



EUROPEISKA
KOMMISSIONEN

Bryssel den 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

BILAGOR

till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

**om inrättande av en ram med åtgärder för att stärka Europas moln- och AI-ekosystem
(förordningen om moln- och AI-utveckling)**

{SEC(2026) 502 final} - {SWD(2026) 502 final} - {SWD(2026) 503 final}

BILAGA I

STORA UTMANINGAR

1. Stor utmaning 1: Miljömässig hållbarhet, prestanda och säkerhet hos unionens datorcentraler

Prova och införa teknik för datorcentraler i hela unionen för att överträffa den senaste tekniken för energi- och resurseffektivitet.

Detta inbegriper att uppnå lägre energianvändningseffektivitet (PUE) och möjliggöra en betydligt högre utnyttjandegrad för servern. Här följer ett antal exempel:

- (1) **Sänka den genomsnittliga energianvändningseffektiviteten:** Förbättra den miljömässiga hållbarheten och miljöprestandan hos unionens datorcentraler för moln- och kantdatateknik till en genomsnittlig energianvändningseffektivitet på 1,15 i hela unionen. De viktigaste fokusområdena inbegriper att möjliggöra utvecklingen av
 - (a) avancerad teknik för datorcentralernas energieffektivitet, däribland kylning och återvinning av spillvärme,
 - (b) kvantdatorteknik för driften av moln- och datorinfrastruktur,
 - (c) nätintegrering och avancerade energiledningssystem,
 - (d) pilotlinjer för valideringen av nästa generations energieffektiva teknik på operativ nivå.
- (2) **Öka den genomsnittliga utnyttjandegraden för datorcentralernas servrar:** Öka den genomsnittliga utnyttjandegraden för servrarna i alla unionens datorcentraler med 50 %, till exempel genom att integrera AI-baserad teknik för hantering av dynamisk serveranvändning, hantering och schemaläggning av arbetsbelastningen eller balansering av utnyttjandegrad, energikostnad, termiska begränsningar och latenskrav.
- (3) **Förbättra datorcentralernas säkerhet och motståndskraft:** Förbättra säkerheten och motståndskraften hos datorcentralernas värde- och försörjningskedjor genom att integrera halvledarteknik och kvantteknik som utformats och tillverkats i unionen, och genom att förbättra deras motståndskraft mot fysiska hot och cyberhot, inbegripet riktade attacker.

2. Stor utmaning 2: Molnstackar

Bygga upp fullständiga molnstackar för maskinvara och programvara, inklusive AI-verktyg, infrastruktur, tjänster och förvaltningsnivåer för att överbrygga unionens kritiska kapacitetsklyftor.

Detta inbegriper att bygga AI-servrar som drivs med halvledare och kvantteknik som utformats och tillverkats i unionen för distribuerade och decentraliserade moln- och kantdatorsystem för AI.

Pilotprogram kan bidra till att visa kapaciteten hos de europeiska öppna molnstackarna inom strategiskt viktiga sektorer.

3. Stor utmaning 3: Banbrytande AI

Utveckla nästa generation av multimodala modeller och system för banbrytande AI och bana väg för utvecklingen av nya möjligheter.

Fokus kommer att ligga på den arkitektoniska utformningen och utvecklingen av nästa generations multimodala modeller och system som flyttar gränserna för de nuvarande algoritmiska möjligheterna för att uppnå överlägsen prestanda inom avancerad slutledningsförmåga, tvärmodal förståelse och agentisk förmåga, samt undersöka nya metoder för modelleffektivitet, kognitiva modeller, alternativa datorstrukturer osv.

De möjliga användningsområdena skulle kunna omfatta grundforskning, däribland vetenskapliga upptäckter och komplex datatolkning, och utveckling av världsmodeller för bättre slutledningsförmåga, automatiserad hanteringssimulering och planering.

4. Stor utmaning 4: Fysisk AI

Utveckla avancerade fysiska AI-modeller och AI-system som fungerar självständigt och säkert för att möjliggöra tillförlitliga funktioner för manipulering och navigering i ostrukturerade miljöer.

Fokus kommer att ligga på gemensam utformning av programvaran och dess underliggande maskinvaruarkitektur och på att kombinera banbrytande AI-teknik med världsmodeller som stöder fysisk slutledningsförmåga för att möjliggöra tillförlitliga funktioner för manipulering, navigering och interaktion med minimal mänsklig övervakning.

De möjliga användningsområdena kan omfatta autonoma robotar, industrisystem och drönare som används i dynamiska verkliga miljöer.

5. Stor utmaning 5: Industriell AI

Påskynda utvecklingen och införandet av europeisk industriell AI inom unionens strategiska sektorer.

Fokus kommer att ligga på att utveckla europeiska industriella AI-modeller och AI-system som kan betjäna värdefulla industriella tillämpningar. Modellerna och systemen bör kunna anpassas till sektorsspecifika användningsfall och möjliggöra ett säkert införande.

De initiativ som inleds inom ramen för denna stora utmaning bör bygga på de specialiserade datorresurser och provningsanläggningar som krävs för att validera AI-system i verkliga miljöer innan de införs i stor skala, inbegripet på regional och lokal nivå.

Inom fordonssektorn kan dessa initiativ underlätta utvecklingen och införandet av innovativa programvaruplattformar och AI-modeller för automatisk körning, och inom tillverkningsindustrin kan de bidra till att skapa specialiserade modeller som optimerar produktionsprocesserna. Andra strategiska sektorer som skulle kunna dra nytta av industriell AI kan omfatta hälso- och sjukvård, energi, jordbruksbaserade livsmedel och försvar.

6. Stor utmaning 6: Samverkande europeiska industriella modeller

Utveckla samverkande europeiska industriella AI-modeller och AI-system inom strategiska sektorer genom att möjliggöra samarbete på europeisk industrinivå utan att röja kommersiellt känsliga uppgifter mellan deltagarna.

Fokus kommer att ligga på avancerad teknik som bevarar konfidentialiteten. Dessa mekanismer omfattar strategier för federerad och distribuerad träning där algoritmerna skickas till data snarare än att data överförs centralt, säkra exekveringsmiljöer, krypteringsbaserad behandling, anonymiserings- och pseudonymiseringsteknik, uppdelning av åtkomsträttigheter och skydd mot extrahering av kommersiellt känslig information ur tränade modeller.

Strategiska sektorer som skulle kunna dra nytta av samverkande europeiska industriella AI-modeller och AI-system kan omfatta rymdfart, läkemedelsproduktion, cybersäkerhet, rörlighet, självkörande fordon och drönare, energi och försvar.

7. Stor utmaning 7: Plattform för AI-agenter

Utveckla en europeisk ram för samordning av AI-agenter som tillhandahåller de nödvändiga mellanprogrammen för en motståndskraftig och säker användning av autonoma agenter i stor skala.

Fokus kommer att ligga på att i) utforska innovativa tekniska paradigmer som gör att flera AI-agenter kan samarbeta effektivt och överträffa kapaciteten hos fristående system, samtidigt som strikta säkerhetsstandarder upprätthålls, och ii) skapa motståndskraftiga, molnbaserade öppna plattformar för storskalig hantering av AI-agenter.

De möjliga användningsområdena skulle kunna omfatta hälso- och sjukvård (t.ex. kliniskt beslutsstöd och samordning av forskning), cybersäkerhet (t.ex. upptäckt av hot och insatser) samt grundforskning.

8. Stor utmaning 8: AI inom den offentliga sektorn

Utveckla AI-modeller och AI-system som bygger på högkvalitativa data från den offentliga sektorn och är inriktade på kritiska områden (t.ex. hälso- och sjukvård, offentlig förvaltning, lagstiftning och krishantering samt offentliga tjänster).

Fokus kommer att ligga på lösningar för offentliga tjänster som förväntas ha en stor positiv inverkan på de mest kritiska offentliga tjänsterna och som delas på olika nivåer av den offentliga sektorns organisationer.

