COMISIA
EUROPEANĂ

Bruxelles, 3.6.2026
COM(2026) 502 final

ANNEXES 1 to 3

ANEXE

la

REGULAMENTUL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

de stabilire a unui cadru de măsuri pentru consolidarea ecosistemului european al tehnologiei de tip cloud și al IA (Regulamentul privind dezvoltarea tehnologiei de tip cloud și a IA)

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

ANEXA I

MARI PROVOCĂRI

1. Marea provocare 1: durabilitatea din punctul de vedere al mediului, performanța și securitatea centrelor de date ale Uniunii

Testarea și implementarea de tehnologii pentru centrele de date din întreaga Uniune pentru a depăși stadiul actual în materie de eficiență energetică și utilizare eficientă a resurselor.

Aceasta include obținerea unui indice mai scăzut al eficacității utilizării energiei electrice (PUE) și asigurarea unor rate semnificativ mai mari de utilizare a serverelor. Printre exemple se numără:

(1) ***Scăderea indicelui mediu al eficacității utilizării energiei electrice***: îmbunătățirea durabilității din punctul de vedere al mediului și a performanței centrelor de date de cloud și edge computing ale Uniunii la o eficacitate medie a utilizării energiei electrice (PUE) de 1,15 în întreaga Uniune. Printre principalele domenii prioritare se numără facilitarea dezvoltării:

(a) unor tehnologii avansate de eficiență energetică a centrelor de date, cum ar fi răcirea, recuperarea căldurii reziduale;

(b) unor tehnologii de calcul cuantic pentru operațiunile infrastructurii aferente tehnologiei de tip cloud și de calcul;

(c) integrării în rețea și a sistemelor avansate de gestionare a energiei;

(d) unor linii-pilot pentru validarea la scară operațională a tehnologiilor eficiente din punct de vedere energetic de generație următoare.

(2) ***Creșterea ratelor medii de utilizare a serverelor în centrele de date:*** creșterea ratelor medii de utilizare a serverelor în centrele de date ale Uniunii către un nivel de 50 %, prin integrarea, de exemplu, a tehnologiilor bazate pe IA pentru gestionarea dinamică a utilizării serverelor, gestionarea și planificarea sarcinilor în timp real sau pentru echilibrarea nivelului de utilizare, a costurilor cu energia, a constrângerilor termice și a cerințelor privind latența.

(3) ***Consolidarea securității și a rezilienței centrelor de date:*** consolidarea securității și a rezilienței lanțului valoric și a aprovizionării centrelor de date prin integrarea tehnologiilor semiconductorilor și a tehnologiilor cuantice proiectate și fabricate în Uniune și prin îmbunătățirea rezistenței acestora la amenințările fizice și cibernetice, inclusiv la atacurile specifice.

2. Marea provocare 2: pachete tehnologice de cloud

Dezvoltarea unor pachete tehnologice de cloud complete, atât la nivel de hardware, cât și de software, care să includă instrumente de IA, infrastructură, servicii și straturi de gestionare pentru a elimina lacunele critice în materie de capacitate ale Uniunii.

Aceasta include dezvoltarea de servere de IA bazate pe semiconductori și tehnologii cuantice proiectate și fabricate în Uniune pentru cloud computing și edge computing distribuite și descentralizate pentru IA.

Programele-pilot ar putea contribui la demonstrarea capabilităților pachetelor tehnologice europene deschise de cloud în sectoare importante din punct de vedere strategic.

3. Marea provocare 3: IA de avangardă

Dezvoltarea următoarei generații de modele și sisteme multimodale de IA de avangardă și crearea de noi capabilități inovatoare

Accentul se va pune pe proiectarea arhitecturală și dezvoltarea modelelor și sistemelor multimodale de generație următoare care împing limitele capacităților algoritmice actuale pentru obținerea unei performanțe superioare în ceea ce privește raționamentul avansat, înțelegerea transmodală și capacitățile agentice, investigarea noilor abordări privind eficiența modelelor, modelarea cognitivă și structurile computaționale alternative etc.

Printre aplicațiile potențiale s-ar putea număra știința fundamentală, cum ar fi descoperirile științifice și interpretarea complexă a datelor, precum și dezvoltarea unor modele ale lumii pentru îmbunătățirea raționamentului și pentru simularea și planificarea gestionării automatizate.

4. Marea provocare 4: IA fizică

Dezvoltarea unor modele și sisteme fizice avansate de IA, care să funcționeze autonom și în condiții de siguranță pentru a oferi servicii solide de manipulare și de navigare în medii nestructurate.

Accentul se va pune pe proiectarea în comun a software-ului și a arhitecturilor de hardware subiacente și pe combinarea tehnicilor de IA de avangardă cu modele ale lumii care sprijină raționamentul fizic pentru furnizarea unor capacități solide de manipulare, navigare și interacțiune, cu o supraveghere umană minimă.

Printre aplicațiile potențiale s-ar putea număra roboții autonomi, sistemele industriale și dronele care operează în medii reale dinamice.

5. Marea provocare 5: IA industrială

Accelerarea dezvoltării și a implementării IA industriale europene în toate sectoarele strategice ale Uniunii.

Accentul se va pune pe dezvoltarea unor modele și sisteme europene de IA industrială capabile să deservească aplicații industriale cu valoare ridicată. Astfel de modele și sisteme ar trebui să fie adaptabile la cazurile de utilizare specifice sectorului și să permită implementarea în condiții de siguranță.

Inițiativele lansate în cadrul acestei mari provocări ar trebui să se bazeze pe resurse de calcul specializate și pe instalații de testare necesare pentru validarea sistemelor de IA în medii reale înainte de a sprijini implementarea și adoptarea lor la scară largă, inclusiv la nivel regional și local.

În sectorul autovehiculelor, aceste inițiative pot facilita dezvoltarea și implementarea unor platforme software inovatoare și a unor modele de IA pentru conducerea automată, în timp ce, în industria producătoare, ele pot permite crearea unor modele specializate care să optimizeze procesele de producție. Alte sectoare strategice care ar putea beneficia de IA industrială pot include sectorul asistenței medicale, sectorul energiei, sectorul agroalimentar și industria apărării.

6. Marea provocare 6: modele industriale europene bazate pe cooperare

Dezvoltarea unor modele și sisteme de IA industriale europene bazate pe cooperare pentru sectoarele strategice, care să faciliteze colaborarea la scară europeană în sectorul industrial, fără a expune între participanți date sensibile din punct de vedere comercial.

Accentul se va pune pe tehnologiile avansate de păstrare a confidențialității. Aceste mecanisme includ abordări federate și distribuite în ceea ce privește antrenarea, în care algoritmii sunt aduși la date, în loc ca datele să fie transferate la nivel central; medii de execuție securizate, prelucrarea bazată pe criptare, tehnici de anonimizare și pseudonimizare, compartimentarea accesului și măsuri de protecție împotriva extragerii de informații sensibile din punct de vedere comercial din modele antrenate.

Sectoarele strategice care ar putea beneficia de modele și sisteme de IA industriale europene bazate pe cooperare pot include industria aerospațială, industria farmaceutică, securitatea cibernetică, mobilitatea, vehiculele autonome și dronele, sectorul energiei și industria apărării.

7. Marea provocare 7: platforma agenților IA

Dezvoltarea unui cadru european de orchestrare a agenților IA, care să ofere un program middleware esențial pentru implementarea rezilientă și sigură a agenților autonomi la scară largă.

Accentul se va pune (i) pe explorarea paradigmelor tehnologice inovatoare care le permit mai multor agenți IA să colaboreze în mod eficace, depășind capacitățile sistemelor autonome și menținând în același timp standarde de securitate riguroase și (ii) pe crearea unor platforme deschise reziliente, bazate pe cloud, destinate gestionării la scară largă a agenților IA.

Printre aplicațiile potențiale s-ar putea număra asistența medicală (cum ar fi sprijinul pentru luarea deciziilor clinice și coordonarea cercetării), securitatea cibernetică (cum ar fi detectarea amenințărilor și răspunsul la acestea), precum și știința fundamentală.

