de kräver olika typer av beslut: suveränitet handlar om kontroll, handlingsfrihet och beroenden över tid, medan säkerhet handlar om skyddsnivåer, riskhantering och motståndskraft. När de blandas ihop riskerar kraven att bli antingen för vaga eller för absoluta.

Förändrad efterfrågan - rörelse men ingen tydlig förskjutning

Undersökningen visar att efterfrågan på EU/EES-baserade eller EU/EES-ägda lösningar har ökat det senaste året, men inte dramatiskt.

37 % av våra medlemmar uppger att efterfrågan har ökat något eller mycket under de senaste tolv månaderna. Samtidigt anger 28 %

37 %

uppger att efterfrågan på EU/EES-ägda lösningar ökat.

28 %

ser inte några förändringar alls.

att de inte ser någon förändring alls. Det tyder på en tydlig rörelse i marknaden, men inte en generell eller genomgripande förskjutning.

När det gäller konkreta krav är signalen starkare. 79 % uppger att de ofta eller ibland möter tydliga kundkrav kopplade till digital suveränitet, såsom EU/EES-drift, datalagring inom EU eller minskat beroende av tredjeland. Ca 13 % möter sällan sådana krav och endast en respondent uppger att det aldrig förekommer. Digital suveränitet är alltså en återkommande fråga i dialogen med kund.

79 %
uppger att de möter tydligare kundkrav gällande digital suveränitet.

Samtidigt visar svaren att suveränitet inte alltid är avgörande i praktiken. Om två tjänster är likvärdiga i pris och funktion uppger ca 11 % att de tror att kunden alltid skulle välja den helt EU/EES-baserade eller EU/EES-ägda lösningen, 32 % tror ofta och ca 28 % ibland. Det indikerar att europeiskt ägande och drift har betydelse, men då när pris och funktion redan är jämbördiga. Sammantaget tyder det på att pris och funktion fortfarande väger tyngre än digital suveränitet när faktorerna ställs mot varandra.

Företagens syn på sin beredskap, affärskritiska beroenden och framtiden

Vår undersökning visar att många företag har betydande beroende av tredjeland i sina leverantörskedjor. 28 % uppger att mellan 76-100 % av deras leverantörskedja är beroende av teknik eller tjänster utanför EU/EES. Endast knappt 18 % anger att de inte alls har något sådant beroende. Någon form av tredjelandskopplingar framstår därmed som en realitet för en majoritet av företagen.

Molntjänster det mest kritiska beroendet

När det gäller affärskritiska områden är molntjänster det tydligaste beroendet: nästan 35 % anger detta som mest kritiskt. AI-tjänster (11 %) samt support och ärendehantering (13 %) nämns också. Samtidigt uppger 26 % att de inte har något affärskritiskt område i tredjeland, vilket inte är helt i linje med svaren om hur stor del av leverantörskedjan som är beroende av teknik från tredjeland. Här är en tolkning att man i sitt svar fokuserat på just om det är affärskritiskt eller ej, inte om hela leverantörskedjan är inom EU/EES.

Ingen anger säkerhet som ett affärskritiskt beroende, vilket är anmärkningsvärt, särskilt med tanke på att centrala säkerhetsfunktioner globalt ofta domineras av amerikanska aktörer. De stora leverantörerna på området är Cloudfare och Akamai som driftsleverantörerna använder. De stora molntjänsterna erbjuder också visst skydd. Det finns något enstaka europeiskt företag på området, men de ligger på en prisskillnad på tusentals procent.

Beredskap anses god och risken för avbrott låg

60 %
har en exit- eller beredskapsplan.

Över 70 %
bedömer risken för påverkan som låg eller obefintlig.

Det största hindret att byta till en EU/EES-lösning är bristen på likvärdiga alternativ.