Ett mål kommer att vara att möjliggöra datadelning och utveckling av banbrytande modeller i alla nationella offentliga tjänster för att öka effekterna på unionens offentliga sektor överlag, även på områden där känsliga uppgifter hanteras. Ramar för sekretesskydd (däribland federerad träning och generering av syntetiska data med hög tillförlitlighet), som gör det möjligt att träna modeller utan att äventyra konfidentialiteten hos underliggande datauppsättningar, samt åtgärder för att påskynda en bred spridning av sådana modeller, även på regional och lokal nivå, kommer också att bidra till att uppnå detta mål.

BILAGA II

KRITERIER FÖR UNIONENS ASSURANSNIVÅER

I denna bilaga fastställs de kriterier som leverantörer av molntjänster och de molntjänster de erbjuder ska uppfylla för att erkännas som tjänster enligt assurancesnivåerna 1, 2, 3 och 4 i unionen. Vid tillämpning av kriterierna enligt unionens assurancesnivåer 1, 2, 3 och 4 omfattas ”programvara”, i den mening som avses i artikel 3.4 i förordning (EU) 2024/2847, av tillämpningsområdet för denna bilaga och bilaga III till denna förordning. ”Hårdvara” i den mening som avses i artikel 3.5 i förordning (EU) 2024/2847 omfattas inte av tillämpningsområdet.

1. Unionens assurancesnivå 1

1.1. För att uppnå assurancesnivå 1 i unionen ska leverantörer av molntjänster uppfylla följande kumulativa kriterier:

- (a) Leverantören av molntjänster är etablerad i unionen.
 - (b) Den infrastruktur och de tillgångar som tillhör leverantören av molntjänster, inbegripet de som tillhör underleverantörer som är delaktiga i tillhandahållandet av tjänsten, finns i unionen, såvida inte den offentliga myndigheten uttryckligen kräver något annat.
 - (c) Kunduppgifter, inklusive metadata och telemetridata, som behandlas, lagras och överförs av leverantören av molntjänster och av de underleverantörer som är delaktiga i tillhandahållandet av tjänsten, finns kvar inom unionen, såvida inte den offentliga myndigheten vid något tillfälle uttryckligen kräver något annat, inbegripet före, under eller efter konfigurationen eller användningen av tjänsten.
 - (d) Om leverantören av molntjänster lägger ut tekniskt och operativt stöd eller bistånd, inbegripet eventuella efterföljande arrangemang för underentreprenad, till tredjepartsleverantörer utanför unionen, ska de nödvändiga rättsliga, tekniska och organisatoriska åtgärderna genomföras för att säkerställa spårbarhet, säkerhet och styrning av dessa verksamheter, så att verksamheterna inte på något sätt äventyrar molntjänstleverantörens operativa oberoende.
 - (e) Leverantören av molntjänster visar att tjänsten uppfyller de senaste standarderna för cybersäkerhet.
 - (f) Leverantören av molntjänster garanterar fullständig insyn i användningen av underleverantörer. Leverantören av molntjänster ålägger sina underleverantörer att visa tillbörlig aktsamhet, fullgöra avtalsförpliktelser och utöva löpande tillsyn för att fullgöra unionens rättsliga skyldigheter.
 - (g) Om leverantören av molntjänster kontrolleras av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland garanterar leverantören av molntjänster att det inte finns några befintliga lagar och förfaranden i det tredjelandet som kräver att leverantören av molntjänster rapporterar information om sårbarheter i programvaran till myndigheterna i det tredjelandet innan det har blivit känt att sårbarheterna har utnyttjats, vilket styrks av oberoende källor.
- 1.2. För att uppnå assurancesnivå 1 i unionen ska de underleverantörer som avses i första stycket vara underleverantörer som är tredje parter med ett direkt avtalsförhållande med leverantören av molntjänster och som bidrar till tillhandahållandet av molntjänsten.

2. Unionens assurancesnivå 2

- 2.1. För att uppnå assurancesnivå 2 i unionen ska leverantörer av molntjänster uppfylla följande kumulativa kriterier:
- (a) Den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten är etablerade i unionen.
 - (b) Infrastruktur, tillgångar och personal som tillhör den leverantör som revisionen avser eller dennes underleverantörer som deltar i tillhandahållandet av tjänsten finns i unionen.
 - (c) Kunduppgifter, inklusive metadata och telemetridata, som behandlas, lagras och överförs av den leverantör som revisionen avser och av de underleverantörer som är delaktiga i tillhandahållandet av tjänsten, finns kvar inom unionen, såvida inte den offentliga myndigheten vid något tillfälle uttryckligen kräver något annat, inbegripet före, under eller efter konfigurationen eller användningen av tjänsten.
 - (d) Om den offentliga myndigheten fastställer att det är nödvändigt att införa ytterligare krav på personalkontroll och unionsmedborgarskap bör den leverantör som revisionen avser se till att personal som uppfyller dessa krav finns tillgänglig.
 - (e) Den granskade tjänsten erhåller ett europeiskt cybersäkerhetscertifikat som åtminstone motsvarar assurancesnivån ”betydande” enligt en europeisk ordning för cybersäkerhetscertifiering som omfattar molntjänster, vilken ska inrättas i enlighet med förordning (EU) 2019/881, förutsatt att en sådan ordning har inrättats enligt den förordningen och är tillgänglig för leverantörer av molntjänster. Innan dess att en sådan ordning har inrättats ska nationella ordningar för cybersäkerhetscertifiering tillämpas i förekommande fall. Om det inte finns några ordningar för cybersäkerhetscertifiering på unionsnivå eller nationell nivå ska den leverantör som revisionen avser visa att tjänsten uppfyller de högsta cybersäkerhetsstandarderna enligt tillämplig unionslagstiftning.
 - (f) De uppgifter som genereras genom användning av den tjänst som revisionen avser används inte för att träna eller finjustera något AI-system som drivs av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland, och de överförs under alla omständigheter inte utanför unionen.
 - (g) Om den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten kontrolleras av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland ska de visa att nödvändiga rättsliga, tekniska och organisatoriska åtgärder har vidtagits för att säkerställa att
 - i. den kontroll som tredjelandet eller den rättsliga enhet som är etablerad i ett tredjeland utövar över den leverantör som revisionen avser inte utövas på ett sätt som hindrar eller begränsar leverantörens förmåga att utföra och tillhandahålla tjänsten, begränsar den infrastruktur, de tillgångar och den personal som krävs för tillhandahållandet av tjänsten eller undergräver den kapacitet och de standarder som krävs för att utföra den granskade tjänsten,
 - ii. ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte har tillgång till kunduppgifter,
 - iii. ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte kan avbryta kontinuiteten i tjänsten och/eller försämra tjänstens kvalitet,
 - iv. den kontroll som tredjelandet eller den rättsliga enhet som är etablerad i ett tredjeland utövar över den leverantör som revisionen avser inte utövas på ett sätt som ålägger leverantören att genomföra, verkställa, ge verkan åt eller vidta

restriktiva åtgärder såsom sanktionssystem, embargon eller motsvarande rättsliga eller administrativa åtgärder som antagits av ett tredjeland, såvida inte sådana åtgärder är legitima enligt medlemsstaternas nationella lagstiftning eller unionslagstiftningen.