8. Marea provocare 8: IA din sectorul public

Dezvoltarea de modele și sisteme de IA bazate pe date de înaltă calitate din sectorul public, care vizează domenii critice (cum ar fi asistența medicală, administrația publică, justiția și gestionarea crizelor, precum și serviciile publice)

Accentul se va pune pe soluțiile pentru servicii publice care se preconizează că vor avea un impact pozitiv ridicat asupra celor mai critice servicii publice și care sunt partajate la diferite niveluri ale organizațiilor din sectorul public.

Unul dintre obiective va fi să se permită schimbul de date și dezvoltarea de modele de avangardă în cadrul serviciilor publice naționale pentru a spori impactul asupra sectorului public general al Uniunii, inclusiv în domeniile care gestionează date sensibile. Cadrele de protecție a vieții private (cum ar fi învățarea federată și generarea de date sintetice de înaltă fidelitate), care permit antrenarea modelelor fără a compromite confidențialitatea seturilor de date subiacente, precum și măsurile de accelerare a adoptării la scară largă a acestor modemuri, inclusiv la nivel regional și local, vor contribui, de asemenea, la atingerea acestui obiectiv.

ANEXA II

CRITERII PENTRU NIVELURILE DE ASIGURARE ALE UNIUNII

Prezenta anexă stabilește criteriile care trebuie îndeplinite de furnizorii de servicii de cloud computing și de serviciile lor de cloud computing pentru a fi recunoscuți ca furnizori de servicii la nivelurile de asigurare 1, 2, 3 și 4 ale Uniunii. În sensul criteriilor aferente nivelurilor de asigurare 1, 2, 3 și 4 ale Uniunii, „software-ul” în sensul articolului 3 punctul 4 din Regulamentul (UE) 2024/2847 intră în domeniul de aplicare al prezentei anexe și al anexei III la prezentul regulament. „Hardware-ul” în sensul articolului 3 punctul 5 din Regulamentul (UE) 2024/2847 nu intră în domeniul de aplicare.

1. Nivelul de asigurare 1 al Uniunii

1.1. Pentru nivelul de asigurare 1 al Uniunii, furnizorii de servicii de cloud computing trebuie să îndeplinească următoarele criterii cumulative:

(a) furnizorul de servicii de cloud computing trebuie să fie stabilit în Uniune;

(b) infrastructura și activele furnizorului de servicii de cloud computing, inclusiv cele ale subcontractanților săi, care sunt implicate în furnizarea serviciului trebuie să fie situate în Uniune, cu excepția cazului în care organismul din sectorul public solicită în mod explicit contrariul;

(c) datele clienților, inclusiv metadatele și datele de telemetrie, care sunt prelucrate, stocate și transferate de furnizorul de servicii de cloud computing și de subcontractanții care sunt implicați în furnizarea serviciului trebuie să rămână exclusiv pe teritoriul Uniunii, cu excepția cazului în care organismul din sectorul public solicită în mod explicit contrariul și în orice moment, inclusiv înainte, în timpul sau după configurarea sau utilizarea serviciului;

(d) în cazul în care furnizorul de servicii de cloud computing externalizează sprijinul sau asistența tehnică și operațională, inclusiv eventualele acorduri ulterioare de subcontractare către furnizori terți de servicii din afara Uniunii, trebuie puse în aplicare măsurile juridice, tehnice și organizatorice necesare pentru a asigura trasabilitatea, securitatea și guvernanța operațiunilor respective, iar operațiunile respective nu trebuie să compromită în niciun fel autonomia operațională a furnizorului de servicii de cloud computing;

(e) furnizorul de servicii de cloud computing trebuie să demonstreze că serviciul respectă standardele actuale de securitate cibernetică;

(f) furnizorul de servicii de cloud computing trebuie să asigure o transparență deplină în ceea ce privește utilizarea subcontractanților. Furnizorul de servicii de cloud computing trebuie să supună subcontractanții unei verificări de diligență necesară, unor obligații contractuale și supravegherii continue pentru a îndeplini obligațiile legale ale Uniunii;

(g) în cazul în care furnizorul de servicii de cloud computing face obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță, furnizorul de servicii de cloud computing trebuie să garanteze că nu există legi și practici în vigoare în țara terță respectivă, demonstrate de surse independente, care să îi impună furnizorului de servicii de cloud computing în cauză să raporteze informații privind vulnerabilitățile software-ului autorităților din țara terță respectivă înainte de a se cunoaște faptul că vulnerabilitățile respective au fost exploatate.

1.2. Pentru nivelul de asigurare 1 al Uniunii, subcontractanții menționați la primul paragraf trebuie să fie subcontractanți părți terțe care au o relație contractuală directă cu furnizorul de servicii de cloud computing și care contribuie la furnizarea serviciului de cloud computing.

2. Nivelul de asigurare 2 al Uniunii

2.1. Pentru nivelul de asigurare 2 al Uniunii, furnizorii de servicii de cloud computing trebuie să îndeplinească următoarele criterii cumulative:

(a) furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat trebuie să fie stabiliți în Uniune;

(b) infrastructura, activele și personalul furnizorului auditat, inclusiv cele ale subcontractanților săi, care sunt implicate în furnizarea serviciului trebuie să fie situate în Uniune;

(c) datele clienților, inclusiv metadatele și datele de telemetrie, care sunt prelucrate, stocate și transferate de furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului trebuie să rămână exclusiv pe teritoriul Uniunii, cu excepția cazului în care organismul din sectorul public solicită în mod explicit contrariul și în orice moment, inclusiv înainte, în timpul sau după configurarea sau utilizarea serviciului;

(d) în cazul în care organismul din sectorul public stabilește că este necesară impunerea unor cerințe suplimentare privind verificarea personalului și cetățenia Uniunii, furnizorul auditat ar trebui să se asigure că dispune de personal care îndeplinește aceste cerințe;

(e) serviciul auditat trebuie să obțină un certificat european de securitate cibernetică ce prevede un nivel de asigurare cel puțin „substanțial” în cadrul unui sistem european de certificare a securității cibernetice care acoperă serviciile de cloud computing și care urmează să fie instituit în temeiul Regulamentului (UE) 2019/881, cu condiția ca un astfel de sistem să fi fost instituit în temeiul regulamentului respectiv și să fie disponibil pentru furnizorii de servicii de cloud computing. Până la instituirea unui astfel de sistem, se aplică sistemele naționale de certificare a securității cibernetice, în cazul în care acestea există. În cazul în care nu există sisteme de certificare a securității cibernetice la nivelul Uniunii sau la nivel național, furnizorul auditat trebuie să demonstreze că serviciul respectă cele mai înalte standarde de securitate cibernetică în temeiul dreptului aplicabil al Uniunii;

(f) datele generate prin utilizarea serviciului auditat nu sunt utilizate pentru a antrena sau a perfecționa vreun sistem de IA operat de o țară terță sau de o entitate juridică stabilită într-o țară terță și nu sunt transferate în niciun caz în afara Uniunii;

(g) dacă furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță, aceștia trebuie să demonstreze că au fost puse în aplicare măsurile juridice, tehnice și organizatorice necesare pentru a se asigura că:

(i) controlul țării terțe sau al entității juridice stabilite într-o țară terță asupra furnizorului auditat nu este exercitat într-un mod care limitează sau restricționează capacitatea furnizorului de a presta și de a furniza serviciul, impune limitări privind infrastructura, activele și personalul necesar pentru furnizarea serviciului sau subminează capabilitățile și standardele necesare pentru prestarea serviciului auditat;

(ii) accesul unei țări terțe sau al unei entități juridice stabilite într-o țară terță la datele clienților este împiedicat;

(iii) se previne posibilitatea perturbării continuității serviciului și/sau a degradării calității serviciului de către o țară terță sau de către o entitate juridică stabilită într-o țară terță;

(iv) controlul țării terțe sau al entității juridice stabilite într-o țară terță asupra furnizorului auditat nu este exercitat într-un mod care să oblige furnizorul auditat să pună în aplicare sau să asigure respectarea unor măsuri restrictive sau să aplice sau să respecte măsurile respective, cum ar fi regimuri de sancțiuni, embargouri sau orice măsură juridică sau administrativă echivalentă adoptată de o țară terță, cu excepția cazului în care astfel de măsuri sunt legitime în temeiul legislației naționale a statelor membre sau al dreptului Uniunii;

