

DUAL-USE

Praktisk arbetsmanual för Innovationsrådgivare

EU 2021/821 — Export av produkter med dubbla användningsområden

Timo Lagerbjelke
lagerbjelke.se

Version 1.0 — Mars 2026

Inledning

Den här manualen är ett utbildningsverktyg för innovationsrådgivare som möter frågor om exportkontroll i sitt arbete. Den ger dig tillräcklig förståelse för att känna igen när dual-use-regelverket är relevant, ge klienter ett första orienterande råd och veta när och hur du ska eskalera till specialistkompetens.

Vad dual-use faktiskt är — och inte är

Begreppet dual-use är missvisande och skapar ofta förvirring i innovationsmiljöer. Dubbla användningsområden för tankarna till produkter som kan användas av både civila och militära — och i den tolkningen faller plötsligt mycket in: spadar, fordon, standardverktyg, kontorsmateriel. Militären är en verklig kund på många marknader och det är fullt legitimt att sälja till den. Men det är inte vad EU:s dual-use-förordning handlar om.

EU 2021/821 reglerar export av en specifik och avgränsad kategori produkter: sådana som har potential att bidra till massförstörelsevapen, avancerade vapensystem eller teknologier som kan användas för att destabilisera stater eller kränka mänskliga rättigheter i stor skala. Det rör sig om krypteringsteknik, avancerade halvledare, sensorer, navigeringssystem, biologiska och kemiska ämnen med mera. Vad som faktiskt kontrolleras definieras inte av en allmän princip utan av en konkret lista — Annex I till förordningen — med tekniska parametrar som avgör om en specifik produkt träffas.

En spade är inte dual-use i lagens mening, även om en soldat använder den. Ett avancerat navigeringssystem kan vara det, även om det säljs till en civil kund. Det är teknikens potential, inte kundens uniform, som avgör.

Det här är viktigt att ha klart för sig redan från början — både för att undvika onödig oro och för att inte missa de fall som faktiskt är relevanta.

Vad den här manualen ger dig

Som innovationsrådgivare möter du klienter som utvecklar och internationaliserar teknikintensiva produkter och tjänster. Det är i den miljön dual-use-frågor uppstår — inte som abstrakta regelverksproblem utan som konkreta situationer: ett techbolag som vill sälja sin mjukvara till en kund i ett land utanför EU, ett forskningsprojekt med internationella partners, en startup som ska presentera sin teknologi på en konferens utomlands, en utbytesforskare som ska ha tillgång till intern teknisk dokumentation.

De flesta klienter i den här miljön har aldrig hört talas om dual-use-regelverket. En del har hört talas om det men tror att det inte gäller dem — för de säljer ju inte vapen. Och en del har ett verkligt problem som de inte vet om.

Din roll är inte att vara exportkontrolljurist. Den är att ha tillräcklig förståelse för att känna igen när frågan är relevant, kunna ge klienten ett första orienterande perspektiv och veta när du ska eskalera till specialistkompetens. Det är en värdefull

funktion — för många klienter är du den första och enda person som kan fånga upp att de har ett problem innan det blir ett allvarligt ett.

Manualen ger dig det du behöver för det: förståelse för regelverkets logik, verktyg för att identifiera potentiellt kontrollerade produkter och transaktioner, de vanligaste scenarierna i innovationsrådgivning och en tydlig bild av när och hur du eskalerar. Den är skriven för att vara användbar i de gråzoner där teknisk förståelse och rättslig analys möts — vilket är exakt där de flesta exportkontrollproblem i praktiken uppstår.

Manualen är inte juridisk rådgivning och ersätter inte konsultation med ISP eller specialiserad jurist i komplexa fall. Den är ett levande dokument — Annex I uppdateras löpande och myndigheters praxis utvecklas. Kontrollera alltid att du arbetar med aktuella versioner av de regelverk som refereras.

Del 1 — Regelverkets grund

1.1 Varför exportkontroll finns

Exportkontroll är inte en modern uppfinning. Tanken att vissa varor och teknologier är för känsliga för att fritt exporteras till vem som helst har funnits länge och har vuxit fram ur säkerhetspolitiska erfarenheter under och efter andra världskriget. Det som förändrats över tid är vad som kontrolleras och varför.

Den grundläggande logiken är enkel: en del teknologi kan användas för att bygga vapen, övervaka befolkningar, destabilisera stater eller ge auktoritära regimer verktyg de annars inte skulle ha tillgång till. Marknaden löser inte detta på egen hand — en tillverkare av krypteringsmjukvara har inget naturligt incitament att fråga sig om kunden tänker använda produkten för att skydda dissidenter eller för att avlyssna dem.

Exportkontroll är statens svar på detta. Genom att kräva tillstånd för export av vissa produkter och teknologier skapar staten en kontrollpunkt där dessa frågor kan ställas och bedömas innan överföringen sker.

För teknikintensiva verksamheter — systemutvecklare, innovationsprojekt, forskningsinstitutioner — är detta relevant på ett sätt som ofta inte uppmärksammas. Exportkontroll associeras ofta med vapen och militär utrustning. I praktiken gäller det i lika hög grad mjukvara, algoritmer, krypteringsteknik, sensorer, halvledare och kunskap om hur system är uppbyggda.

1.2 Det internationella ramverket

EU:s dual-use-förordning är inte skapad i ett vakuum. Den är EU:s implementering av ett antal internationella exportkontrollregimer som förhandlats fram mellan länder med liknande säkerhetsintressen. För att förstå varför Annex I ser ut som det gör, och varför vissa teknologier kontrolleras och andra inte, behöver du känna till dessa regimer.