Bilden av beredskap är blandad. Nära 60 % uppger att de helt eller delvis har en exit- eller beredskapsplan för att kunna byta ut kritiska tredjelandskomponenter, medan 30 % saknar en sådan plan och var tionde inte vet. Hälften bedömer att de kan byta ut en tjänst inom tre månader och ytterligare ca 22 % inom tre till tolv månader. Samtidigt anger över 42 % att det största hindret för att byta till en EU/EES-lösning är bristen på europeiska alternativ och 13 % pekar på funktion och prestanda. Detta speglar den starka tekniska och prismässiga dominans som några globala leverantörer har, särskilt inom moln.

Trots dessa beroenden bedömer över 70 % att risken för påverkan genom avbrott, exportrestriktioner eller policyförändringar hos leverantörer utanför EU/EES är låg eller obefintlig, medan 19 % ser en medel eller hög risk. Sammantaget tyder resultaten på att företagen är medvetna om sina beroenden och i viss mån arbetar med beredskap, men att riskuppfattningen i nuläget är relativt låg, samtidigt som alternativen inom EU/EES ofta upplevs som begränsade.

Vad våra medlemmar uppger behövs framåt

Frågan om digital suveränitet är inte enkel att lösa. I fritextsvaren blir det tydligt att många av våra medlemmar uppfattar att diskussionen om digital suveränitet ofta fastnar i principer, medan det som saknas är förutsättningar att faktiskt genomföra förändring, där så behövs. Det handlar dels om ökade kostnader, dels om hur upphandlingar utformas, vilka tekniska grundvalar som finns och vilken vägledning eller styrning som kommer från EU och nationell nivå.

Policy och upphandling: kvalitet, behov och budget
Många efterlyser att upphandlingar i högre grad behöver prioritera kvalitet framför pris och att krav ska utgå från behov och arbetsprocesser snarare än detaljerade funktionalitetskrav. Flera vill också se upphandlingar som öppnar för dialog och innovation, så att nya alternativ kan komma in. Det betonas också att digitalt suveränare lösningar och byten ofta innebär merkostnader och att det behövs budget för omställningen.

> **Högre budget behövs för suveräna lösningar”**
> citat från medlemsundersökningen 2026

Minska leverantörsinlåsning: fler leverantörer och europeiska alternativ
Ett tydligt budskap är att dagens lösningar och upphandlingar ofta leder till inlåsning. Man efterlyser arkitekturer och krav som möjliggör flera leverantörer i stället för en “totalleverantör” och en mer aktiv linje för att främja europeiska alternativ. Samtidigt lyfts utmaningen att EU-baserade alternativ inte alltid upplevs vara i funktionell paritet, vilket gör byten svår att motivera.

Kunskap och förståelse: krav måste förstås
Flera svar i vår undersökning pekar på att beslutsfattare ibland ställer krav utan att förstå konsekvenserna för kostnad, integrationer och ansvar. “De måste själva förstå vad deras krav betyder” återkommer som en kärnpunkt.

Juridisk tydlighet och stöd: mindre osäkerhet och EU-beslut
Slutligen efterfrågas tydligare vägledning kring GDPR och andra relaterade krav, mindre “skrämsel” och mer praktiskt stöd. Flera menar också att det behövs beslut och riktning på EU-nivå för att skapa harmonisering och verklig effekt.

> **Det behövs beslut på EU-nivå”**
> citat från medlemsundersökningen 2026

Valet är inte svart-vitt - hur ska resultaten tolkas?

Frågan om digital suveränitet i utbildningssektorn kan inte reduceras till ett enkelt val mellan amerikanska och europeiska lösningar. Resultaten pekar istället på en mer komplex verklighet, där beroenden till tredjeland är omfattande, samtidigt som alternativen inom EU/EES ofta upplevs som begränsade i fråga om funktion, prestanda eller kostnad. Det finns en medvetenhet om frågan och en växande efterfrågan från kunder, men ännu ingen genomgripande förskjutning i marknaden. Sammantaget tyder detta på att sektorn befinner sig i ett mellanläge: viljan att stärka handlingsfrihet och beredskap ökar, men de praktiska förutsättningarna för omställning är fortfarande otillräckliga. Nästa steg behöver därför handla mindre om principdiskussioner och mer om att skapa genomförbara vägar framåt – genom tydligare vägledning, mer ändamålsenlig upphandling, ökad kompetens och bättre förutsättningar för europeiska alternativ att växa.