- (h) Det tekniska och operativa stödet eller biståndet i samband med den tjänst som revisionen avser, inbegripet efterföljande arrangemang för underentreprenad, inleds och genomförs uteslutande inom unionen.
 - (i) Den leverantör som revisionen avser visar att följande åtgärder i försörjningskedjan för programvara har vidtagits:
 - i. En fullständig och uppdaterad programvaruförteckning, enligt definitionen i artikel 3.39 i förordning (EU) 2024/2847, och en förteckning över identifierade beroenden som är relevanta för tillhandahållandet av tjänsten dokumenteras och görs tillgängliga för revisionsföretaget.
 - ii. Om programvarukomponenter enligt definitionen i artikel 3.6 i förordning (EU) 2024/2847 eller produkter tillhandahålls, ägs och licensieras av en rättslig enhet som är etablerad i ett tredjeland, genomförs och dokumenteras kontroller för att blockera eventuella fjärrfunktioner som i väsentlig grad kan manipulera eller störa en produkt, ett system eller en programvara (även under uppdateringar) och för att säkerställa att säkerhetsrelevanta komponenter från programvarutillverkare i tredjeländer, enligt definitionen i artikel 3.13 i förordning (EU) 2024/2847, omfattas av källkodsrevisioner och har en dokumenterad migreringsplan om leverantören underkänns eller ett tredjeland inför restriktioner.
 - iii. Om leverantören av molntjänster kontrolleras av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland garanterar leverantören av molntjänster att det inte finns några befintliga lagar och förfaranden i det tredjelandet som kräver att leverantören av molntjänster rapporterar information om sårbarheter i programvaran till myndigheterna i det tredjelandet innan det har blivit känt att sårbarheterna har utnyttjats, vilket styrks av oberoende källor.
 - (j) Om programvara som släppts ut enligt en licens med öppen källkod används för att tillhandahålla tjänsten visar den leverantör som revisionen avser att den har genomfört och dokumenterat lämpliga kontroller för att förhindra användningen av fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara.
 - (k) I den mån den leverantör som revisionen avser tillhandahåller sina tjänster globalt och har ett dotterbolag i ett tredjeland har leverantören vidtagit nödvändiga åtgärder för att säkerställa och verkställa en effektiv rättslig, teknisk och organisatorisk åtskillnad mellan moderbolaget i unionen och dotterbolaget i tredjeland.
- 2.2. För att uppnå assurancesnivå 2 i unionen ska de underleverantörer som avses i första stycket vara underleverantörer som är tredje parter med ett direkt avtalsförhållande med leverantören av molntjänster och som bidrar till tillhandahållandet av molntjänsten.
- 3. Unionens assurancesnivå 3**
- 3.1. För att uppnå assurancesnivå 3 i unionen ska leverantörer av molntjänster uppfylla följande kumulativa kriterier:

- (a) Den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten är etablerade i unionen.
- (b) Infrastruktur, tillgångar och personal som tillhör den leverantör som revisionen avser eller dennes underleverantörer som deltar i tillhandahållandet av tjänsten finns i unionen.
- (c) Kunduppgifter, inklusive metadata och telemetridata, som behandlas, lagras och överförs av den leverantör som revisionen avser och av de underleverantörer som är delaktiga i tillhandahållandet av tjänsten, finns kvar inom unionen, såvida inte den offentliga myndigheten vid något tillfälle uttryckligen kräver något annat, inbegripet före, under eller efter konfigurationen eller användningen av tjänsten.
- (d) Personal, inbegripet personal hos de underleverantörer som deltar i tillhandahållandet av den tjänst som revisionen avser, är unionsmedborgare och har i förekommande fall det nödvändiga nationella säkerhetsgodkännande som utfärdats av en medlemsstat för hantering av säkerhetsskyddsklassificerade uppgifter enligt definitionen i artikel 2.21 i förordning (EU) 2021/697.
- (e) Den granskade tjänsten erhåller ett europeiskt cybersäkerhetscertifikat som åtminstone motsvarar assurancesnivån ”betydande” enligt en europeisk ordning för cybersäkerhetscertifiering som omfattar molntjänster, vilken ska inrättas i enlighet med förordning (EU) 2019/881, förutsatt att en sådan ordning har inrättats enligt den förordningen och är tillgänglig för leverantörer av molntjänster. Innan dess att en sådan ordning har inrättats ska nationella ordningar för cybersäkerhetscertifiering tillämpas i förekommande fall. Om det inte finns några ordningar för cybersäkerhetscertifiering på unionsnivå eller nationell nivå ska den leverantör som revisionen avser visa att tjänsten uppfyller de högsta cybersäkerhetsstandarderna enligt tillämplig unionslagstiftning.
- (f) De uppgifter som genereras genom användning av den tjänst som revisionen avser används inte för att träna eller finjustera något AI-system som drivs av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland, och de överförs under alla omständigheter inte utanför unionen.
- (g) Den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten kontrolleras inte av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland. Genom undantag från detta kriterium får en leverantör av molntjänster och dennes underleverantörer som är delaktiga i tillhandahållandet av den tjänst som revisionen avser och som står under kontroll av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland granskas för unionens assurancesnivå 3 om kommissionen har antagit en genomförandeakt enligt artikel 19. Om kommissionen har antagit en genomförandeakt enligt artikel 19 ska den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten även visa att nödvändiga rättsliga, tekniska och organisatoriska åtgärder har vidtagits för att säkerställa att
 - i. den kontroll som tredjelandet eller den rättsliga enhet som är etablerad i ett tredjeland utövar över den leverantör som revisionen avser inte utövas på ett sätt som hindrar eller begränsar leverantörens förmåga att utföra och tillhandahålla tjänsten, begränsar den infrastruktur, de tillgångar och den personal som krävs för tillhandahållandet av tjänsten eller undergräver den

- kapacitet och de standarder som krävs för att utföra den granskade tjänsten, varvid den leverantör som revisionen avser bör ge rimlig åtkomst till koden,
- ii. ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte har tillgång till kunduppgifter,
 - iii. ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte kan avbryta kontinuiteten i tjänsten och/eller försämra tjänstens kvalitet,
 - iv. den kontroll som tredjelandet eller den rättsliga enhet som är etablerad i ett tredjeland utövar över den leverantör som revisionen avser inte utövas på ett sätt som ålägger leverantören att genomföra, verkställa, ge verkan åt eller vidta restriktiva åtgärder såsom sanktionssystem, embargo eller motsvarande rättsliga eller administrativa åtgärder som antagits av ett tredjeland, såvida inte sådana åtgärder är legitima enligt medlemsstaternas nationella lagstiftning eller unionslagstiftningen.
- (h) Det tekniska och operativa stödet eller biståndet i samband med den tjänst som revisionen avser, inbegripet efterföljande arrangemang för underentreprenad, inleds och genomförs uteslutande inom unionen, av personal som är bosatt i unionen och av tredje parter som inte står under kontroll av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland.
- (i) Den leverantör som revisionen avser visar att följande åtgärder i försörjningskedjan för programvara har vidtagits:
- i. En fullständig och uppdaterad programvaruförteckning och en förteckning över identifierade beroenden som är relevanta för tillhandahållandet av tjänsten dokumenteras och görs tillgängliga för revisionsföretaget.
 - ii. Om programvarukomponenter eller produkter tillhandahålls, ägs och licensieras av en rättslig enhet som är etablerad i ett tredjeland, genomförs och dokumenteras kontroller för att blockera eventuella fjärrfunktioner som i väsentlig grad kan manipulera eller störa en produkt, ett system eller en programvara (även under uppdateringar) och för att säkerställa att säkerhetsrelevanta komponenter från tillverkare i tredjeländer omfattas av källkodsrevisioner och har en dokumenterad migreringsplan om leverantören underkänns eller ett tredjeland inför restriktioner.
 - iii. Om leverantören av molntjänster kontrolleras av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland garanterar leverantören av molntjänster att det inte finns några befintliga lagar och förfaranden i det tredjelandet som kräver att leverantören av molntjänster rapporterar information om sårbarheter i programvaran till myndigheterna i det tredjelandet innan det har blivit känt att sårbarheterna har utnyttjats, vilket styrks av oberoende källor.
- (j) Om programvara som släppts ut enligt en licens med öppen källkod används för att tillhandahålla tjänsten visar den leverantör som revisionen avser att den har genomfört och dokumenterat lämpliga kontroller för att förhindra användningen av fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara.
- (k) I den mån den leverantör som revisionen avser tillhandahåller sina tjänster utanför unionen och har ett dotterbolag i ett tredjeland har leverantören visat att nödvändiga åtgärder har vidtagits för att säkerställa och verkställa en effektiv rättslig, teknisk och

organisatorisk åtskillnad mellan moderbolaget i unionen och dotterbolaget i tredjeland.