Wassenaar Arrangement grundades 1996 och har idag 42 deltagande stater, däribland Sverige och övriga EU-länder, USA, Japan och Australien. Wassenaar fokuserar på konventionella vapen och dual-use-produkter i bred mening och är den regim som ligger bakom många kontrollposter inom elektronik, datorer, telekommunikation och informationssäkerhet i Annex I.

Nuclear Suppliers Group (NSG) har 48 deltagande regeringar och kontrollerar produkter och teknik med koppling till kärnvapen och kärnenergi. NSG:s listor ligger till grund för de kärntekniska delarna av Annex I.

Australia Group har 42 deltagande länder och fokuserar på kemiska och biologiska vapen. Gruppen koordinerar exportkontroller för kemikalier, biologiska ämnen och relaterad utrustning.

Missile Technology Control Regime (MTCR) har 35 partners och reglerar export av raketer och relaterad teknik som kan bära massförstörelsevapen.

Annex I bygger sammantaget på samtliga fyra regimer, och olika delar av listan har sin grund i olika regimer beroende på produktkategori.

En viktig praktisk konsekvens: Annex I är inte statisk. Den uppdateras löpande genom delegerade akter när de internationella regimerna uppdaterar sina listor. En ny uppdatering antogs exempelvis den 8 september 2025 och publicerades som delegerad förordning EU 2025/2003. Du behöver alltid arbeta med den senaste versionen av Annex I — inte den som gällde när förordningen antogs 2021.

1.3 EU 2021/821 — förordningens struktur

EU:s dual-use-förordning, formellt förordning EU 2021/821, trädde i kraft den 9 september 2021 och ersatte den tidigare förordningen EU 428/2009. Den är en direkt tillämplig EU-förordning, vilket innebär att den gäller i alla medlemsstater utan att behöva omvandlas till nationell lagstiftning. Däremot kräver den nationella åtgärder för verkställighet och sanktioner, vilket innebär att den praktiska tillämpningen och sanktionsnivåerna kan variera något mellan länder.

Förordningen reglerar fem typer av kontrollerade transaktioner.

Export avser fysisk eller elektronisk utförsel av en produkt från EU:s tullområde till ett land utanför EU. Det inkluderar inte bara traditionell varuexport utan också elektronisk överföring av mjukvara och teknisk dokumentation.

Förmedling avser situationer där en person eller organisation i EU förhandlar om eller arrangerar transaktioner som innebär överföring av dual-use-produkter från ett tredjeland till ett annat tredjeland, eller köper och säljer sådana produkter i syfte att överföra dem mellan tredjeländer. Begreppet är snävare än allmänt affärsstöd — huruvida en persons roll i en transaktion utgör förmedling beror på transaktionens konkreta struktur och personens faktiska roll i den.

Tekniskt bistånd avser överföring av kunskap och kompetens — instruktioner, utbildning, konsultation — som kan användas för att utveckla, tillverka eller använda kontrollerade produkter.

Transitering avser transport av kontrollerade produkter genom EU:s tullområde när slutdestinationen är utanför EU.

Överföring inom EU är en specialkategori som gäller för de mest känsliga produkterna i Annex IV, där kontroll gäller även för förflyttning mellan EU-länder.

Förordningens bilagor är centrala för det praktiska arbetet. Annex I är den centrala kontrollistan och den du kommer att arbeta med mest. Annex II innehåller EU:s generella exporttillstånd som möjliggör export till vissa destinationer utan individuellt tillstånd för specifika produktkategorier. Annex III innehåller formulär och modeller för tillståndshandlingar. Annex IV listar de produkter som är så känsliga att de kräver

tillstånd även för överföring inom EU.

1.4 Nationell administration — ISP:s roll

Även om förordningen är direkt tillämplig administreras den nationellt. I Sverige är Inspektionen för strategiska produkter, ISP, den behöriga myndigheten. ISP handlägger tillståndsansökningar, genomför klassificeringsbedömningar, utfärdar vägledningar och samarbetar med tullen och andra myndigheter.

ISP publicerar vägledningar på isp.se och tar emot frågor från exportörer som är osäkra på om deras produkter eller transaktioner kräver tillstånd. Som innovationsrådgivare är det viktigt att känna till när en fråga bör ställas till ISP direkt.

ISP samarbetar med tullen för att kontrollera faktiska exportflöden och med andra EU-länders exportkontrollmyndigheter. Exportkontroll är med andra ord inte ett isolerat regelefterlevnadsproblem — det är ett säkerhetsrelaterat område där myndigheter aktivt övervakar flöden och aktörer.

Praktisk rekommendation: När du hjälper en klient med en dual-use-bedömning, dokumentera alltid arbetet noggrant. Om ISP eller tullen senare ställer frågor om en transaktion är det avgörande att klienten kan visa att de gjort en seriös och systematisk bedömning.

1.5 Grundläggande begrepp du behöver behärska

Exportör definieras i förordningen brett och täcker inte bara företag som ingår exportavtal utan även fysiska personer som för med sig kontrollerade produkter eller teknik när de lämnar EU, samt den som elektroniskt överför kontrollerad mjukvara eller teknik till mottagare utanför EU. Det är exportören som bär det primära ansvaret för att bedöma om tillstånd krävs.