Om medlemsundersökningen

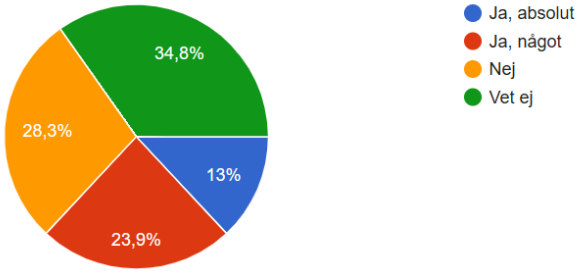
Medlemsundersökningen skickades ut till Swedish Edtech Industrys medlemmar under perioden 2–12 februari 2026. Svarsfrekvensen var 64 procent. De svarande speglar bredden i vår medlemsbas, med företag inom bland annat förlag, lärplattformar, provtjänster, hårdvara, undervisningsnära tjänster och tjänster kopplade till digital infrastruktur.

Resultaten ska läsas som en temperaturmätare bland våra medlemmar, inte som en heltäckande bild av hur det ser ut i utbildningssektorn som helhet. Undersökningen ger indikationer på hur de svarande företagen uppfattar frågor om tillgång, beroenden, risker och krav, utifrån sin verksamhet och sina kunddialoger.

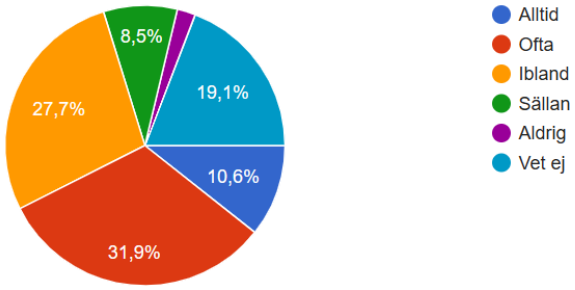
De svarande levererar till skolväsendet, yrkeshögskolan och högre utbildning, men också till företags lärande. Majoriteten levererar främst till skolväsendet. Resultaten speglar inte tillgången till eller användningen av de stora kommunikations- och produktivitetsplattformar, såsom Microsoft och Google, som används brett inom utbildning och företag.

Tabeller och data ur undersökningen

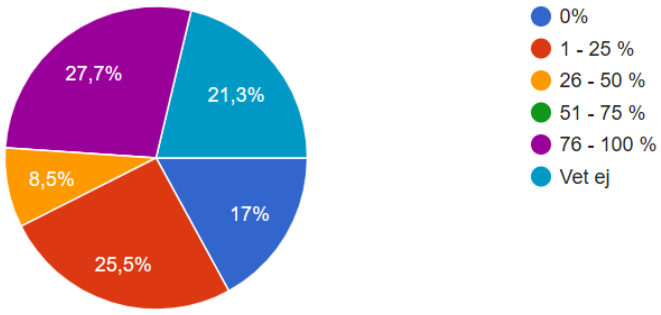
Har efterfrågan på EU/EES-baserade/ägda lösningar ökat de senaste 12 månaderna?