(h) sprijinul sau asistența tehnică și operațională legată de serviciul auditat, inclusiv acordurile ulterioare de subcontractare a serviciilor externalizate, trebuie să fie inițiate și executate exclusiv în cadrul Uniunii;

(i) furnizorul auditat trebuie să demonstreze că sunt instituite următoarele măsuri privind lanțul de aprovizionare cu software:

(i) o listă completă și actualizată a materialelor software (SBOM), astfel cum sunt definite la articolul 3 punctul 39 din Regulamentul (UE) 2024/2847, și o listă a dependențelor identificate relevante pentru furnizarea serviciului sunt documentate și puse la dispoziția organizației de audit;

(ii) în cazul în care componentele software, astfel cum sunt definite la articolul 3 punctul 6 din Regulamentul (UE) 2024/2847, sau produsele sunt furnizate, deținute și fac obiectul unei licențe deținute de către o entitate juridică stabilită într-o țară terță, sunt puse în aplicare și documentate controale pentru a bloca orice funcționalități de la distanță care ar putea manipula sau perturba în mod semnificativ un dispozitiv, un sistem sau un software (inclusiv în timpul actualizărilor) și pentru a se asigura că respectivele componente relevante pentru securitate ale producătorilor de software din țări terțe, astfel cum sunt definiți la articolul 3 punctul 13 din Regulamentul (UE) 2024/2847, fac obiectul unor audituri ale codurilor sursă și au un plan de migrare documentat în cazul în care vânzătorul intră în dificultate sau o țară terță impune restricții;

(iii) în cazul în care furnizorul de servicii de cloud computing face obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță, furnizorul de servicii de cloud computing garantează că nu există legi și practici în vigoare în țara terță respectivă, demonstrate de surse independente, care să îi impună furnizorului de servicii de cloud computing în cauză să raporteze informații privind vulnerabilitățile software-ului autorităților din țara terță respectivă înainte de a se cunoaște faptul că vulnerabilitățile respective au fost exploatate;

(j) în cazul în care software-ul publicat în temeiul unei licențe cu sursă deschisă este utilizat pentru furnizarea serviciului, furnizorul auditat trebuie să demonstreze că a pus în aplicare și a documentat controalele adecvate pentru a preveni utilizarea oricăror funcționalități sau mecanisme de la distanță care ar putea fi utilizate pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software;

(k) în măsura în care furnizorul auditat își furnizează serviciile la nivel mondial și menține o filială într-o țară terță, furnizorul auditat trebuie să fi pus în aplicare măsurile necesare pentru a prevedea și a asigura separarea juridică, tehnică și organizațională efectivă între societatea-mamă din Uniune și orice astfel de filială dintr-o țară terță.

2.2. Pentru nivelul de asigurare 2 al Uniunii, subcontractanții menționați la primul paragraf trebuie să fie subcontractanți părți terțe care au o relație contractuală directă cu furnizorul de servicii de cloud computing și care contribuie la furnizarea serviciului de cloud computing.

3. Nivelul de asigurare 3 al Uniunii

3.1. Pentru nivelul de asigurare 3 al Uniunii, furnizorii de servicii de cloud computing trebuie să îndeplinească următoarele criterii cumulative:

(a) furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat trebuie să fie stabiliți în Uniune;

(b) infrastructura, activele și personalul furnizorului auditat, inclusiv cele ale subcontractanților, care sunt implicate în furnizarea serviciului trebuie să fie situate în Uniune;

(c) datele clienților, inclusiv metadatele și datele de telemetrie, care sunt prelucrate, stocate și transferate de furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului trebuie să rămână exclusiv pe teritoriul Uniunii, cu excepția cazului în care organismul din sectorul public solicită în mod explicit contrariul și în orice moment, inclusiv înainte, în timpul sau după configurarea sau utilizarea serviciului;

(d) membrii personalului, inclusiv ai personalului subcontractanților, care sunt implicați în furnizarea serviciului auditat, trebuie să fie cetățeni ai Uniunii și, după caz, personalul trebuie să dețină, de asemenea, autorizarea de securitate națională necesară eliberată de un stat membru atunci când gestionează informații clasificate, astfel cum sunt definite la articolul 2 punctul 21 din Regulamentul (UE) 2021/697;

(e) serviciul auditat trebuie să obțină un certificat european de securitate cibernetică ce prevede un nivel de asigurare cel puțin „substanțial” în cadrul unui sistem european de certificare a securității cibernetice care acoperă serviciile de cloud computing și care urmează să fie instituit în temeiul Regulamentului (UE) 2019/881, cu condiția ca un astfel de sistem să fi fost instituit în temeiul regulamentului respectiv și să fie disponibil pentru furnizorii de servicii de cloud computing. Până la instituirea unui astfel de sistem, se aplică sistemele naționale de certificare a securității cibernetice, în cazul în care acestea există. În cazul în care nu există sisteme de certificare a securității cibernetice la nivelul Uniunii sau la nivel național, furnizorul auditat trebuie să demonstreze că serviciul respectă cele mai înalte standarde de securitate cibernetică în temeiul dreptului aplicabil al Uniunii;

(f) datele generate prin utilizarea serviciului auditat nu sunt utilizate pentru a antrena sau a perfecționa vreun sistem de IA operat de o țară terță sau de o entitate juridică stabilită într-o țară terță și nu sunt transferate în niciun caz în afara Uniunii;

(g) furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat nu fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță. Prin derogare de la acest criteriu, un furnizor de servicii de cloud computing și subcontractanții săi care sunt implicați în furnizarea serviciului auditat

care fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță pot fi auditați pentru nivelul de asigurare 3 al Uniunii în cazul în care Comisia a adoptat un act de punere în aplicare în temeiul articolului 19. În cazul în care Comisia a adoptat un act de punere în aplicare în temeiul articolului 19, furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat trebuie, de asemenea, să demonstreze că au fost puse în aplicare măsurile juridice, tehnice și organizatorice necesare pentru a se asigura că:

(i) controlul țării terțe sau al entității juridice stabilite într-o țară terță asupra furnizorului auditat nu este exercitat într-un mod care limitează sau restricționează capacitatea furnizorului de a presta și de a furniza serviciul, impune limitări privind infrastructura, activele și personalul necesar pentru furnizarea serviciului sau subminează capabilitățile și standardele necesare pentru prestarea serviciului auditat. Furnizorul auditat ar trebui să permită un acces rezonabil la cod;

(ii) accesul unei țări terțe sau al unei entități juridice stabilite într-o țară terță la datele clienților este împiedicat;

(iii) se previne posibilitatea perturbării continuității serviciului și/sau a degradării calității serviciului de către o țară terță sau de către o entitate juridică stabilită într-o țară terță;

(iv) controlul țării terțe sau al entității juridice stabilite într-o țară terță asupra furnizorului auditat nu este exercitat într-un mod care să oblige furnizorul auditat să pună în aplicare sau să asigure respectarea unor măsuri restrictive sau să aplice sau să respecte măsurile respective, cum ar fi regimuri de sancțiuni, embargouri sau orice măsură juridică sau administrativă echivalentă adoptată de o țară terță, cu excepția cazului în care astfel de măsuri sunt legitime în temeiul legislației naționale a statelor membre sau al dreptului Uniunii;

(h) sprijinul sau asistența tehnică și operațională legată de serviciul auditat, inclusiv acordurile ulterioare de subcontractare a serviciilor externalizate, trebuie să fie inițiate și efectuate exclusiv în Uniune, de către membri ai personalului care sunt rezidenți în Uniune și de către părți terțe care nu fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță;

(i) furnizorul auditat trebuie să demonstreze că sunt instituite următoarele măsuri privind lanțul de aprovizionare cu software:

(i) o listă completă și actualizată a materialelor software (SBOM) și o listă a dependențelor identificate relevante pentru furnizarea serviciului sunt documentate și puse la dispoziția organizației de audit;

(ii) în cazul în care componentele software sau produsele sunt furnizate, deținute și fac obiectul unei licențe deținute de către o entitate juridică stabilită într-o țară terță, sunt puse în aplicare și documentate controale pentru a bloca orice funcționalități de la distanță care ar putea manipula sau perturba în mod semnificativ un dispozitiv, un sistem sau un software (inclusiv în timpul actualizărilor) și pentru a se asigura că respectivele componente relevante pentru securitate ale producătorilor din țări terțe fac obiectul unor audituri ale codurilor sursă și au un plan de migrare documentat în cazul în care vânzătorul intră în dificultate sau o țară terță impune restricții;