Dual-use-produkter definieras som produkter, inklusive mjukvara och teknik, som kan användas för både civila och militära ändamål. Det inkluderar produkter som kan användas i samband med spridning av massförstörelsevapen. Det är inte produktens primära användningsområde som avgör utan dess potential för militär användning eller användning i samband med massförstörelsevapen.

Teknik i förordningens mening är specifik information som är nödvändig för utveckling, produktion eller användning av en produkt. Teknik kan ha många former: ritningar, specifikationer, manualer, formler, ingenjörssdesign, eller know-how som överförs muntligt eller genom demonstration.

Mjukvara behandlas i förordningen som en separat kategori från varor och teknik. Kontrollerad mjukvara inkluderar inte bara kommersiell mjukvara utan också källkod, algoritmer och specifika programvarukomponenter som uppfyller kontrollkriterierna.

Slutanvändare och slutanvändning är centrala begrepp i tillståndsbedömningen. Tillståndsbedömningen och exportens tillåtlighet kan variera beroende på

slutanvändare och slutanvändning, även om produktens listningsstatus i Annex I i sig är densamma.

Public domain är ett viktigt undantagsbegrepp i kontrollistan. Information som är genuint allmänt tillgänglig utan åtkomstbegränsningar faller i regel utanför tekniköverföringskontrollen. Public domain i exportkontrollrättslig mening är ett definierat undantag, inte ett allmänt internetbegrepp. Huruvida specifik teknisk information faller inom undantaget kräver alltid en konkret bedömning.

Basic scientific research är ett annat undantagsbegrepp. Grundläggande vetenskaplig forskning som inte är inriktad mot en specifik praktisk tillämpning faller utanför kontrollen av tekniköverföring. Tillämpad forskning med tydliga tekniska output gör det däremot inte, och gränsdragningen kan i praktiken vara svår att göra.

1.6 Ansvar och kunskapströsklar

En av de viktigaste principerna i dual-use-regelverket är att okunnighet inte är ett försvar. Exportören förväntas känna till regelverket och göra en aktiv bedömning av sina produkter och transaktioner.

Förordningen arbetar med flera olika kunskapströsklar beroende på situation, och det är viktigt att du förstår skillnaden mellan dem.

Faktisk kännedom — exportören vet att produkten eller tekniken är avsedd för ett kontrollerat eller förbjudet ändamål. Här är tillståndsplikt eller exportförbud tydligt.

Skäl att misstänka — exportören har information som ger anledning att misstänka problematisk slutanvändning, utan att ha full kännedom. Förordningens catch-all-regler kan aktualiseras bland annat när exportören har skäl att misstänka att produkten är avsedd för massförstörelsevapen eller militär slutanvändning i ett vapenembargerat land.

Myndighetsunderrättelse — ISP eller annan behörig myndighet har informerat exportören om att en specifik transaktion eller kund är problematisk. Efter en sådan underrättelse kan exportören inte längre hävda okunnighet.

I rådgivningsarbetet innebär detta att du behöver hjälpa klienter att bygga system för att du behöver hjälpa klienter att bygga system för att identifiera potentiellt kontrollerade produkter och transaktioner, bedöma slutanvändare och slutanvändning, dokumentera sina bedömningar löpande, och eskalera osäkra fall till ISP eller juridisk rådgivning.

1.7 Sanktioner och konsekvenser

Överträdelser av dual-use-förordningen hanteras i Sverige genom lag (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd. Sanktionerna är differentierade beroende på överträdelsens allvar.

Grova överträdelser kan ge fängelse i lägst sex månader och högst sex år. Mindre

allvarliga överträdelser kan ge böter eller fängelse upp till två år. Utöver straffrättsliga påföljder kan export stoppas eller tillstånd nekas, och affärsrelationer med internationella partners kan skadas allvarligt.

Straffrättsligt ansvar kan utkrävas av de fysiska personer vars handlande uppfyller rekvisiten i den svenska sanktionslagstiftningen — det vill säga de individer som faktiskt fattat eller verkställt beslut om en olaglig export.

Del 2 — Förstå tillämpningsområdet

2.1 Den grundläggande frågan

Innan du kan göra en klassificering eller bedöma om tillstånd krävs måste du avgöra en mer grundläggande fråga: är dual-use-förordningen överhuvudtaget aktuell i den situation du tittar på?

Den praktiska frågan du alltid ställer först är denna: finns det en produkt, mjukvara, teknik eller kunskap som potentiellt är kontrollerad, och sker eller planeras en överföring av den till någon utanför EU?

Om svaret på båda delarna är ja, eller kanske, går du vidare med en klassificeringsbedömning. Om svaret på någon av delarna är nej behöver du förstå varför innan du avslutar bedömningen.

2.2 Vad som kan vara kontrollerat

Varor är fysiska produkter. Att en vara normalt sett är kontrollerad innebär att den finns listad i Annex I med specifika tekniska parametrar som avgör om just den produkten träffas. Men även olistade varor kan omfattas av kontroll genom catch-all-reglerna — listning i Annex I är alltså inte den enda vägen till tillståndsplikt.

Mjukvara behandlas separat från varor och teknik. Det avgörande är inte hur mjukvaran distribueras utan om den uppfyller de tekniska kontrollkriterierna i Annex I eller träffas av catch-all-reglerna.

Teknik i förordningens mening är specifik information som är nödvändig för utveckling, produktion eller användning av en kontrollerad produkt. Det avgörande är att informationen är specifik och nödvändig i förhållande till en kontrollerad produkt.