- 3.2. För att uppnå assurancesnivå 3 i unionen ska de underleverantörer som avses i första stycket vara underleverantörer som är tredje parter med ett direkt avtalsförhållande med leverantören av molntjänster, som bidrar till tillhandahållandet av molntjänsten och som får begära tillgång till säkerhetsskyddsklassificerade eller känsliga uppgifter enligt definitionen i artikel 2.22 i förordning (EU) 2021/697.

4. Unionens assurancesnivå 4

- 4.1. För att uppnå assurancesnivå 4 i unionen ska leverantörer av molntjänster uppfylla följande kumulativa kriterier:

- (a) Den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten är etablerade i unionen.
- (b) Infrastruktur, tillgångar och personal som tillhör den leverantör som revisionen avser, inbegripet de underleverantörer som deltar i tillhandahållandet av tjänsten, finns i unionen.
- (c) Kunduppgifter, inklusive metadata och telemetridata, som efter en riskbedömning identifieras som känsliga och som behandlas, lagras och överförs av den leverantör som revisionen avser och av de underleverantörer som är delaktiga i tillhandahållandet av tjänsten, finns kvar inom unionen, inbegripet före, under eller efter konfigurationen eller användningen av tjänsten.
- (d) Personal, inbegripet personal hos de underleverantörer som deltar i tillhandahållandet av den tjänst som revisionen avser, är unionsmedborgare och har i förekommande fall det nödvändiga nationella säkerhetsgodkännande som utfärdats av en medlemsstat för hantering av säkerhetsskyddsklassificerade uppgifter.
- (e) Den granskade tjänsten erhåller ett europeiskt cybersäkerhetscertifikat som åtminstone motsvarar assurancesnivån "hög" enligt en europeisk ordning för cybersäkerhetscertifiering som omfattar molntjänster, vilken ska inrättas i enlighet med förordning (EU) 2019/881, förutsatt att en sådan ordning har inrättats enligt den förordningen och är tillgängligt för leverantörer av molntjänster. Innan dess att en sådan ordning har inrättats ska nationella ordningar för cybersäkerhetscertifiering tillämpas i förekommande fall. Om det inte finns några ordningar för cybersäkerhetscertifiering på unionsnivå eller nationell nivå ska den leverantör som revisionen avser visa att tjänsten uppfyller de högsta cybersäkerhetsstandarderna enligt tillämplig unionslagstiftning.
- (f) De uppgifter som genereras genom användning av den tjänst som revisionen avser används inte för att träna eller finjustera något AI-system som drivs av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland, och de överförs under alla omständigheter inte utanför unionen.
- (g) Den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten kontrolleras inte av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland.
- (h) Det tekniska och operativa stödet eller biståndet i samband med den tjänst som revisionen avser, inbegripet efterföljande arrangemang för underentreprenad, inleds och genomförs uteslutande inom unionen, av personal som är bosatt i unionen och av tredje parter som inte står under kontroll av ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland.

- (i) Den leverantör som revisionen avser visar att följande åtgärder i försörjningskedjan för programvara har vidtagits:
 - i. En fullständig och uppdaterad programvaruförteckning och en förteckning över identifierade beroenden som är relevanta för tillhandahållandet av tjänsten dokumenteras och görs tillgängliga för revisionsföretaget.
 - ii. Åtgärder vidtas för att bibehålla effektiv kontroll över programvarukomponenter eller produkter genom att visa att ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte har eller utövar faktisk kontroll över utformningen, framtagningen, underhållet och utvecklingen av dessa komponenter eller produkter. Med faktisk kontroll avses bland annat förmågan att i väsentlig grad påverka komponentens tekniska utveckling, underhållsprioriteringar, säkerhetsåtgärder och långsiktiga kontinuitet.
 - (j) Om programvara som släppts ut enligt en licens med öppen källkod används visar den leverantör som revisionen avser att den har genomfört och dokumenterat lämpliga kontroller för att förhindra användningen av fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara.
 - (k) I den mån den leverantör som revisionen avser tillhandahåller sina tjänster utanför unionen och har ett dotterbolag i ett tredjeland har leverantören visat att nödvändiga åtgärder har vidtagits för att säkerställa och verkställa en effektiv rättslig, teknisk och organisatorisk åtskillnad mellan moderbolaget i unionen och dotterbolaget i tredjeland.
- 4.2. För att uppnå assurancesnivå 4 i unionen ska de underleverantörer som avses i första stycket vara underleverantörer som är tredje parter med ett direkt avtalsförhållande med leverantören av molntjänster, som bidrar till tillhandahållandet av molntjänsten och som får begära tillgång till säkerhetsskyddsklassificerade eller känsliga uppgifter för att tillhandahålla tjänsten.

BILAGA III

REVISIONSBEVIS FÖR REVISIONSFÖRFARANDET

Revisionsföretag bör begära de revisionsbevis som förtecknas i denna bilaga från den leverantör som revisionen avser när de bedömer den granskade tjänstens överensstämmelse med tillämpliga revisionskriterier enligt bilaga II.

Denna bilaga är vägledande och begränsar inte de bevis som revisionsföretagen får begära eller beakta. Revisorer får inhämta all ytterligare information som behövs för att säkerställa en heltäckande och korrekt bedömning av efterlevnaden av de revisioner som utförts. Även om de bevis som begärs kan vara desamma kommer de aspekter som behöver analyseras att variera beroende på assurancesnivåns kriterier och deras stränghet.

1. Revisionskriterium A – Etablering i unionen

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 a i bilaga II på grundval av följande:

- (1) Bevis som visar att den leverantör som revisionen avser är registrerad enligt en medlemsstats lagstiftning i unionen eller på annat sätt har bildats i enlighet med en medlemsstats bolagsrätt i unionen.
- (2) Bevis för att den granskade leverantörens säte, centrala administration och huvudsakliga verksamhetsställe finns i unionen.
- (3) Revisionsföretaget bör kontrollera den tillämpliga unionsrättsliga ramen för den leverantör som revisionen avser och kontrollera om leverantörens etablering är verklig och stabil eller om leverantören i stället endast uppfyller kraven för en leverantör utanför EU som erbjuder tjänster i unionen.
- (4) Revisionsföretaget bör kontrollera om leverantören har bildats på ett lagligt sätt i en av unionens medlemsstater. Bevis på detta kan omfatta, men är inte begränsat till, utdrag ur det nationella bolagsregistret, dokumentation om skatterättsligt hemvist, verksamhetstillstånd, momsregistrering samt kontroll av huruvida leverantören är registrerad i företagsregistrens sammankopplingssystem (Bris) och systemet för utbyte av information om mervärdesskatt (VIES).
- (5) Revisionsföretaget bör kontrollera att den leverantör som revisionen avser har en stabil och verklig närvaro i unionen. Revisionsföretaget bör därför kontrollera att
 - (a) leverantören har fysiska kontor eller verksamhetslokaler i EU (t.ex. genom leasingavtal, tjänstefakturer eller fastighetshandlingar),
 - (b) fast anställd personal är hemmahörande i unionen och att verksamhet för kundstöd bedrivs i unionen (t.ex. genom anställningsavtal, löneregister, personalens tidrapporter),
 - (c) avtalsenlig verksamhet hanteras i unionen (t.ex. genom dokumentation av verksamhetshantering, incidentrapportering),
 - (d) bank- och redovisningsfunktioner uteslutande finns i unionen (t.ex. genom årsbokslut och lagstadgade revisionsberättelser).
- (6) Revisionsföretaget bör kontrollera närvaron av etableringsenheter eller filialer i EU-medlemsstaterna (t.ex. genom hyresavtal, tjänstefakturer, fastighetsdokument, anställningsavtal, tidrapporter, löneregister eller inköpsorder).