(iii) în cazul în care furnizorul de servicii de cloud computing face obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță,

furnizorul de servicii de cloud computing garantează că nu există legi și practici în vigoare în țara terță respectivă, demonstrate de surse independente, care să îi impună furnizorului de servicii de cloud computing în cauză să raporteze informații privind vulnerabilitățile software-ului autorităților din țara terță respectivă înainte de a se cunoaște faptul că vulnerabilitățile respective au fost exploatate;

(j) în cazul în care software-ul publicat în temeiul unei licențe cu sursă deschisă este utilizat pentru furnizarea serviciului, furnizorul auditat trebuie să demonstreze că a pus în aplicare și a documentat controalele adecvate pentru a preveni utilizarea oricăror funcționalități sau mecanisme de la distanță care ar putea fi utilizate pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software;

(k) în măsura în care furnizorul auditat își furnizează serviciile în afara Uniunii și menține o filială într-o țară terță, furnizorul auditat trebuie să demonstreze că a pus în aplicare măsurile necesare pentru a prevedea și a asigura separarea juridică, tehnică și organizațională efectivă între societatea-mamă din Uniune și orice astfel de filială dintr-o țară terță.

3.2. Pentru nivelul de asigurare 3 al Uniunii, subcontractanții menționați la primul paragraf trebuie să fie subcontractanți părți terțe care au o relație contractuală directă cu furnizorul de servicii de cloud computing, care contribuie la furnizarea serviciului de cloud computing și care pot necesita accesul la informații clasificate sau sensibile, astfel cum sunt definite la articolul 2 punctul 22 din Regulamentul (UE) 2021/697.

4. Nivelul de asigurare 4 al Uniunii

4.1. Pentru nivelul de asigurare 4 al Uniunii, furnizorii de servicii de cloud computing trebuie să îndeplinească următoarele criterii cumulative:

(a) furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat trebuie să fie stabiliți în Uniune;

(b) infrastructura, activele și personalul furnizorului auditat, inclusiv ale subcontractanților, care sunt implicate în furnizarea serviciului trebuie să fie situate în Uniune;

(c) datele clienților, inclusiv metadatele și datele de telemetrie, care, în urma unei evaluări a riscurilor, sunt identificate drept sensibile, care sunt prelucrate, stocate și transferate de furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului trebuie să rămână exclusiv pe teritoriul Uniunii și în orice moment, inclusiv înainte, în timpul sau după configurarea sau utilizarea serviciului;

(d) membrii personalului, inclusiv ai personalului subcontractanților, care sunt implicați în furnizarea serviciului auditat trebuie să fie cetățeni ai Uniunii și, după caz, personalul trebuie să dețină, de asemenea, autorizarea de securitate națională necesară eliberată de un stat membru atunci când gestionează informații clasificate;

(e) serviciul auditat trebuie să obțină un certificat european de securitate cibernetică ce prevede un nivel de asigurare cel puțin „ridicat” în cadrul unui sistem european de certificare a securității cibernetice care acoperă serviciile de cloud computing și care urmează să fie instituit în temeiul Regulamentului (UE) 2019/881, cu condiția ca un astfel de sistem să fi fost instituit în temeiul regulamentului respectiv și să fie disponibil pentru furnizorii de servicii de cloud computing. Până la instituirea unui astfel de sistem, se aplică sistemele naționale de certificare a securității cibernetice,

în cazul în care acestea există. În cazul în care nu există sisteme de certificare a securității cibernetice la nivelul Uniunii sau la nivel național, furnizorul auditat trebuie să demonstreze că serviciul respectă cele mai înalte standarde de securitate cibernetică în temeiul dreptului aplicabil al Uniunii;

(f) datele generate prin utilizarea serviciului auditat nu sunt utilizate pentru a antrena sau a perfecționa vreun sistem de IA operat de o țară terță sau de o entitate juridică stabilită într-o țară terță și nu sunt transferate în niciun caz în afara Uniunii;

(g) furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat nu fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță;

(h) sprijinul sau asistența tehnică și operațională legată de serviciul auditat, inclusiv acordurile ulterioare de subcontractare a serviciilor externalizate, trebuie să fie inițiate și efectuate exclusiv în Uniune, de către membri ai personalului care sunt rezidenți în Uniune și de către părți terțe care nu fac obiectul controlului unei țări terțe sau al unei entități juridice stabilite într-o țară terță;

(i) furnizorul auditat trebuie să demonstreze că sunt instituite următoarele măsuri privind lanțul de aprovizionare cu software:

  (i) o listă completă și actualizată a materialelor software (SBOM) și o listă a dependențelor identificate relevante pentru furnizarea serviciului sunt documentate și puse la dispoziția organizației de audit;

  (ii) măsuri pentru a menține controlul efectiv asupra componentelor software sau a produselor prin demonstrarea faptului că o țară terță sau o entitate juridică stabilită într-o țară terță nu deține sau nu exercită controlul efectiv asupra proiectării, dezvoltării, întreținerii și evoluției componentelor sau produselor respective. Controlul efectiv include capacitatea de a influența în mod semnificativ evoluția tehnică, prioritățile de întreținere, remedierea securității și continuitatea pe termen lung a componentei respective;

(j) în cazul în care este utilizat software publicat în temeiul unei licențe cu sursă deschisă, furnizorul auditat trebuie să demonstreze că a pus în aplicare și a documentat controalele adecvate pentru a preveni utilizarea oricăror funcționalități sau mecanisme de la distanță care ar putea fi utilizate pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software;

(k) în măsura în care furnizorul auditat își furnizează serviciile în afara Uniunii și menține o filială într-o țară terță, furnizorul auditat trebuie să demonstreze că a pus în aplicare măsurile necesare pentru a prevedea și a asigura separarea juridică, tehnică și organizațională efectivă între societatea-mamă din Uniune și orice astfel de filială dintr-o țară terță.

4.2. Pentru nivelul de asigurare 4 al Uniunii, subcontractanții menționați la primul paragraf trebuie să fie subcontractanți părți terțe care au o relație contractuală directă cu furnizorul de servicii de cloud computing, care contribuie la furnizarea serviciului de cloud computing și care pot necesita accesul la informații clasificate sau sensibile pentru a furniza serviciul.

ANEXA III

PROBE DE AUDIT PENTRU PROCEDURA DE AUDIT

Organizațiile de audit ar trebui să solicite probele de audit enumerate în prezenta anexă de la furnizorul auditat atunci când evaluează conformitatea serviciului auditat cu criteriile de audit aplicabile în temeiul anexei II.

Prezenta anexă este orientativă și nu limitează probele care pot fi solicitate sau luate în considerare de organizațiile de audit. Auditorii pot solicita orice informații suplimentare necesare pentru a asigura o evaluare cuprinzătoare și exactă a conformității în vederea desfășurării auditurilor. Deși probele solicitate pot fi aceleași, aspectele care trebuie analizate vor fi diferite în funcție de criteriile aferente nivelului de asigurare și de strictețea acestora.

1. Criteriul de audit A – stabilirea în Uniune

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (a) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor elemente:

(1) Orice dovadă care demonstrează că furnizorul auditat este înregistrat în Uniune în temeiul legislației unui stat membru sau este constituit în alt mod în conformitate cu dreptul societăților comerciale dintr-un stat membru al Uniunii.

(2) Orice dovadă că sediul social, administrația centrală și sediul principal al furnizorului auditat sunt stabilite în Uniune.

(3) Organizația de audit ar trebui să verifice cadrul juridic al Uniunii aplicabil furnizorului auditat, precum și dacă sediul acestuia este autentic și stabil sau dacă furnizorul auditat se califică, în schimb, numai ca furnizor din afara UE care oferă servicii în Uniune.

(4) Organizația de audit ar trebui să verifice dacă furnizorul este înregistrat legal într-un stat membru al Uniunii. Dovezile în acest sens ar putea include, fără a se limita la acestea, extrase din registrul național al societăților, documente privind rezidența fiscală, licențe comerciale, înregistrarea în scopuri de TVA, verificarea înregistrării furnizorului în sistemul de interconectare a registrelor comerțului (BRIS) și în sistemul de schimb de informații privind TVA (VIES).