Tekniskt bistånd är en variant av tekniköverföring med fokus på den personliga kunskapsöverföringen — utbildning, instruktioner, konsultation, demonstrationsaktiviteter.

2.3 Vad som utgör export och överföring

Fysisk export är den klassiska formen — en vara packas och skickas till ett land utanför EU.

Elektronisk överföring av mjukvara eller teknisk dokumentation från EU:s territorium till en mottagare utanför EU är export i förordningens mening. Det avgörande är att överföringen sker från EU — en server belägen utanför EU som gör information tillgänglig för en mottagare i tredjeland utgör inte en EU-export.

Muntlig kunskapsöverföring — att förklara hur något fungerar, ge instruktioner, hålla en föreläsning eller genomföra en demonstration — kan utgöra tekniskt bistånd och falla inom förordningen.

Personligt bagage är en kategori som ofta förbises. En forskare som reser från EU till en konferens utomlands och tar med sig kontrollerat material kan i vissa situationer anses vara exportör.

Fjärråtkomst till system inom EU kan i vissa fall utgöra export om åtkomsten ges till en person utanför EU och möjliggör nedladdning eller kopiering av kontrollerat material.

Intangible Technology Transfer (ITT) är samlingsnamnet för alla former av icke-fysisk överföring av kontrollerad teknik — elektronisk, muntlig eller visuell.

2.4 Vem som är exportör

Exportörsdefinitionen är knuten till vem som ingår exportavtalet, fattar beslutet om export och kontrollerar överföringen. Ansvar kan i olika situationer falla på organisationen, individen eller båda.

En fysisk person som reser utomlands med kontrollerat material kan i vissa situationer anses vara exportör. En forskare som presenterar kontrollerad teknisk information vid en konferens utomlands kan i vissa situationer anses vara exportör. En utländsk student som får tillgång till kontrollerad teknik och återvänder hem med kunskapen — ett scenario som i internationell praxis ibland kallas *deemed export* (ett informellt praktikuttryck, inte ett definierat begrepp i EU 2021/821) — kan vara mottagare av en export.

2.5 Destinationslandets betydelse

Länder med vapenembargo — export kan vara förbjuden eller kräva tillstånd även för produkter som normalt inte är tillståndspliktiga, genom sanktionsregler och catch-all-regler.

Länder med generellt exporttillstånd — EU001 täcker Australien, Kanada, Island, Japan, Nya Zeeland, Norge, Schweiz, Liechtenstein, Storbritannien och USA. Ytterligare generella tillstånd finns för specifika situationer.

Alla övriga länder och situationer — för länder och situationer som inte täcks av ett relevant generellt exporttillstånd krävs normalt individuellt eller globalt tillstånd för listade produkter.

2.6 Undantagen du behöver känna till

Public domain-undantaget och basic scientific research-undantaget är de två etablerade undantagen. Det finns inga generella undantag i EU 2021/821 för personliga tillhörigheter, konsumentprodukter eller varor som returneras till ursprungslandet. Bedömningen görs alltid mot Annex I och catch-all-reglerna.

2.7 De röda flaggorna — när du ska reagera direkt

Följande situationer ska alltid utlösa en fördjupad bedömning:

Destinationen: land med vapenembargo, känt spridningsprogram eller restriktiva EU-åtgärder.

Slutanvändaren: militär, statlig säkerhetsapparat, oklar identitet eller koppling till försvars-/underrättelsesektorn.

Produktens karaktär: kryptering, sensorteknik, navigeringssystem, halvledare med höga prestanda, cybersäkerhetsverktyg.

Transaktionens struktur: ovanlig betalnings- eller leveransstruktur, svåridentifierad slutanvändare, omotiverad mellanhand.

Forsknings- och utbildningskontext: utländsk student eller utbytesforskare med tillgång till intern teknisk information, anställd som reser med tekniskt material.

2.8 Din arbetsprocess i detta steg

Kartlägg vad som ska överföras. Identifiera vem som är inblandad. Fastställ destinationen. Identifiera slutanvändaren och slutanvändningen. Kontrollera röda flaggor. Dokumentera bedömningen oavsett slutsats.

Del 3 — Klassificering och navigering av Annex I

3.1 Vad klassificering innebär och varför det är centralt

Klassificering är processen att avgöra om en specifik produkt, mjukvara eller teknik träffas av en kontrollpost i Annex I — och i så fall vilken. En felaktig klassificering i ena riktningen innebär export utan tillstånd. En felaktig klassificering i andra riktningen innebär onödig tillståndsansökan — mindre riskfyllt rättsligt men kostsamt och operativt störande.

Klassificering är exportörens ansvar. En viktig distinktion: klassificering och tillståndsbedömning är inte samma sak. Klassificering avgör om en produkt är listad. Tillståndsbedömning avgör om export av den produkten till ett specifikt land och en specifik slutanvändare kräver tillstånd.

3.2 Annex I:s struktur

De tio kategorierna

Kategori 0: kärnmaterial, anläggningar och utrustning. Kategori 1: specialmaterial och relaterad utrustning. Kategori 2: materialbearbetning. Kategori 3: elektronik — halvledare, integrerade kretsar. Kategori 4: datorer. Kategori 5: telekommunikation (del 1) och informationssäkerhet (del 2) — inkluderar varor, mjukvara och teknik med kryptografiska funktioner. Kategori 6: sensorer och lasrar. Kategori 7: navigering och flygelektronik. Kategori 8: marin teknik. Kategori 9: flyg- och rymdteknik samt framdrivning.