2. Revisionskriterium B – Lokalisering av infrastruktur, tillgångar och personal

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assuransnivåerna 2, 3 och 4 b i bilaga II på grundval av följande bevis:

(1) Lokalisering av infrastruktur

- (a) En förteckning med relevanta uppgifter om var den infrastruktur och de datalagringsplatser som används vid tillhandahållandet av den granskade tjänsten är belägna. Denna förteckning bör omfatta infrastrukturens exakta plats (nummer, gata, stad, postnummer och land) och visa att alla delar finns kvar i unionen för tillhandahållandet av den tjänst som revisionen avser. Detta innebär platsen för primär lagring, säkerhetskopiering, katastrofhantering och lagring av loggar.
- (b) Andra bevis på att it-infrastrukturen finns i unionen, t.ex. hyresavtal, fastighetshandlingar, underhållsavtal, tjänstekontrakt och loggar över tillträde till anläggningarna.
- (c) Nätverksdiagram och strukturdokument som styrker den exklusiva användningen av unionsbaserad infrastruktur för datalagring och databehandling, inklusive säkerhetskopierade och replikerade data.

(2) Lokalisering av tillgångar

- (a) En förteckning över och relevanta uppgifter om de tillgångar som används vid tillhandahållandet av den tjänst som revisionen avser, t.ex. ett tillgångsregister.
- (b) Bevis för att servrar, utrustning och driftsinventarier finns i unionen, t.ex. register som visar servern och dess placering, inköpsfakturer, följesedlar, licensavtal, prenumerationsavtal eller fakturer för inköp av eller prenumerationer på programvara, fakturer med leveransbevis för maskinvara.
- (c) Bevis för att kapaciteten för tillhandahållande av tjänster är baserad i unionen, t.ex. utstationeringsregister, installationsregister, rapporter om tjänstestatus, konfigurationsrapporter, övervakningsuppgifter, administratörsloggar som visar att tjänsten används.

(3) Lokalisering av personal

- (a) En förteckning över och relevanta uppgifter om den personal som deltar i tillhandahållandet av den tjänst som revisionen avser.
- (b) Bevis för att den personal som deltar i tillhandahållandet av den tjänst som revisionen avser är hemmahörande i unionen, inbegripet anställningsavtal, löneregister, tidrapporter, verksamhetsregister och organisationsscheman som visar att personalen är baserad i unionen och har ett operativt ansvar.

(4) Överväganden kring infrastruktur, tillgångar och personal

- (a) Revisionsföretaget bör även bedöma om infrastrukturen, tillgångarna eller personalen
 - i. lagrar, överför, kommer åt, bearbetar eller på annat sätt hanterar kunduppgifter,
 - ii. tillhandahåller, möjliggör eller skulle kunna möjliggöra administrativ åtkomst till, kontroll över, konfiguration av eller visning av kunduppgifter,

- iii. om de äventyras, felkonfigureras, görs otillgängliga eller avbryts, rimligen kan leda till att den tjänst som revisionen avser avbryts eller görs otillgänglig.

Anm.: Med "infrastruktur" avses fysisk infrastruktur, inbegripet men inte begränsat till infrastruktur för datorcentraler eller samlokalisering, nät, kylsystem och it-system som möjliggör drift av datorcentralen.

Med "tillgångar" avses maskinvara och programvara, inklusive, men inte begränsat till, bibliotek, det interna nätverk som krävs för att programvarukomponenterna ska kunna kommunicera och kryptografiskt material som gör det möjligt att tillhandahålla molntjänsten.

Med "personal", inklusive personal som anlitas av underleverantörer, avses personer som stöder leverans, administration, säkerhet, tillgänglighet eller drift av den tjänst som revisionen avser.

3. Revisionskriterium C – Datalokalisering i unionen

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 c i bilaga II på grundval av följande bevis:

- (1) Bevis som visar att kunduppgifter uteslutande lagras och behandlas i unionen och att tredje parter eller underleverantörer som inte uppfyller villkoren i denna bilaga inte under några omständigheter, varken tekniskt eller operativt, kan få tillgång till, inhämta, otillgängliggöra, förstöra eller mer allmänt behandla kunduppgifter utan förhandstillstånd. Exempel på detta är åtkomstloggar, regler för tillgång till support, register över privilegierad åtkomst, principer för säkerhetskopiering och dataflödesdiagram som visar var kunduppgifterna lagras, behandlas, replikeras och säkerhetskopieras. Vid behandling av personuppgifter, avtal med underleverantörer som visar överensstämmelse med förordning (EU) 2016/679.
- (2) Bevis på loggar och övervakningsregister som visar att alla uppgifter uteslutande lagras och behandlas inom unionen. Exempel på detta är ramavtal om tjänster, avtal om databehandling, avtal om datalokalisering eller datagränser inom EU.
- (3) Bevis (t.ex. avtal, loggar och förfaranden som erbjuds offentliga myndigheter) som visar att den leverantör som revisionen avser och de underleverantörer som deltar i tillhandahållandet av den granskade tjänsten har vidtagit nödvändiga åtgärder för att säkerställa att
 - (a) inga kunduppgifter, inbegripet krypterade uppgifter, överförs utanför unionen utan godkännande från den offentliga myndigheten,
 - (b) inga uppgifter överförs till någon annan tredje part än de underleverantörer som deltar i tillhandahållandet av tjänsten eller mottagare som uttryckligen godkänts av den offentliga myndigheten.
- (4) Ett flödesdiagram som visar dataflödena mellan leverantören av molntjänster och kunduppgifterna, samt med tredjepartstjänster och underleverantörer. Diagrammet ska tydligt ange källan till och målet för uppgifterna och visa att uppgifterna inte lämnar unionen.

Anm.: Vid tillämpning av denna bilaga avses med "kund" en offentlig myndighet som har ingått ett kontrakt eller ett annat rättsligt bindande avtal med leverantören av molntjänster i syfte att få åtkomst till eller använda molntjänsten.

Med "kunduppgifter" avses alla uppgifter som kontrolleras av molntjänstens kunder, oavsett om det sker på laglig, avtalsmässig eller annan väg, och som

- (a) matas in till molntjänsten av kunden eller för kundens räkning, inbegripet autentiseringsuppgifter,*
- (b) framställs genom kundens användning av molntjänsten.*

Kunduppgifter kan även omfatta uppgifter som kontrolleras av den leverantör som revisionen avser och som härrör från molntjänstkundernas samverkan med den granskade tjänsten. Detta omfattar kunduppgifter och alla uppgifter som genereras vid användningen av molntjänster (dvs. telemetridata, metadata).

"Uppgifter som härrör från en molntjänst" omfattar den del av logguppgifterna som innehåller poster om vem som använde tjänsten, vid vilka tidpunkter, vilka funktioner, vilka typer av uppgifter som ingår osv. De kan även innehålla information om antalet auktoriserade användare och deras identiteter. De kan även omfatta alla konfigurations- eller anpassningsuppgifter, om molntjänsten har sådana konfigurations- och anpassningsfunktioner.