(5) Organizația de audit ar trebui să verifice prezența stabilă și efectivă în Uniune a furnizorului auditat. Prin urmare, organizația de audit ar trebui să verifice dacă:

   (a) există birouri fizice sau spații operaționale în UE (de exemplu, în baza unor contracte de închiriere, facturi la utilități sau documente de proprietate);

   (b) personalul permanent este situat în Uniune, iar operațiunile de asistență pentru clienți sunt efectuate în Uniune (de exemplu, în baza unor contracte de muncă, evidențe ale statelor de plată, fișe de pontaj ale personalului);

   (c) operațiunile contractuale sunt gestionate în Uniune (de exemplu, în baza unor evidențe de gestionare a activităților, evidențe de raportare a incidentelor);

   (d) funcția bancară și cea contabilă sunt exercitate exclusiv în Uniune (de exemplu, în baza situațiilor financiare și a rapoartelor de audit statutar).

(6) Organizația de audit ar trebui să verifice prezența unităților sau a sucursalelor înființate în statele membre ale UE (de exemplu, în baza unor contracte de închiriere, facturi la utilități, documente de proprietate, contracte de muncă, fișe de pontaj, evidențe ale statelor de plată sau ordine de achiziție).

2. Criteriul de audit B – locația infrastructurii, a activelor și a personalului

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (b) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Locația infrastructurii

(a) O listă cu detaliile relevante ale locației în care este situată infrastructura și ale locației în care sunt stocate datele, utilizate pentru furnizarea serviciului auditat. Această listă ar trebui să includă locația exactă (numărul, strada, orașul, codul poștal și țara) a infrastructurii, demonstrând că toate elementele rămân în Uniune pentru furnizarea serviciului auditat. Aceasta include locația pentru stocarea primară, de rezervă, de recuperare în caz de dezastru și a jurnalelor.

(b) Orice alte dovezi că infrastructura informatică este situată în Uniune, cum ar fi contractele de închiriere, documentele de proprietate, contractele de întreținere, contractele de servicii, jurnalele de acces la infrastructură.

(c) Diagrame de rețea și documente de arhitectură care ilustrează utilizarea exclusivă a infrastructurii situate în Uniune pentru stocarea și prelucrarea datelor, inclusiv a datelor de rezervă și a datelor duplicate.

(2) Locația activelor

(a) O listă și detalii relevante privind activele utilizate pentru furnizarea serviciului auditat, cum ar fi un registru al activelor.

(b) Dovezi că serverele, echipamentele și activele operaționale sunt situate în Uniune, cum ar fi evidențe care identifică serverul și locația acestuia, facturi de achiziție, note de livrare, acorduri de licență, contracte de abonament sau facturi pentru achiziții de software sau abonamente, facturi cu dovezi de livrare pentru hardware.

(c) Dovezi ale faptului că respectivele capacități de furnizare a serviciilor se află în Uniune, cum ar fi evidențe ale implementării, evidențe ale instalării, rapoarte privind starea serviciilor, rapoarte de configurare, rezultate ale monitorizării, jurnale administrative care indică utilizarea serviciului.

(3) Locația personalului

(a) O listă și detalii relevante privind personalul implicat în furnizarea serviciului auditat.

(b) Dovada că personalul implicat în furnizarea serviciului auditat se află în Uniune, inclusiv contractele de muncă, evidențele statelor de plată, fișele de pontaj, fișele de activitate și organigramele care prezintă personalul cu responsabilități operaționale aflat în Uniune.

(4) Considerații privind infrastructura, activele și personalul

(a) Organizația de audit ar trebui, de asemenea, să evalueze dacă infrastructura, activele sau personalul respectiv:

(i) stochează, transmit, accesează, prelucrează sau gestionează în alt mod datele clienților;

(ii) oferă, permit sau ar putea permite accesul administrativ la datele clienților, precum și controlul, configurarea sau vizibilitatea acestora;

(iii) ar putea duce, în mod rezonabil, la perturbarea sau indisponibilitatea serviciului auditat dacă sunt compromise, configurate greșit, puse la dispoziție sau perturbate.

***NB**: „Infrastructură" înseamnă infrastructura fizică, inclusiv, dar fără a se limita la aceasta, infrastructura centrului de date sau infrastructura de colocare, rețeaua, sistemele de răcire și sistemele informatice care permit gestionarea centrului de date.*

„Active" înseamnă hardware și software, inclusiv, dar fără a se limita la biblioteci, rețeaua internă necesară pentru comunicarea între componentele software, materiale criptografice care permit furnizarea serviciului de cloud computing.

„Personal", inclusiv personalul gestionat de subcontractanți, înseamnă persoane care sprijină furnizarea, administrarea, securitatea, disponibilitatea sau exploatarea serviciului auditat.

3. Criteriul de audit C – localizarea datelor în Uniune

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (c) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Dovezi care să demonstreze că datele clienților sunt stocate și prelucrate exclusiv în Uniune și că părțile terțe sau subcontractanții care nu îndeplinesc condițiile prevăzute în prezenta anexă nu sunt în niciun caz în măsură, din punct de vedere tehnic sau operațional, să acceseze, să obțină, să pună la dispoziție, să distrugă sau, cu caracter mai general, să prelucreze datele clienților fără autorizare prealabilă. Printre exemple se numără jurnalele de acces, politicile de acces la serviciile de asistență, evidențele privind accesul privilegiat, politica de păstrare a copiilor de rezervă, diagrama fluxurilor de date care demonstrează unde sunt stocate, prelucrate, reproduse și salvate în copii de rezervă datele clienților. Atunci când prelucrează date cu caracter personal, contractele cu subcontractanții care demonstrează conformitatea cu Regulamentul (UE) 2016/679.

(2) Dovezi ale jurnalelor și ale înregistrărilor de monitorizare care demonstrează că toate datele sunt stocate și prelucrate exclusiv în Uniune. Printre exemple se numără acordurile-cadru de servicii, acordurile de prelucrare a datelor, acordurile contractuale privind rezidența datelor sau orice limită de date în UE.

(3) Dovezi (cum ar fi acorduri contractuale, jurnale și proceduri oferite organismelor din sectorul public) care să demonstreze că furnizorul auditat și subcontractanții care sunt implicați în furnizarea serviciului auditat au instituit măsurile necesare pentru a se asigura că:

   (a) datele clienților, inclusiv datele criptate, nu sunt transferate în afara Uniunii fără aprobarea organismului din sectorul public;

   (b) datele nu sunt transferate niciunei părți terțe, alta decât subcontractanții care sunt implicați în furnizarea serviciului sau destinatarii autorizați în mod expres de organismul din sectorul public.

(4) O diagramă a fluxului de date care prezintă fluxurile de date dintre furnizorul de servicii de cloud computing și datele clienților, precum și cu serviciile furnizate de terți și subcontractanții. Diagrama trebuie să identifice în mod clar sursa și destinația datelor și să demonstreze că datele nu părăsesc Uniunea.

NB: În sensul prezentei anexe, client înseamnă un organism din sectorul public care a încheiat un acord contractual sau un alt acord obligatoriu din punct de vedere juridic cu furnizorul de servicii de cloud computing în scopul accesării sau al utilizării serviciului de cloud computing.

„Date ale clienților" ar putea însemna orice date aflate sub controlul clientului serviciului de cloud computing, prin mijloace juridice, contractuale sau de altă natură, care sunt:

(a) introduse în serviciul de cloud computing de către client sau în numele acestuia, inclusiv datele de autentificare;

(b) produse prin utilizarea de către client a serviciului de cloud computing.

Datele clienților pot include, de asemenea, date aflate sub controlul furnizorilor auditați care sunt derivate ca urmare a interacțiunii clientului serviciului de cloud computing cu serviciul auditat. Acestea includ datele clienților și orice date care rezultă din utilizarea serviciilor de cloud computing (și anume de telemetrie, metadatele).