De fem produktgrupperna

Grupp A: system, utrustning och komponenter (fysiska varor). Grupp B: test-, inspektions- och produktionsutrustning. Grupp C: material. Grupp D: mjukvara. Grupp E: teknik.

Kontrollpostnumret kombinerar kategori och grupp. 5A002 = kategori 5, grupp A, post 002.

3.3 De allmänna anmärkningarna — GTN, GSN och GDN

Läs alltid dessa anmärkningar i sin faktiska ordalydelse i Annex I. Beskrivningarna nedan är orienterande, inte fullständiga återgivningar.

General Technology Note (GTN) anger att kontrollen av teknik inte gäller information i public domain, basic scientific research eller information som är det minimum som krävs för patent. Tekniken måste vara specifikt nödvändig för att utveckla, producera eller använda en listad produkt.

General Software Note (GSN) anger att kontrollen av mjukvara inte gäller mjukvara i public domain. GSN innehåller också ett separat undantag för viss allmänt

tillgänglig mjukvara som säljs från lagerställe utan restriktioner och kan installeras utan väsentligt leverantörsstöd. Bedömningen måste göras mot GSN:s exakta ordalydelse.

General Note for Dual-Use (GDN) innehåller ytterligare avgränsningar. Läs alltid GDN i sin helhet i Annex I. Den utgör inte ett generellt undantag för konsumentprodukter.

3.4 Hur du läser en kontrollpost

Läsordning: (1) Kontrollmeningen — vad kontrolleras. (2) Tekniska parametrar — gränsvärden och egenskaper som avgör om produkten träffas. (3) Undantag och noter inom posten. (4) Tillämpa GTN, GSN eller GDN om relevant.

3.5 Klassificeringsprocessen steg för steg

Steg 1 — Samla produktinformation. Funktion, tekniska specifikationer, uppbyggnad, militära tillämpningar. För mjukvara: funktioner, kryptografiska komponenter, distributionssätt. För teknik: exakt information som ska överföras, specificitetskrav, public domain-status.

Steg 2 — Identifiera möjliga kategorier. Kontrollera alla relevanta kategorier, inte bara den mest uppenbara.

Steg 3 — Läs de relevanta kontrollposterna. Jämför faktiska specifikationer med kontrollpostens parametrar.

Steg 4 — Tillämpa de allmänna anmärkningarna. GTN, GSN eller GDN beroende på vad som klassificeras.

Steg 5 — Bedöm catch-all även om produkten är olistad. Finns kännedom om eller skäl att misstänka problematisk slutanvändning?

Steg 6 — Dokumentera din klassificering. Produktbeskrivning, kontrollposter undersökta, slutsats per post, GTN/GSN/GDN-bedömning, catch-all-bedömning.

3.6 Kategori 5 del 2 — informationssäkerhet i praktiken

Kategori 5 del 2 kontrollerar vissa varor, mjukvaror och tekniker med kryptografiska funktioner — primärt posterna 5A002, 5D002 och 5E002. Dessa poster innehåller egna noter och undantag med specifika tekniska kriterier som måste läsas i Annex I. Det är ett av de områden där tumregler är farligast. Varje mjukvara med kryptografiska funktioner ska analyseras mot kategori 5 del 2. Vid osäkerhet, kontakta ISP.

3.7 När du är osäker — klassificeringsbesked från ISP

Tre alternativ: (1) Fördjupad teknisk analys med teknisk expertis. (2) Kontakt med

ISP för vägledning — ett formellt klassificeringsbesked ger starkt stöd för klassificeringen och minskar den rättsliga risken väsentligt, förutsatt att lämnade uppgifter är korrekta. (3) Försiktighetsprincipen — behandla produkten som kontrollerad tills frågan är utredd.

3.8 Klassificering av mjukvara — särskilda överväganden

Funktionen avgör, inte marknadsföringen. Både källkod och kompilerad mjukvara kan vara kontrollerade — bedömningen beror på den specifika kontrollposten. Mjukvara med kryptografiska funktioner utlöser alltid kategori 5 del 2-analys. Open source är inte automatiskt undantaget — bedöm mot GSN:s exakta ordalydelse.

3.9 Klassificering av teknik — särskilda överväganden

Specificitetskravet är centralt — tekniken måste vara specifikt nödvändig för en konkret listad produkt. Information i public domain och basic scientific research faller utanför kontrollen av teknik enligt GTN. Muntlig tekniköverföring är lika kontrollerad som skriftlig. Teknik för underhåll kan vara kontrollerad.

3.10 Dokumentationsstandard

Varje klassificeringsbedömning dokumenteras med: datum och vem som gjort bedömningen; produktbeskrivning och specifikationer; kontrollposter undersökta och varför; slutsats per post med motivering; GTN/GSN/GDN-påverkan; catch-all-bedömning; slutlig klassificering med kontrollpostnummer eller konstaterande att produkten är olistad. ISP-kontakter och formella klassificeringsbesked ska framgå med datum och referensnummer.

Del 4 — Scenarion och bedömningsguide

4.1 Hur du använder den här delen

Del 4 går igenom de vanligaste situationerna du möter i dual-use-arbetet. Varje scenario följer strukturen: situationsbeskrivning, frågor du ställer, bedömning och åtgärder. Använd scenarierna som referenspunkter, inte som mallar. Dokumentera alltid din bedömning.