4. Revisionskriterium D – Medborgarskap i unionen

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 d i bilaga II på grundval av följande bevis:

- (1) Den leverantör som revisionen avser bör förse revisionsföretaget med bevis på att åtgärder har vidtagits för att säkerställa att den personal som deltar i tillhandahållandet av den granskade tjänsten är unionsmedborgare, om ett offentligt organ begär unionsmedborgarskap. Detta kan visas genom giltiga officiella statliga handlingar (t.ex. giltigt pass eller nationellt identitetskort).
- (2) Den leverantör som revisionen avser bör tillhandahålla organisationsscheman och arbetsbeskrivningar som bekräftar att leverantören, på begäran, kan säkerställa att endast personal med unionsmedborgarskap kan delta i den granskade tjänstens drift, förvaltning, underhåll och stöd.
- (3) Den leverantör som revisionen avser bör tillhandahålla handlingar som visar principer för åtkomstkontroll och verifieringskedjor som visar att endast auktoriserad personal som är unionsmedborgare har tillgång till tjänstens system och uppgifter.
- (4) Den leverantör som revisionen avser bör visa att förfaranden har införts för att beskriva hur medborgarskapet kontrolleras före uppdraget och hur efterlevnaden av detta revisionskriterium upprätthålls under hela anställningsperioden.

Anm.: *Personal som deltar i tillhandahållandet av den tjänst som revisionen avser kan omfatta personal som har logisk eller fysisk tillgång till infrastruktur och tillgångar som används för att driva molntjänsten, personer som ansvarar för kundsupport och all personal som har ledningskontroll över leverantören av molntjänster.*

5. Revisionskriterium E – Den europeiska ordning för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 e i bilaga II på grundval av följande bevis:

- (1) Ett giltigt europeiskt cybersäkerhetscertifikat utfärdat av ett behörigt organ för bedömning av överensstämmelse som visar att den tjänst som revisionen avser har bedömts och befunnits uppfylla de krav som motsvarar de "grundläggande",

”betydande” eller ”höga” assurancesnivåerna inom ramen för en europeisk ordning för cybersäkerhetscertifiering som antagits enligt förordning (EU) 2019/881, förutsatt att sådana krav har fastställts.

- (2) En certifieringsrapport med en beskrivning av de huvudkomponenter som används för utveckling och drift av den molntjänst som omfattas av revisionsintyget.
- (3) Fram till dess att den europeiska ordning för cybersäkerhetscertifiering som omfattar molntjänster har inrättats kan den leverantör som revisionen avser påvisa efterlevnad genom giltiga cybersäkerhetsintyg. Detta kan omfatta, men är inte begränsat till
 - (a) ett giltigt intyg utfärdat av ett behörigt organ för bedömning av överensstämmelse (i enlighet med CEN/CLC/TS 18072:2025) som visar att molntjänsten har bedömts och befunnits uppfylla de krav som motsvarar de ”grundläggande” eller ”betydande” eller ”höga” assurancesnivåer som definieras i CEN/TS 18026:2024,
 - (b) ett giltigt intyg utfärdat av den relevanta nationella behöriga myndigheten som visar att molntjänsten har bedömts och befunnits uppfylla kraven i den nationella ordning för cybersäkerhet som för närvarande har inrättats i medlemsstaten,
 - (c) i avsaknad av en nationell ordning, bevis för efterlevnad av de högsta cybersäkerhetsstandarder som finns tillgängliga på marknaden.

6. Revisionskriterium F – AI-system som drivs av ett tredjeland eller ett tredjelands rättsliga enhet

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 f i bilaga II på grundval av följande bevis:

- (1) Avtalsklausuler som fastställer att uppgifter som behandlas eller genereras med hjälp av den tjänst som revisionen avser, inklusive kundhärledda uppgifter, loggar och telemetridata, inte kommer att användas för att träna eller finjustera någon AI-modell eller något AI-system som drivs av ett tredjeland eller en rättslig enhet i ett tredjeland och inte kommer att överföras utanför unionen under några omständigheter.
- (2) Avtalsklausuler som fastställer att uppgifter endast behandlas för tillhandahållande av den tjänst som revisionen avser och inte för förbättringar av tjänster, modeller eller system eller något annat sekundärt ändamål.
- (3) Flödesdiagram som dokumenterar dataflödet från ändpunkt till ändpunkt och som omfattar insamling, lagring, bearbetning och radering av data. Diagrammen bör även visa AI-flödenas eller maskininlärningsoperationernas kopplingar till kunduppgifterna.
- (4) Register över maskininlärningsoperationer eller installationer som visar att platserna för utbyggnad, provning och utgivning finns i EU.
- (5) Modell- eller systemkort som omfattar modellens eller systemets namn, version och tränings- och valideringskällor, inbegripet bevis för att de uppgifter som genereras genom användning av den tjänst som revisionen avser inte lämnar unionen.
- (6) Regler för datahistorik och tillhörande dokumentation av genomförandet som visar att leverantören använder verktyg för datahistorik och härkomst och som kan visa (per post) vad uppgifterna har använts till.

- (7) En förteckning över de underleverantörer (med uppgift om etableringsland) som får tillgång till de uppgifter som genereras vid användning av den tjänst som revisionen avser.

7. Revisionskriterium G – Avsaknad av kontroll av ett tredjeland eller ett tredjelands rättsliga enhet

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 g i bilaga II på grundval av följande bevis:

- (1) Revisionsföretaget bör identifiera och analysera
- (a) alla direkta och indirekta aktieägare, upp till de verkliga huvudmännen,
 - (b) den tabell som innehåller en dokumentation av företagets ägarstruktur,
 - (c) det eller de organ som har befogenhet att fatta strategiska beslut (bolagsstämma, tillsynsråd, styrelse osv.),
 - (d) reglerna för utnämning, val eller avsättning av styrelser och styrelsernas faktiska sammansättning (t.ex. för att fastställa om en aktieägare har rätt att utse en styrelserepresentant eller har majoritetsplats i styrelsen),
 - (e) den beslutsförhet och den majoritet som krävs för att fatta strategiska beslut, i syfte att avgöra om någon aktieägare kan fatta ett strategiskt beslut (antingen på grund av att aktieägaren har den majoritet som krävs för att godkänna ett sådant beslut eller kan blockera ett sådant beslut genom veto eller andra särskilda rättigheter, även om aktieägaren inte kan tvinga igenom ett sådant beslut på egen hand osv.),
 - (f) eventuell påverkan på strategiska beslut genom handelsförbindelser, finansiella förbindelser eller andra medel osv.
- (2) Den leverantör som revisionen avser bör begära all ovanstående information från sina underleverantörer och göra den tillgänglig för revisionsföretaget.

7.1. Bedömning av ägande och kontroll:

- (1) Den leverantör som revisionen avser bör förse revisionsföretaget med följande uppgifter om huvudkontoret:
- (a) Plats och fullständig adress för det globala huvudkontoret och/eller huvudkontoret.
 - (b) Platsen för den verkställande ledningen.
- (2) Den leverantör som revisionen avser bör förse revisionsföretaget med följande bevis avseende ägarstrukturen och de särskilda rättigheterna:
- (a) En detaljerad förteckning över alla ägare som
 - i. direkt eller indirekt innehar minst 5 % av kapitalet eller minst 5 % av rösträtterna, inbegripet genom innehåll, överenskommelse, anknytning eller förmedlare, vilket inbegriper röstningsavtal mellan aktieägare som tillsammans skulle ha mer än 5 % av rösterna eller 5 % av kapitalet,
 - ii. har en eller flera av följande särskilda rättigheter i förhållande till sitt ägande: a) rätt att lägga in veto mot en överföring av aktier, b) teckningsrätt, c) rätt att köpa ytterligare aktier eller investeringar på vissa villkor.