„Datele derivate din serviciul de cloud computing" includ porțiunea de date din jurnale care conține înregistrări privind persoana care a utilizat serviciul, momentul utilizării, funcțiile aferente, tipurile de date implicate etc. Acestea pot include, de asemenea, informații cu privire la numărul de utilizatori autorizați și la identitățile acestora. Ele pot include, de asemenea, orice date de configurare sau de personalizare, în cazul în care serviciul de cloud computing are astfel de funcționalități de configurare și de personalizare.

4. Criteriul de audit D – cetățenia Uniunii

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (d) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Furnizorul auditat ar trebui să îi furnizeze organizației de audit dovada că a pus în aplicare măsurile pentru a se asigura că, în cazul în care un organism din sectorul public ar solicita cetățenia Uniunii, membrii personalului implicați în furnizarea serviciului auditat sunt cetățeni ai Uniunii. Acest lucru poate fi demonstrat prin documente oficiale valabile emise de administrația publică (de exemplu, un pașaport valabil și o carte de identitate națională valabilă).

(2) Furnizorul auditat ar trebui să furnizeze organigrame și fișe ale posturilor care să confirme că poate garanta, la cerere, că numai membri ai personalului care dețin cetățenia Uniunii au acces la operarea, gestionarea, întreținerea și asistența aferente serviciului auditat.

(3) Furnizorul auditat ar trebui să furnizeze documente care să demonstreze politicile de control al accesului și piste de audit care să arate că numai membrii personalului autorizat care sunt cetățeni ai Uniunii pot accesa sistemele și datele aferente serviciului.

(4) Furnizorul auditat ar trebui să demonstreze că a instituit proceduri care descriu modul în care este verificată cetățenia înainte de atribuirea sarcinilor și modul în care respectarea acestui criteriu de audit este menținută pe tot parcursul angajării.

***NB:** Personalul implicat în furnizarea serviciului auditat ar putea include personalul care are acces logic sau fizic la infrastructura și activele utilizate pentru operarea serviciului de cloud computing, precum și personalul responsabil cu asistența pentru clienți și întregul personal care deține controlul de gestiune asupra furnizorului de servicii de cloud computing.*

5. Criteriul de audit E – sistemul european de certificare a securității cibernetice adoptat în temeiul Regulamentului (UE) 2019/881

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (e) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Un certificat european de securitate cibernetică valabil, eliberat de un organism competent de evaluare a conformității, care să demonstreze că serviciul auditat a fost evaluat și considerat conform cu cerințele corespunzătoare nivelurilor de asigurare „de bază”, „substanțial” sau „ridicat” în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul Regulamentului (UE) 2019/881, cu condiția ca un astfel de sistem să fi fost instituit.

(2) Un raport de certificare care include o descriere a principalelor componente utilizate pentru dezvoltarea și operarea serviciului de cloud computing care face obiectul certificatului de audit.

(3) Până la instituirea sistemului european de certificare a securității cibernetice care acoperă serviciile de cloud computing, furnizorul auditat poate demonstra conformitatea prin certificări de securitate cibernetică valabile. Acestea pot include, dar nu se limitează la următoarele:

   (a) un certificat valabil eliberat de un organism competent de evaluare a conformității (în conformitate cu CEN/CLC/TS 18072:2025) care să demonstreze că serviciul de cloud computing a fost evaluat și considerat conform cu cerințele corespunzătoare nivelurilor de asigurare „de bază”, „substanțial” sau „ridicat” definite în CEN/TS 18026:2024;

   (b) un certificat valabil eliberat de autoritatea națională competentă relevantă care să demonstreze că serviciul de cloud computing a fost evaluat și considerat conform cu cerințele sistemului național de securitate cibernetică în vigoare în prezent în statul membru în cauză;

   (c) în absența unui sistem național, dovezi care să demonstreze respectarea celui mai înalt nivel de standarde de securitate cibernetică disponibile pe piață.

6. Criteriul de audit F – sisteme de IA operate de o țară terță sau de o entitate juridică dintr-o țară terță

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (f) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Clauze contractuale care să prevadă că datele prelucrate sau generate prin utilizarea serviciului auditat, inclusiv datele derivate de la clienți, jurnalele și datele de telemetrie, nu vor fi utilizate pentru a antrena sau a perfecționa vreun model sau sistem de IA operat de o țară terță sau de o entitate juridică dintr-o țară terță și nu sunt transferate în afara Uniunii în niciun caz.

(2) Clauze contractuale care să prevadă că datele sunt prelucrate numai pentru furnizarea serviciului auditat și nu pentru îmbunătățiri ale serviciului sau ale modelului sau îmbunătățiri ale sistemului sau în orice alt scop secundar.

(3) Diagrame privind fluxul de date care să documenteze fluxul de date complet, acoperind introducerea, stocarea, prelucrarea și ștergerea datelor. Diagramele ar trebui să indice, de asemenea, locul în care fluxurile de lucru de IA sau operațiunile de învățare automată se conectează cu datele clienților.

(4) Evidențe ale operațiunilor de învățare automată sau ale implementării care să demonstreze că locațiile de compilare, testare și lansare se află în UE.

(5) Fișe de model sau de sistem care să conțină denumirea modelului sau a sistemului, versiunea, sursele de antrenare și de validare, inclusiv declarații potrivit cărora datele generate prin utilizarea serviciului auditat nu părăsesc Uniunea.

(6) Politici privind trasabilitatea datelor și documentația de punere în aplicare aferentă care arată că furnizorul utilizează instrumente de trasabilitate și de proveniență și care pot demonstra (pentru fiecare înregistrare) în ce scop au fost utilizate datele.

(7) O listă a subcontractanților (indicând țara lor de stabilire) care accesează datele generate prin utilizarea serviciului auditat.

7. Criteriul de audit G – absența controlului exercitat de o țară terță sau de o entitate dintr-o țară terță

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (g) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Organizația de audit ar trebui să identifice și să analizeze:

(a) toți acționarii direcți și indirecți, până la proprietarii finali;

(b) tabelul de capital care documentează structura acționariatului societății;

(c) organismul sau organismele abilitate să ia decizii strategice (adunarea generală a acționarilor, consiliul de supraveghere, consiliul de administrație etc.);

(d) normele privind numirea/alegerea/revocarea organelor de conducere și componența efectivă a organelor de conducere (de exemplu, pentru a identifica dacă un acționar are dreptul de a numi un reprezentant în consiliul de administrație sau deține majoritatea locurilor în consiliul de administrație);

(e) cvorumurile și majoritatea necesare pentru adoptarea deciziilor strategice, pentru a stabili dacă un acționar poate lua o decizie strategică (fie pentru că deține majoritatea necesară pentru a aproba o astfel de decizie, fie pentru că poate bloca o astfel de decizie prin veto sau alte drepturi specifice, chiar dacă nu poate impune o astfel de decizie pe cont propriu etc.);

(f) posibila influență asupra deciziilor strategice prin legături comerciale, financiare sau prin alte mijloace etc.

(2) Furnizorul auditat ar trebui să le solicite subcontractanților săi toate informațiile de mai sus și să le pună la dispoziția organizației de audit.

7.1. Evaluarea proprietății și a controlului:

(1) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi referitoare la sediul central:

(a) localizarea și adresa completă a sediului general și/sau a sediului central;

(b) localizarea structurilor de conducere executivă.

(2) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi referitoare la structura de proprietate și la drepturile specifice:

(a) O listă detaliată care să descrie orice acționari care:

(i) dețin, direct sau indirect, cel puțin 5 % din capital sau cel puțin 5 % din drepturile de vot, inclusiv prin orice conținut, înțelegere, relație sau intermediar. Aceasta include acorduri de vot între acționari care împreună ar deține peste 5 % din drepturile de vot sau 5 % din capital;

(ii) dețin unul sau mai multe dintre următoarele drepturi specifice în raport cu participația deținută: (a) dreptul de veto asupra unui transfer de acțiuni; (b) drepturi de preempțiune; (c) dreptul de a achiziționa acțiuni sau de a face investiții suplimentare, sub rezerva anumitor condiții.