4.2 Scenario 1 — Produktexport

Frågorna du ställer

Vad är produkten tekniskt? Vart ska den? Vem är slutanvändaren och vad ska den användas till? Finns röda flaggor?

Bedömningen

Klassificera mot Annex I. Om listad: individuellt tillstånd eller generellt exporttillstånd tillämpligt? Om olistad: catch-all-triggers?

Åtgärder

Listad med individuellt tillståndskrav: stöd klienten i tillståndsansökan. ISP kräver i regel slutanvändarintyg i original. Listad med generellt tillstånd: säkerställ att villkoren uppfylls och anmälan gjorts. Olistad utan triggers: dokumentera. Olistad med triggers: avvakta, kontakta ISP.

4.3 Scenario 2 — Export av mjukvara och källkod

Frågorna du ställer

Vad gör mjukvaran? Innehåller den kryptografiska funktioner? Kan den användas för intrång eller övervakning? Hur levereras den? Är den öppen källkod?

Bedömningen

Kryptografiska funktioner: alltid mot 5D002/5A002. Intrångsmjukvara: mot kategori 4 och 5 samt artikel 5 catch-all. Open source: bedöm mot GSN:s ordalydelse.

Åtgärder

Kontrollerad mjukvara: ordinarie tillståndsprocess. Cyberövervaknings-catch-all: kontakta ISP. Ställ alltid frågan om kryptografiska funktioner även om mjukvaran marknadsförs för annat syfte.

4.4 Scenario 3 — Teknisk dokumentation och know-how

Frågorna du ställer

Vad innehåller dokumentationen? Är det specifik information nödvändig för en kontrollerad produkt? Är produkten listad i Annex I? Är informationen i public domain?

Bedömningen

Teknik kontrolleras under grupp E. Tillämpa GTN. Tekniskt bistånd måste bedömas parallellt med teknisk dokumentation — de är separata rättsliga mekanismer i förordningen.

Åtgärder

Tillståndsplikt måste bedömas under både teknikreglerna och biståndsreglerna. Vid osäkerhet: kontakta ISP.

4.5 Scenario 4 — Forskare som reser utomlands

Material som tas med fysiskt bedöms som fysisk export. Presentationer och muntliga diskussioner bedöms under både teknik- och biståndsreglerna. Publicerad forskning i public domain faller normalt under GTN. Akademisk kontext är inte avgörande — det är informationens karaktär och mottagarnas hemland som räknas.

Genomför en genomgång av vad personen tar med och vad som presenteras innan resan. Om osäkerhet: begränsa till publicerat material eller kontakta ISP.

4.6 Scenario 5 — Utbytesforskare och utländska studenter

Bedömningen är alltid konkret, inte automatisk. Generell utbildning faller normalt under GTN. Specifik tillgång till opublicerad teknisk information om listade produkter kan vara exportkontrollrelevant. Hemlandets status är central — länder med vapenembargo, högriskländer eller kända spridningsprogram kräver alltid fördjupad bedömning.

Genomför due diligence innan vistelsen börjar. Rådge klienter att bygga in exportkontrollbedömning i onboarding-processen för utländska gäster.

4.7 Scenario 6 — Molntjänster och fjärråtkomst

Det avgörande är att överföringen sker från EU. Fjärråtkomst till system inom EU som möjliggör nedladdning av kontrollerat material kan utgöra export. Åtkomst med tekniska begränsningar mot extraktion är ett rättsligt och tekniskt gränsfall. Kontakta ISP i komplexa fall — rättspraxis på detta område utvecklas fortfarande.

4.8 Scenario 7 — Internationella forskningssamarbeten

Grundforskning med publicerade resultat faller normalt under GTN. Tillämpad forskning med tekniska lösningar och listade produkter kräver noggrann bedömning. Genomför due diligence innan samarbetsavtal tecknas. Inkludera

exportkontrollklausuler i avtalet. Kontakta ISP för komplexa samarbeten med partners i länder utan generella exporttillstånd.

4.9 Scenario 8 — Konsultuppdrag och teknisk rådgivning

Teknisk rådgivning med specifik information om kontrollerade produkter till mottagare utanför EU kan utgöra tekniskt bistånd. Den muntliga informationen kanske inte överförs från EU om du är på plats hos kunden, men resan och det medförda materialet kan ändå aktualisera exportkontroll. Bedöm tillståndsfrågan under både teknik- och biståndsreglerna innan uppdraget inleds.

4.10 Snabbguide — röda flaggor och direkta åtgärder

Eskalera omedelbart för fördjupad bedömning om:

Land med EU-vapenembargo. Militär eller statlig säkerhetsapparat som slutanvändare. Kunden vägrar uppge slutanvändning. Produkten innehåller kryptografiska funktioner. Avancerad elektronik, sensor eller navigeringssystem. Utländsk person från högriskland ska ha tillgång till intern teknisk information. Anställd eller forskare reser till högriskland med tekniskt material.

Ingen av dessa situationer innebär automatiskt tillståndsplikt — de innebär att en fördjupad bedömning krävs.

Kontakta ISP om:

Du inte kan avgöra om produkten är listad efter klassificeringsbedömning. Du identifierar catch-all-triggers men är osäker på tröskeln. Teknik- eller mjukvaruöverföring till land utan generellt exporttillstånd. Klienten behöver ett mer systematiskt förhållningssätt.

Dokumentera alltid:

Vad som bedömts. Mot vilka kontrollposter. Vilken slutsats och varför. Vem och när.