- (b) Revisionsföretaget bör begära följande styrkande handlingar för att bedöma de delar som anges i punkt 2 a:
- i. Utdrag ur handelsregistret, aktieägarnas bokföring inom organisationen och andra relevanta handlingar som tydligt anger aktieägarna och deras rösträtter eller procentandelar.
 - ii. Överenskommelser och samförståndsavtal mellan aktieägarna, stadgar, bolagsordning eller andra relevanta handlingar om beslutsförfarandena inom den rättsliga enheten, investeringsavtal mellan aktieägarna osv.
 - iii. För varje aktieägare som är en juridisk person som innehar minst 5 % av kapitalet eller minst 5 % av rösträtterna
 - (1) ett diagram som beskriver de olika nivåerna av ägande eller kontrollkedjan fram till de verkliga huvudmännen,
 - (2) organisationens bolagsordning, stadgar eller motsvarande handlingar,
 - (3) ett register över styrelseledamöter, tjänstemän och undertecknare.
- (3) Den leverantör som revisionen avser bör förse revisionsföretaget med följande uppgifter om företagsstyrningen:
- (a) Den leverantör som revisionen avser bör ge revisionsföretaget en beskrivning av
- i. de beslutande organen, deras sammansättning och ledamöternas nationalitet eller etableringsort (i förekommande fall),
 - ii. reglerna för val, utnämning eller tjänstgöring av de beslutande organens ledamöter eller andra ledande befattningar,
 - iii. beslutsförfaranden, inbegripet information om den majoritet och/eller beslutsförhet som krävs för beslut,
 - iv. interna styrstrategier som beskriver hur ägar- och kontrollbeslut registreras och godkänns,
- styrelse- och ledningsbeslut som återspeglar den angivna kontrollstrukturen, styrelseprotokoll och resolutioner för kontrolländringar.
- (b) Den leverantör som revisionen avser bör förse revisionsföretaget med styrkande handlingar som fastställer eller beskriver de beslutande organen och reglerna för deras val, utnämning eller tjänstgöring, beslutsförfaranden, rösträtt, vetorätt, utnämningsrätt, godkännanderätt inom den rättsliga enheten (t.ex. stadgar, rapporter om företagsstyrning osv.). Styrkande handlingar och uppgifter ska lämnas för var och en de mellanliggande rättsliga enheter som direkt eller indirekt innehar 5 % eller mer av kapitalet eller rösträtterna, ända upp till de verkliga huvudmännen på samtliga nivåer.
- (4) Den leverantör som revisionen avser bör lämna följande bevis med anknytning till kontroll till revisionsföretaget:
- (a) Den leverantör som revisionen avser bör förse revisionsföretaget med bevis avseende de handelsförbindelser som ligger till grund för kontrollen. Detta inbegriper, men är inte begränsat till, en förteckning över personer eller rättsliga enheter med vilka de leverantörer som revisionen avser (eller ägarna

till den leverantör som revisionen avser, inklusive mellanliggande nivåer upp till de verkliga huvudmännen) har en affärsförbindelse som a) leder till en liknande nivå av kontroll över styrning och resurser som ägandet av aktier eller tillgångar, och b) har mycket lång varaktighet (t.ex. mycket viktiga långsiktiga leveransavtal eller krediter som tillhandahålls av programvarutillverkare/kunder, i kombination med strukturella kopplingar).

- (b) De styrkande handlingarna bör omfatta samarbetsavtal med den offentliga sektorns organ, programvarutillverkare osv.
- (5) Den leverantör som revisionen avser bör förse revisionsföretaget med följande bevis avseende de finansiella förbindelser som ligger till grund för kontrollen:
 - (a) Den leverantör som revisionen avser bör tillhandahålla en förteckning över de personer eller rättsliga enheter (inklusive kontrollerande aktieägare eller ägare) som den leverantör som revisionen avser (eller ägarna) är ekonomiskt beroende av på ett sätt som skulle kunna göra det möjligt för dem att erhålla koncessioner inom strategiska affärsområden.
 - (b) De styrkande handlingarna bör omfatta lånehandlingar, stadgar och handlingar som visar den finansiella förbindelsen osv.
- (6) Den leverantör som revisionen avser bör förse revisionsföretaget med följande bevis avseende andra källor till kontroll:
 - (a) De leverantörer som revisionen avser bör uppge för revisionsföretaget om det finns andra medel, processer eller förbindelser som i slutänden ger kontroll till ett annat tredjeland eller en rättslig enhet som är etablerad i ett tredjeland (liknande kontrollnivå för styrning och resurser som ägande av aktier eller tillgångar och förbindelser med lång varaktighet).
 - (b) Styrkande handlingar bör tillhandahållas för att styrka all sådan kontroll eller en försäkran lämnas om att det inte finns någon sådan kontroll (denna försäkran kan komma från tjänsteleverantörens styrelse).

Anm.: De faktorer som bör beaktas vid bedömningen av kontrollen är ägarstrukturerna och de särskilda rättigheterna, företagsstyrningen, affärsförbindelser som ger kontroll, finansiella förbindelser som ger kontroll och andra källor till kontroll.

7.2. Ytterligare åtgärder baserade på slutsatserna av undersökningen av ägande och kontroll

Om revisionsföretaget fastställer att den leverantör som revisionen avser kontrolleras av ett tredjeland eller en rättslig enhet i ett tredjeland bör företaget begära följande ytterligare bevis:

- (c) Bevis för att kommissionen har antagit ett beslut i enlighet med artikel 19 avseende det tredjeland som kontrollerar leverantören av molntjänster.
- (d) Alla bevis som visar att den leverantör som revisionen avser och eventuella underleverantörer som deltar i tillhandahållandet av den granskade tjänsten har genomfört de åtgärder som krävs för att genomdriva en effektiv rättslig, teknisk och organisatorisk åtskillnad mellan leverantören av molntjänster och eventuella tredjeländer eller rättsliga enheter som är etablerade i ett tredjeland, för att säkerställa att leverantören av molntjänster inte på ett lagligt, tekniskt eller operativt sätt kan tillgodose en begäran om tillgång till kunduppgifter,

inbegripet krypterade uppgifter, och inte kan avbryta tjänstens kontinuitet eller försämra dess kvalitet.

- (e) Alla bevis som visar att den offentliga myndigheten kommer att informeras om varje sådan begäran och en bekräftelse på att begäran har avslagits.
- (f) Alla bevis som visar att det finns ett uppdaterat register över varje begäran om åtkomst till kunduppgifter, om att avbryta kontinuiteten i tjänsten eller om att försämra kvaliteten på tjänsterna från ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland, vilka åtminstone ska omfatta begäran och svaret på begäran.

8. Revisionskriterium H – Inget tekniskt och operativt stöd utanför unionen

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 h i bilaga II på grundval av följande bevis:

- (1) Bevis för att den leverantör som revisionen avser har genomfört bindande avtalsklausuler om att all verksamhet i samband med stöd, administration, underhåll, övervakning, incidenthantering och daglig drift ska inledas och utföras uteslutande i unionen. Detta skulle kunna inbegripa avtalsklausuler med krav på förhandsinformation om alla underleverantörer och stödfunktioner, skriftligt förhandsgodkännande innan nya underleverantörer anlitas och en rättighet att avvisa underleverantörer utanför unionen.
- (2) Bevis för att den leverantör som revisionen avser upprätthåller ett uppdaterat register över underleverantörer.
- (3) Bevis för att den leverantör som revisionen avser inte lägger ut verksamheten på entreprenad eller överför den utanför unionen.
- (4) Bevis för att den leverantör som revisionen avser har genomfört de rättsliga, tekniska och organisatoriska åtgärder som krävs för att säkerställa att tekniskt och operativt stöd inte finns tillgängligt på distans från länder utanför unionen för den granskade tjänsten.
- (5) Bevis för att den leverantör som revisionen avser endast använder hjälp-/stödtjänster, infrastrukturadministration, säkerhetscentrum (SOC) eller nätverksdriftscenter (NOC) samt rutiner för privilegierad åtkomst, säkerhetskopiering och katastrofhantering av den granskade tjänsten som tillhandahålls från unionen, inbegripet åtkomstvägen för att driva tjänsten.
- (6) Bevis för att den leverantör som revisionen avser säkerställer att personal som lämnar företaget inte har tillgång till den granskade tjänsten och återkallar alla åtkomsträttigheter.
- (7) Bevis för att den leverantör som revisionen avser har genomfört de tekniska och organisatoriska åtgärder som krävs för att säkerställa att administrativt tillträde till de system som används för att driva den granskade tjänsten tillhandahålls via åtkomstvägar inom unionen. Detta kan visas genom tillämpning av geografiskt begränsade nätverkskontroller, unionsbaserad administrativ infrastruktur, kontroller av privilegierad åtkomst och övervakningsmekanismer.
- (8) Bevis för att den leverantör som revisionen avser har rutiner som säkerställer att ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland inte har någon faktisk kontroll, inbegripet för efterföljande underentreprenad.