(b) Organizația de audit ar trebui să solicite următoarele documente justificative pentru a evalua elementele de la punctul 2 litera (a):

(i) extrase din registrul comerțului și registrele acționarilor organizației, precum și orice alt document relevant care indică în mod clar acționarii și drepturile lor de vot sau procentul de participare;

(ii) acordul acționarilor, memorandumul de înțelegere între acționari, statutul, actul constitutiv sau alte documente relevante privind procedurile decizionale din cadrul entității juridice, acordurile de investiții dintre acționari etc.;

(iii) pentru acționarii persoane juridice care dețin cel puțin 5 % din capital sau cel puțin 5 % din drepturile de vot:

(1) un grafic care să descrie diferitele niveluri de proprietate/lanțuri de control până la proprietarii finali;

(2) actul constitutiv, statutul sau documente constitutive echivalente;

(3) un registru al directorilor, al responsabililor și al semnatarilor.

(3) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi legate de guvernanța corporativă:

(a) furnizorul auditat ar trebui să îi furnizeze organizației de audit o descriere:

(i) a organelor de decizie, a componenței lor, precum și a cetățeniei sau a locului lor de stabilire (dacă este cazul);

(ii) a normelor privind alegerea, numirea, nominalizarea sau mandatul membrilor organelor de decizie sau în ceea ce privește alte funcții de conducere;

(iii) a procedurilor decizionale, inclusiv a informațiilor privind majoritatea necesară și/sau cvorumul necesar pentru decizii;

(iv) a politicilor de guvernanță internă care descriu modul în care sunt înregistrate și aprobate deciziile privind proprietatea și controlul;

a deciziilor consiliului de administrație și ale conducerii care reflectă structura de control declarată;

a proceselor-verbale și a rezoluțiilor consiliului de administrație pentru modificările legate de control.

(b) furnizorul auditat ar trebui să îi furnizeze organizației de audit documente justificative care să stabilească sau să descrie: organismele decizionale și normele privind alegerea, numirea, nominalizarea sau mandatul acestora, procedurile decizionale, drepturile de vot, drepturile de veto, drepturile de numire, drepturile de aprobare în cadrul entității juridice (de exemplu, statutul, rapoartele privind guvernanța corporativă etc.). Documentele justificative și informațiile ar trebui furnizate pentru fiecare entitate juridică intermediară care deține direct sau indirect 5 % sau mai mult din capital sau din drepturile de vot, până la proprietarii finali ai tuturor nivelurilor implicate.

(4) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi legate de control:

(a) furnizorul auditat ar trebui să îi furnizeze organizației de audit dovezi ale legăturilor comerciale care conferă controlul. Acestea includ, dar nu se limitează la o listă de persoane fizice sau juridice cu care furnizorii auditați (sau acționarii furnizorului auditat, inclusiv nivelurile intermediare până la proprietarii finali) au o relație comercială care (a) conduce la un nivel de control asupra conducerii și a resurselor similar cu cel al proprietății asupra deținerii de acțiuni sau active și (b) are o durată foarte lungă (de exemplu, contracte de furnizare pe termen lung foarte importante sau credite oferite de producătorii de software/clienți, împreună cu legături structurale);

(b) documentele justificative ar trebui să includă acorduri de cooperare cu organismul din sectorul public sau cu producătorii de software etc.

(5) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi referitoare la legăturile financiare care conferă controlul:

(a) furnizorul auditat ar trebui să enumere persoanele fizice sau juridice (inclusiv acționarii sau proprietarii care dețin controlul) de care furnizorul auditat (sau proprietarii) sunt dependenți din punct de vedere financiar într-un mod care le-ar putea permite să obțină concesiuni în domenii strategice de activitate;

(b) documentele justificative ar trebui să includă documente de împrumut, statute, documente care să demonstreze legătura financiară etc.

(6) Furnizorul auditat ar trebui să îi furnizeze organizației de audit următoarele dovezi referitoare la alte surse de control:

(a) furnizorii auditați ar trebui să îi indice organizației de audit dacă există orice alte mijloace, procese sau legături care conferă în cele din urmă controlul unei alte țări terțe sau unei entități juridice stabilite într-o țară terță (nivel de control asupra gestiunii și a resurselor similar cu cel al dreptului de proprietate asupra acțiunilor sau activelor și de lungă durată);

(b) documentele justificative ar trebui să furnizeze dovezi ale unui astfel de control sau o declarație conform căreia nu există un astfel de control (această declarație poate proveni de la consiliul de administrație al furnizorului de servicii).

NB: *Elementele care ar trebui luate în considerare la evaluarea controlului sunt structurile de proprietate și drepturile specifice, guvernanța corporativă, legăturile comerciale care conferă control, legăturile financiare care conferă control și orice alte surse de control.*

7.2. Etape suplimentare bazate pe încheierea testului privind proprietatea și controlul

În cazul în care organizația de audit stabilește că furnizorul auditat face obiectul controlului unei țări terțe sau al unei entități juridice dintr-o țară terță, aceasta ar trebui să solicite următoarele probe suplimentare:

(c) care să demonstreze adoptarea de către Comisie a unei decizii în temeiul articolului 19 cu privire la țara terță care exercită controlul asupra furnizorului de servicii de cloud computing;

(d) toate dovezile care demonstrează că furnizorul auditat și orice subcontractant implicat în furnizarea serviciului auditat au pus în aplicare măsurile necesare

pentru a asigura separarea juridică, tehnică și organizațională efectivă între furnizorul de servicii de cloud computing și orice țară terță sau entitate juridică stabilită într-o țară terță, asigurându-se că furnizorul de servicii de cloud computing nu este în măsură să respecte, din punct de vedere juridic, tehnic și operațional, nicio cerere de acces la datele clienților, inclusiv la datele criptate, sau de perturbare a continuității serviciului sau de degradare a calității serviciului;

(e) toate dovezile care demonstrează că organismul din sectorul public va fi informat cu privire la orice astfel de cerere și o confirmare că respectiva cerere a fost refuzată;

(f) toate dovezile care demonstrează menținerea unei evidențe actualizate a oricărei cereri de acces la datele clienților, de perturbare a continuității serviciului sau de degradare a calității serviciului din partea unei țări terțe sau a unei entități juridice stabilite într-o țară terță, care conțin cel puțin cererea și răspunsul la cerere.

8. Criteriul de audit H – absența asistenței tehnice și operaționale din afara Uniunii

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (h) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) dovada că furnizorul auditat a stabilit clauze contractuale obligatorii care prevăd că toate activitățile de asistență, administrare, întreținere, monitorizare, răspuns la incidente și activități operaționale trebuie inițiate și efectuate exclusiv în Uniune. Aceasta ar putea include clauze contractuale care să impună divulgarea prealabilă a tuturor subcontractanților și a locațiilor de unde se asigură asistența, aprobarea scrisă prealabilă înainte de contractarea oricăror noi subcontractanți și dreptul de a refuza serviciile oricărui subcontractant situat în afara Uniunii;

(2) dovada că furnizorul auditat ține un registru actualizat al subcontractanților;

(3) dovada că furnizorul auditat nu subcontractează sau nu transferă astfel de activități în afara Uniunii;

(4) dovada că furnizorul auditat a pus în aplicare măsurile juridice, tehnice și organizatorice necesare pentru a se asigura că nu poate exista acces de la distanță pentru asistență tehnică și operațională din afara Uniunii pentru serviciul auditat;

(5) dovada că serviciul de asistență/serviciile de suport ale furnizorului auditat, administrarea infrastructurii, operațiunile centrului său de operațiuni de securitate (SOC) sau ale centrului său de operațiuni de rețea (NOC), accesul privilegiat, gestionarea copiilor de rezervă și operațiunile de recuperare în caz de dezastru ale serviciului auditat sunt furnizate exclusiv din Uniune, inclusiv calea de acces pentru operarea serviciului;

(6) dovada că furnizorul auditat se asigură că personalul care părăsește societatea nu mai are acces la serviciul auditat și revocă toate politicile de acces;

(7) dovada că furnizorul auditat a pus în aplicare măsurile tehnice și organizatorice necesare pentru a se asigura că accesul administrativ la sistemele utilizate pentru exploatarea serviciului auditat este furnizat prin intermediul unor căi de acces situate pe teritoriul Uniunii. Acest lucru poate fi demonstrat prin punerea în aplicare a unor controale de rețea limitate din punct de vedere geografic, a unei infrastructuri

administrative cu sediul în Uniune, a unor controale de gestionare a accesului privilegiat și a unor mecanisme de monitorizare;

(8) dovada că furnizorul auditat dispune de proceduri care atestă că nu există un control efectiv al unei țări terțe sau al unei entități juridice stabilite într-o țară terță, inclusiv pentru subcontractarea ulterioară.