Del 5 — Åtgärder och eskalering

5.1 Det grundläggande beslutsträdet

Läge 1 — Listad, individuellt tillstånd krävs: Exporten får inte genomföras utan tillstånd. Initiera tillståndsansökan till ISP.

Läge 2 — Listad, generellt exporttillstånd tillämpligt: Säkerställ att villkoren uppfylls och att anmälan gjorts.

Läge 3 — Olistad, inga catch-all-triggers: Exporten kan genomföras. Dokumentera bedömningen.

Läge 4 — Olistad med catch-all-triggers, eller oklar situation: Exporten ska inte genomföras förrän frågan är utredd.

5.2 När du avvaktar

Avvakta och utred vidare när: du identifierat möjliga catch-all-triggers men är osäker på tröskeln; klassificeringen är oklar på grund av otillräckliga tekniska specifikationer; ny information har framkommit som kan påverka slutsatsen; situationen inte täcks av standardscenarierna i del 4.

5.3 Individuell tillståndsansökan till ISP

Vad ansökan innehåller

Exportöruppgifter. Mottagaruppgifter och slutanvändaruppgifter. Produktbeskrivning med kontrollpostnummer. Teknisk beskrivning. Slut användningsuppgifter. Destinationsland. Värde och kvantitet. Slut användarintyg i original — ISP kräver i regel original som bekräftar avsedd användning och åtagande om icke-vidareexport. Originalen ska bevaras hos exportören.

Processen

Ansökan via ISP:s ärendehanteringssystem. Påskyndad handläggning medges normalt inte. Erfarenhetsmässigt: räkna med minst några veckor för okomplicerade ärenden, betydligt längre för komplexa. ISP kan bevilja, bevilja med villkor eller avslå.

Tidsplanering

Initiera alltid exportkontrollbedömningen tidigt i affärsprocessen, inte som sista steg innan leverans.

5.4 Generella exporttillstånd — villkor och anmälan

EU001: brett spektrum av Annex I-produkter till Australien, Kanada, Island, Japan, Nya Zeeland, Norge, Schweiz, Liechtenstein, Storbritannien och USA. EU002: vissa

kategori 1 och 3-produkter till Argentina, Sydafrika, Sydkorea och Turkiet. EU003: export efter reparation/ersättning. EU004: tillfällig export för utställningar och mässor. EU005: viss telekommunikationsutrustning. EU006: vissa kemikalier. EU007: viss koncernintern export av teknik och mjukvara för civil produktutveckling. EU008: vissa informationssäkerhetsprodukter inklusive mjukvara i kategori 5 del 2.

Varje tillstånd har egna villkor som måste läsas i Annex II. Användning kräver ofta anmälan till ISP — för flera tillstånd ska en engångsanmälan göras senast 30 dagar efter första exporttillfället. Kontrollera alltid aktuella krav på isp.se.

5.5 Eskalering — när och till vem

Eskalera till ISP när:

Du inte kan avgöra om produkten är listad. Du identifierar catch-all-triggers men är osäker på tröskeln. Okänd destination, slutanvändare eller produktkategori. Klienten genomfört export utan tillstånd. Osäkerhet om förmedling eller tekniskt bistånd.

Vägledningskontakt med ISP är normalt en del av den ordinarie dialogen och är i sig inte samma sak som ett sanktionsärende.

Eskalera till specialiserad jurist när:

Möjligt straffrättsligt ansvar. Föreläggande från ISP eller tullen. Komplexa frågor om förmedling eller tekniskt bistånd. Parallell tillämpning av andra jurisdiktioners regler, särskilt EAR eller ITAR.

Eskalera till klientens ledning när:

Klienten saknar grundläggande exportkontrollprocesser. Export genomförd eller planeras utan tillstånd trots att det krävs. Klienten ovillig att följa rådgivning. Dokumentera din rådgivning och klientens reaktion.

5.6 Hantering av situationer där export skett utan tillstånd

Dokumentera situationen omedelbart. Bedöm allvarlighetsgraden. Involvera juridisk rådgivning med straffrättslig kompetens tidigt om straffrättsliga konsekvenser kan föreligga — innan kontakter tas med myndigheter. Proaktiv kontakt med ISP kan i vissa situationer vara lämplig och kan vara bättre än att myndigheten upptäcker förhållandet på annat sätt, men beslutet fattas i samråd med juridisk rådgivning. Hjälp klienten att bygga bättre processer.

5.7 Interna exportkontrollprogram (ICP)

Ett fullständigt ICP är inte ett generellt krav för alla exportörer, men det är starkt rekommenderat och i vissa delar av regelverket uttryckligen relevant (artikel 2.21 i EU 2021/821). Ett grundläggande ICP innehåller: ledningsengagemang och ansvarsfördelning; klassificeringsprocesser; slutanvändarbedömning; utbildning;

dokumentation och arkivering; avvikelshantering.

5.8 Gränsdragningar för exportkontrollrådgivning — översikt

Det här avsnittet beskriver vad en exportkontrollspecialist kan bidra med, och var gränsen går mot juridisk specialistkompetens. Det ger dig som innovationsrådgivare en orientering om vad som typiskt sker när ett ärende eskaleras.

En exportkontrollspecialist kan stödja och genomföra klassificeringsbedömningar på uppdrag av exportören, identifiera catch-all-triggers, bistå i tillståndsansökningar, ge råd om generella exporttillstånd, hjälpa klienter att bygga interna compliance-program (ICP) samt bistå i kontakt med ISP för vägledning.