9. Revisionskriterium I – Säkerställande av insyn i leveranskedjan för programvara

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 i) i bilaga II på grundval av följande bevis:

- (1) Den leverantör som revisionen avser bör ge revisionsföretaget tillgång till en fullständig och uppdaterad programvaruförteckning för alla programvarukomponenter, inbegripet programvara med öppen källkod.
- (2) Den leverantör som revisionen avser bör se till att en förteckning över beroenden finns tillgänglig för revisionsföretaget. Förteckningen bör omfatta
 - (a) alla programvarumoduler, bibliotek eller gränssnitt för tillämpningsprogram som används, samt alla utvecklingsverktyg,
 - (b) programvarans ursprung: var programvaran kommer ifrån (ursprungslandet), vem som utformar, utvecklar och underhåller den, vilken plats och jurisdiktion som styr distributionen och uppdateringarna av programvaran,
 - (c) graden av beroende av leverantörer, anläggningar eller patentskyddad teknik utanför EU, för nivå 3, bevis för att det inte finns några otillbörliga och omotiverade licensbegränsningar om programvarustacken tillhandahålls av en enhet i tredjeland,
 - (d) graden av beroende av programvara med öppen källkod,
 - (e) öppenheten i hela programvarutillverkarens och undertillverkarens kedja, inklusive granskningsrättigheter.

Anm.: Ovanstående krav innebär att samriskföretag, t.ex. som har bildats av en unionsenhet med en rättslig enhet som är etablerad i ett tredjeland, kan uppfylla kraven för denna nivå.

- (3) Den leverantör som revisionen avser bör tillhandahålla följande:
 - (a) Bevis för en riskbaserad process för att identifiera och minska beroendet av externa programvarutillverkare som är relevant för driften av molntjänsten.
 - (b) Bevis för att leverantören har identifierat en eller flera alternativa programvarulösningar, däribland med öppen programvara. Om motsvarande programvara inte kan identifieras ska en lösning som säkerställer minimal genomförbar funktionalitet identifieras. Tester ska genomföras i kombination med en plan för en övergång till sådana alternativa lösningar.
 - (c) Bevis för att leverantören kan gå över till en alternativ lösning i händelse av defekter, brister från leverantörens sida eller begränsningar från ett tredjeland eller en rättslig enhet som är etablerad i ett tredjeland.
 - (d) En förteckning över öppna standarder som följs som en del av de granskade leverantörernas riktlinjer för den tjänst som revisionen avser.
- (4) Den leverantör som revisionen avser bör säkerställa öppenhet genom att möjliggöra en revision av fjärråtkomsten och källkoden på följande sätt:
 - (a) Ge revisionsföretaget en förteckning över bevis för att det inte finns några fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara. Förteckningen bör omfatta

- i. bevis för att programvarukomponenten har provats för att förhindra användningen av fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara (provningsförfarande, provningsrapporter, provningsplan osv.),
 - ii. bevis för att organisationens förändringshantering omfattar varje förändring av fast programvara, uppdateringar av bios-program och programvara samt integrering av nya komponenter för att förhindra användningen av fjärrstyrda funktioner eller mekanismer,
 - iii. bevis för att underhållsrutinen uppdateras så att den förhindrar alla fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara.
- (b) Den leverantör som revisionen avser ska se till att den oberoende tredjepartsrevisorn får tillgång till och kan granska programvarans källkod. Den leverantör som revisionen avser ska även se till att all dokumentation, allt tekniskt material och all information som krävs för att utvärdera och granska källkoden görs tillgänglig för revisionsföretaget i ett fullständigt, korrekt och tillgängligt format.

10. Revisionskriterium J – Programvara med öppen källkod

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 j i bilaga II på grundval av följande bevis:

- (1) Den leverantör som revisionen avser bör säkerställa öppenhet genom att möjliggöra en revision av fjärråtkomsten och källkoden på följande sätt:
- (a) Ge revisionsföretaget en förteckning över bevis för att det inte finns några fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara. Förteckningen bör omfatta
 - i. bevis för att programvarukomponenten har provats för att förhindra användningen av fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara (provningsförfarande, provningsrapporter, provningsplan osv.),
 - ii. bevis för att organisationens förändringshantering omfattar varje förändring av fast programvara, uppdateringar av bios-program och programvara samt integrering av nya komponenter för att förhindra användningen av fjärrstyrda funktioner eller mekanismer,
 - iii. bevis för att underhållsrutinen uppdateras så att den förhindrar alla fjärrstyrda funktioner eller mekanismer som kan användas för att i väsentlig grad manipulera eller störa en produkt, ett system eller programvara.
- (2) Den leverantör som revisionen avser bör tillhandahålla följande:
- (a) Bevis för en riskbaserad process för att identifiera och begränsa i) ett svagt ekosystem och svagt stöd för programvaran med öppen källkod, ii)

underlåtenhet att kontinuerligt övervaka uppdateringarna, iii) fall där programvaran med öppen källkod är föråldrad eller inte längre underhålls.

- (b) Bevis för att den leverantör som revisionen avser har tillämpat den uppdaterade programvaran med öppen källkod utan onödigt dröjsmål.
 - (c) Bevis för att den leverantör som revisionen avser har identifierat en eller flera alternativa lösningar med öppen källkod. Om den leverantör som revisionen avser inte kan identifiera en likvärdig programvara ska leverantören identifiera en lösning som säkerställer minsta möjliga genomförbara funktionalitet. Den leverantör som revisionen avser ska genomföra provningar och utarbeta en plan som möjliggör en övergång till alternativa lösningar.
- (3) Om den leverantör som revisionen avser använder programvara som släppts ut enligt en licens med öppen källkod bör leverantören införa mekanismer för att upptäcka och i god tid underrätta den offentliga myndigheten om programvaran förvärvas av eller kommer att kontrolleras av ett tredjeland eller en rättslig enhet eller stiftelse som är etablerad i ett tredjeland.

11. Revisionskriterium K – Globala tjänster och dotterbolag i tredjeländer

Revisionsföretaget bör bedöma det revisionskriterium som förtecknas under assurancesnivåerna 2, 3 och 4 k i bilaga II på grundval av följande bevis:

- (1) Revisionsföretaget bör kontrollera att dotterbolaget är rättsligt och operativt oberoende av den leverantör som revisionen avser.
- (2) Den leverantör som revisionen avser ska visa att dotterbolaget inte har tillgång till system som behandlar eller lagrar kunduppgifterna.
- (3) Den leverantör som revisionen avser ska visa att dotterbolaget inte har några privilegierade konton inom unionens produktionsmiljöer, däribland inom molnadministration, identitets- och åtkomsthantering (IAM), hantering av privilegierad åtkomst (PAM) och privilegier för övervakning eller databasadministration.
- (4) Revisionsföretaget bör kontrollera att dotterbolagets personal inte kan få tillgång till uppgifter om kunder i unionen.
- (5) Revisionsföretaget bör kontrollera att dotterbolaget inte har befogenhet att instruera den operativa personalen i unionen att lämna ut kunduppgifter eller kringgå säkerhetsförfarandena.
- (6) Revisionsföretaget bör kontrollera att alla framställningar från utländska myndigheter som tas emot av dotterbolaget formellt omdirigeras till den behöriga unionsenheten för rättslig bedömning enligt unionens och medlemsstaternas lagstiftning.