9. Criteriul de audit I – asigurarea transparenței lanțului de aprovizionare cu software

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (i) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Furnizorul auditat ar trebui să pună la dispoziția organizației de audit o listă completă și actualizată a materialelor software (SBOM) pentru toate componentele software, inclusiv pentru software-ul cu sursă deschisă.

(2) Furnizorul auditat ar trebui să pună la dispoziția organizației de audit o listă a dependențelor. Aceasta ar trebui să includă:

(a) toate modulele de software, bibliotecile sau interfețele de programare a aplicațiilor (API) utilizate, precum și instrumentele de dezvoltare;

(b) proveniența software-ului: locul (țara de proveniență) în care este proiectat, dezvoltat și întreținut software-ul, precum și partea care l-a proiectat, dezvoltat și întreținut, locul și jurisdicția care reglementează distribuția software-ului și actualizările;

(c) gradul de dependență de furnizori, instalații sau tehnologii care fac obiectul unui drept de proprietate din afara UE; pentru nivelul 3, dovada că, în cazul în care pachetul de software este furnizat de o entitate dintr-o țară terță, nu există restricții nejustificate în materie de acordare a licențelor;

(d) gradul de dependență de software cu sursă deschisă;

(e) vizibilitatea la nivelul întregului lanț de producători și subproducători de software, inclusiv drepturile de audit.

***NB**: cerințele de mai sus implică faptul că întreprinderile comune constituite, de exemplu, de o entitate din Uniune cu o entitate juridică stabilită într-o țară terță se pot califica pentru acest nivel.*

(3) Furnizorul auditat ar trebui să furnizeze:

(a) dovada unui proces bazat pe riscuri pentru identificarea și atenuarea dependențelor de producătorii externi de software relevanți pentru exploatarea serviciului de cloud computing;

(b) dovada că a identificat una sau mai multe soluții de software alternative, inclusiv software cu sursă deschisă. În cazul în care nu poate fi identificat un software echivalent, trebuie identificată o soluție care să asigure o funcționalitate viabilă minimă. Trebuie efectuate teste și elaborat un plan de tranziție care să permită migrarea către astfel de soluții alternative;

(c) dovada că poate migra către o soluție alternativă în cazul unui defect sau al unei deficiențe a furnizorului sau al unor restricții din partea unei țări terțe sau a unei entități juridice stabilite într-o țară terță;

(d) o listă a standardelor deschise care sunt urmate ca parte a politicilor furnizorilor auditați în ceea ce privește serviciul auditat;

(4) Furnizorul auditat ar trebui să asigure transparența prin acces de la distanță și posibilitatea auditării codului sursă prin:

(a) punerea la dispoziția organizației de audit a unei liste de dovezi pentru a dovedi că nu se utilizează nicio funcționalitate și niciun mecanism de la distanță care ar putea fi utilizat pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software. Aceasta ar trebui să includă:

(i) dovezi legate de testarea componentei software pentru a preveni utilizarea oricăror funcționalități sau mecanisme de la distanță care ar putea fi utilizate pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software (procedură de testare, rapoarte de testare, plan de testare etc.);

(ii) dovezi referitoare la faptul că procedurile de gestionare a modificărilor ale organizației acoperă orice modificare la nivel de firmware, BIOS și actualizări de software, precum și integrarea de noi componente pentru a preveni utilizarea oricărei funcționalități sau a oricărui mecanism de la distanță;

(iii) dovezi referitoare la faptul că procedura de întreținere este actualizată pentru a include împiedicarea oricărei funcționalități sau a oricărui mecanism de la distanță care ar putea fi utilizat pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software.

(b) Furnizorul auditat trebuie să se asigure că auditorului independent terț i se acordă dreptul de a accesa și de a audita codul sursă al unui astfel de software. Furnizorul auditat trebuie, de asemenea, să se asigure că întreaga documentație, toate materialele tehnice și toate informațiile necesare pentru evaluarea și auditarea codului sursă sunt puse la dispoziția organizației de audit într-un format complet, exact și accesibil.

10. Criteriul de audit J – software cu sursă deschisă

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (j) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Furnizorul auditat ar trebui să asigure transparența prin acces de la distanță și posibilitatea auditării codului sursă prin:

(a) punerea la dispoziția organizației de audit a unei liste de dovezi pentru a dovedi că nu se utilizează nicio funcționalitate și niciun mecanism de la distanță care ar putea fi utilizat pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software. Aceasta ar trebui să includă:

(i) dovezi legate de testarea componentei software pentru a preveni utilizarea oricăror funcționalități sau mecanisme de la distanță care ar putea fi utilizate pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software (procedură de testare, rapoarte de testare, plan de testare etc.);

(ii) dovezi referitoare la faptul că procedurile de gestionare a modificărilor a organizației includ orice modificare la nivel de firmware, BIOS și actualizări de software, precum și integrarea de noi componente pentru a preveni utilizarea oricărei funcționalități sau a oricărui mecanism de la distanță;

(iii) dovezi referitoare la faptul că procedura de întreținere este actualizată pentru a include împiedicarea oricărei funcționalități sau a oricărui mecanism de la distanță care ar putea fi utilizat pentru a manipula sau a perturba în mod semnificativ un dispozitiv, un sistem sau un software.

(2) Furnizorul auditat ar trebui să furnizeze:

(a) dovada unui proces bazat pe riscuri pentru identificarea și atenuarea: (i) unui ecosistem slab și a unui sprijin insuficient din partea comunității pentru software-ul cu sursă deschisă; (ii) lipsei monitorizării continue a actualizărilor publicate; (iii) situațiilor în care software-ul cu sursă deschisă este perimat sau nu mai este menținut.

(b) dovada faptului că furnizorul auditat a aplicat software-ul cu sursă deschisă actualizat fără întârzieri nejustificate;

(c) dovada faptului că furnizorul auditat a identificat una sau mai multe soluții alternative cu sursă deschisă. În cazul în care furnizorul auditat nu poate identifica un software echivalent, acesta trebuie să identifice o soluție care să asigure o funcționalitate viabilă minimă. Furnizorul auditat trebuie să efectueze teste și să elaboreze un plan de tranziție care să permită migrarea către soluțiile alternative respective.

(3) În cazul în care furnizorul auditat utilizează un software publicat în temeiul unei licențe cu sursă deschisă, furnizorul auditat ar trebui să pună în aplicare mecanisme de detectare și de notificare în timp util a organismului din sectorul public în cazul în care software-ul este achiziționat de o țară terță sau de o entitate juridică sau o fundație stabilită într-o țară terță sau intră sub controlul acestora.

11. Criteriul de audit K – servicii la nivel mondial și filiale în țări terțe

Organizația de audit ar trebui să evalueze criteriul de audit prevăzut la litera (k) din anexa II pentru nivelurile de asigurare 2, 3 și 4 ale Uniunii pe baza următoarelor probe:

(1) Organizația de audit ar trebui să verifice dacă filiala este independentă din punct de vedere juridic și operațional de furnizorul auditat.

(2) Furnizorul auditat trebuie să demonstreze că filiala nu are acces la sistemele de prelucrare sau stocare a datelor clienților.

(3) Furnizorul auditat trebuie să demonstreze că filiala nu are conturi cu privilegii în mediile de producție ale Uniunii, inclusiv în ceea ce privește administrarea în materie de cloud, gestionarea identității și a accesului (IAM), gestionarea accesului privilegiat (PAM), monitorizarea sau administrarea bazelor de date.

(4) Organizația de audit ar trebui să se asigură că personalul filialei nu poate obține acces la datele clienților din Uniune.

(5) Organizația de audit ar trebui să se asigure că filiala nu are autoritatea de a instrui personalul operațional al Uniunii să divulge date ale clienților sau să eludeze procedurile de securitate.

(6) Organizația de audit ar trebui să verifice dacă toate solicitările din partea administrației publice străine primite de filială sunt redirecționate în mod oficial către entitatea competentă din Uniune pentru evaluare juridică în temeiul dreptului Uniunii și al dreptului intern.