Specialiserad juridisk kompetens bör involveras när det finns risk för straffrättsligt ansvar, vid parallell eller potentiell extraterritoriell tillämpning av EAR eller ITAR, vid komplexa analyser av förmedling eller tekniskt bistånd, eller när djup teknisk specialistkompetens krävs för att bedöma produktens funktion eller prestanda.

5.9 Dokumentationsstandard för åtgärder

Dokumentationen innehåller: datum och beslutsfattare; hänvisning till klassificeringsbedömning; vilket läge (1-4); vidtagen åtgärd; ISP-kontakter med datum och svar; tillståndsansökan med beslut och villkor; generellt tillstånd med motivering och villkorsuppfyllelse. Bevara dokumentationen i minst fem år, gärna längre. Den exakta straffrättsliga preskriptionstiden varierar och bör vid behov hanteras med juridisk rådgivning.

Del 6 — Från identifiering till eskalering

6.1 Din roll i dual-use-arbetet

Som innovationsrådgivare är du ofta den första person som möter en klient med ett potentiellt dual-use-problem. Din roll är inte att lösa det — den är att känna igen det, ge klienten ett orienterande perspektiv och säkerställa att rätt kompetens kopplas in i rätt tid.

Det är en värdefull funktion. Många klienter saknar helt kännedom om regelverket. En del tror att det inte gäller dem. Andra anar att de borde ta reda på det men skjuter upp frågan. Du är den som kan fånga upp problemet innan det blir allvarligt.

6.2 Vad du kan bidra med

Du kan hjälpa klienten att förstå vad dual-use-regelverket faktiskt är och varför det kan vara relevant för deras verksamhet. Du kan ställa de inledande frågorna: vad ska exporteras, vart, till vem och för vilket ändamål. Du kan identifiera röda flaggor enligt genomgången i del 2 och 4. Du kan förklara vad en klassificeringsbedömning innebär och varför den behöver göras. Du kan råda klienten att inte genomföra en planerad export förrän frågan är utredd.

Det du ska vara tydlig med är att du inte uppträder som om du lämnar en auktoritativ specialistbedömning när du inte har den kompetensen. Rättsligt är det exportören som ansvarar för att klassificera eller utreda klassificeringen — din roll är att hjälpa klienten att förstå det ansvaret och komma rätt.

6.3 När du eskalerar — och till vem

Eskalera till person med dokumenterad exportkontrollkompetens när:

Du identifierat röda flaggor och inte kan avgöra om produkten eller transaktionen är kontrollerad. Klienten planerar export av mjukvara med kryptografiska funktioner, avancerad elektronik, sensorteknik eller navigeringssystem. Mottagaren är militär, statlig säkerhetsapparat eller oklar aktör. Destinationen är ett land med vapenembargo, kända spridningsprogram eller restriktiva EU-åtgärder. Utländsk person från ett högriskland ska ha tillgång till klientens interna tekniska information. Klienten har genomfört export utan att ha gjort en exportkontrollbedömning.

En exportkontrollspecialist med dokumenterad erfarenhet av klassificering, tillståndsbedömning och ISP-kontakter bör involveras för den fördjupade

bedömningen. Vid möjliga straffrättsliga konsekvenser ska dessutom jurist med straffrättslig kompetens involveras tidigt.

6.4 ISP som resurs för exportören

ISP tar emot vägledningsfrågor från exportörer och lämnar skriftliga bedömningar av klassificering vid produktförfrågan. Det är normalt exportören eller den specialist som bistår exportören som bör hantera den materiella kontakten med ISP, men du kan informera klienten om möjligheten och om värdet av att inhämta sådan vägledning. Ett skriftligt besked från ISP ger starkt stöd för klassificeringen och minskar den rättsliga risken väsentligt, förutsatt att lämnade uppgifter är korrekta.

6.5 Dokumentera din bedömning

Även när din roll är begränsad till identifiering och eskalering — dokumentera. Vad klienten beskrivit, vilka röda flaggor du identifierat, vilket råd du gett och när. Det underlättar spårbarhet, intern uppföljning och senare bedömning av vad som faktiskt identifierats och kommunicerats.

Appendix — Nyckelreferenser och primärkällor

Förordningar och lagtext

EU 2021/821 — Förordningen om kontroll av export av dual-use-produkter. Tillgänglig på EUR-Lex.

EU 2025/2003 — Delegerad förordning med senaste uppdatering av Annex I (september 2025). Tillgänglig på EUR-Lex.

Lag (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd. Svensk implementering av sanktioner.

Myndigheter och vägledning

ISP — Inspektionen för strategiska produkter: isp.se. Tillståndsansökningar, klassificeringsvägledning, PDA-information.

EU-kommissionen — Dual-use trade controls: trade.ec.europa.eu. Kommissionens vägledningar och informationsnoter.

EU-kommissionens rekommendation 2021/1700 om intern efterlevnad för forskning med dual-use-produkter.

Internationella exportkontrollregimer

Wassenaar Arrangement: wassenaar.org. Nuclear Suppliers Group: nuclearsuppliersgroup.org. Australia Group: australiagroup.net. MTCR: mtcr.info.

Angränsande regelverk

AI Act (EU 2024/1689). NIS2 (EU 2022/2555). CRA (EU 2024/2847). GDPR (EU 2016/679). CLOUD Act (USA, 2018). Data Act (EU 2023/2854). DORA (EU 2022/2554).

Timo Lagerbjelke | lagerbjelke.se | Version 1.0, Mars 2026