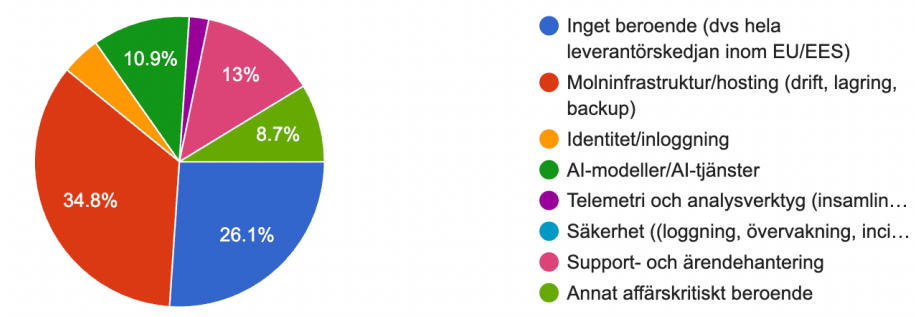
Om två tjänster är likvärdiga i pris och funktion, varav en helt EU/EES-baserad/ägt – hur ofta tror ni att kunden väljer den utifrån suveränitetsskäl?



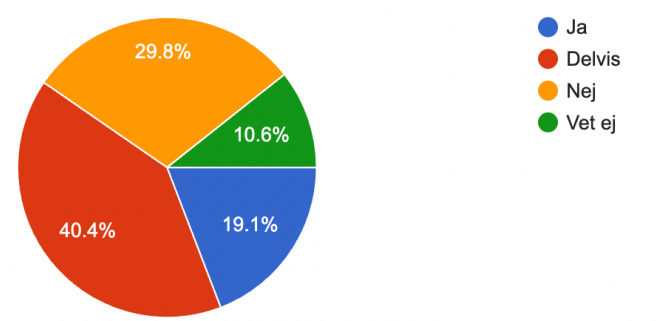
Hur stor del av er leverantörskedja är beroende av teknik från tredjeland (utanför EU/EES)?



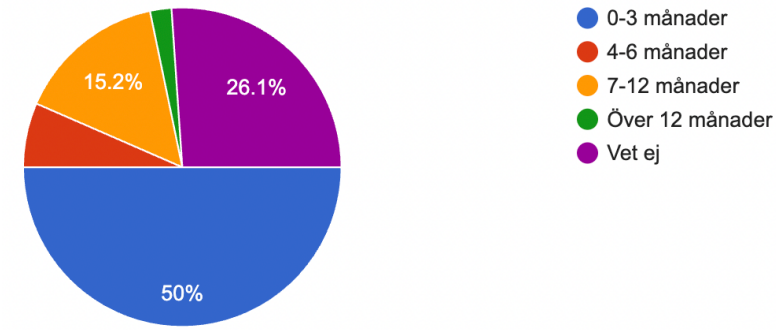
Inom vilket område finns ert mest affärskritiska tredjelandsberoende? (fler svar möjliga)



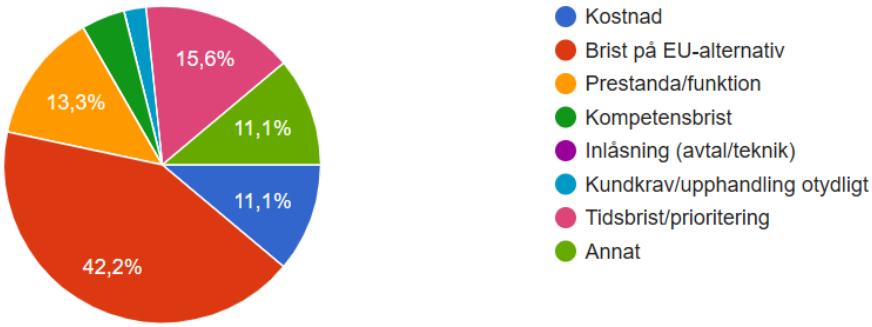
Har ni en exit-plan för att kunna byta ut kritiska tredjelandskomponenter?



Om ni skulle behöva byta ut en kritisk komponent, hur lång tid skulle det ta?



Vilket är det största hindret för att ev. byta ut en tredjelandskomponent mot en inom EU/EES?


15,6%
13,3%
11,1%
11,1%
42,2%
Kostnad
Brist på EU-alternativ
Prestanda/funktion
Kompetensbrist
Inlåsning (avtal/teknik)
Kundkrav/upphandling otydligt
Tidsbrist/prioritering
Annat