2024/1773

25.6.2024

REGULAMENTUL DELEGAT (UE) 2024/1773 AL COMISIEI

din 13 martie 2024

de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează conținutul detaliat al politicii referitoare la acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 ([1]), în special articolul 28 alineatul (10) al treilea paragraf,

întrucât:

(1) Cadrul privind reziliența operațională digitală pentru sectorul financiar instituit prin Regulamentul (UE) 2022/2554 impune entităților financiare obligația să stabilească anumite principii-cheie pentru gestionarea riscurilor TIC generate de părți terțe, care sunt deosebit de importante atunci când entitățile financiare recurg la furnizori terți de servicii TIC care să sprijine funcțiile lor critice sau importante.

(2) Entitățile financiare, ca parte a cadrului lor de gestionare a riscurilor TIC, trebuie să adopte și să revizuiască periodic o strategie privind riscurile TIC generate de părți terțe. În conformitate cu articolul 28 alineatul (2) din Regulamentul (UE) 2022/2554, strategia respectivă trebuie să includă o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC. Aceasta se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată.

(3) Există diferențe mari între entitățile financiare în ceea ce privește dimensiunea, structura și organizarea lor internă, precum și în ceea ce privește natura și complexitatea activităților și operațiunilor lor. Este necesar să se țină seama de această diversitate, impunând totodată anumite cerințe de reglementare fundamentale care sunt adecvate pentru toate entitățile financiare care elaborează politica referitoare la acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC („politica”), și să se asigure că cerințele respective se aplică într-un mod proporțional.

(4) Atunci când entitățile financiare aparțin unui grup, societatea-mamă care este responsabilă cu furnizarea situațiilor financiare consolidate sau subconsolidate pentru grup ar trebui, așadar, să se asigure că politica este aplicată în mod consecvent și coerent în cadrul grupului.

(5) Atunci când aplică politica, furnizorii de servicii TIC intragrup, inclusiv cei deținuți integral sau colectiv de entități financiare din cadrul aceluiași sistem instituțional de protecție, ar trebui să fie considerați furnizori terți de servicii TIC. Riscurile generate de furnizorii de servicii TIC intragrup pot fi diferite, însă în temeiul Regulamentului (UE) 2022/2554 cerințele aplicabile acestora sunt aceleași. În mod similar, atunci când există un lanț de furnizori terți de servicii TIC, politica ar trebui să se aplice subcontractanților care oferă furnizorilor terți de servicii TIC servicii TIC care sprijină funcții critice sau importante sau părți semnificative ale acestora.

(6) Responsabilitatea finală a organului de conducere pentru gestionarea riscurilor TIC ale unei entități financiare este un principiu general care se aplică și în ceea ce privește utilizarea furnizorilor terți de servicii TIC. Această responsabilitate ar trebui transpusă ulterior prin implicarea continuă a organului de conducere în controlul și monitorizarea gestionării riscurilor TIC, inclusiv în adoptarea și revizuirea, cel puțin o dată pe an, a politicii.

([1]) JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Pentru a asigura raportarea adecvată către organul de conducere, politica ar trebui să specifice și să identifice în mod clar responsabilitățile interne pentru aprobarea, gestionarea, controlul și documentarea acordurilor contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizorii terți de servicii TIC („acorduri contractuale"), inclusiv serviciile TIC furnizate în temeiul acordurilor contractuale menționate la articolul 28 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554.

(8) Pentru a ține seama de toate riscurile posibile care pot apărea atunci când sunt contractate servicii TIC care sprijină o funcție critică sau importantă, structura politicii ar trebui să urmeze toate etapele fiecărei faze principale a ciclului de viață pentru acordurile contractuale cu furnizorii terți.

(9) Pentru a atenua riscurile identificate, politica ar trebui să specifice planificarea acordurilor contractuale, inclusiv evaluarea riscurilor, diligența necesară și procesul de aprobare a unor modificări noi sau semnificative ale acordurilor contractuale respective. Pentru a gestiona riscurile care pot apărea înainte de încheierea unui acord contractual cu un furnizor terț de servicii TIC, politica ar trebui să specifice un proces adecvat și proporțional de selectare și evaluare a caracterului adecvat al potențialilor furnizori terți de servicii TIC și să impună entității financiare obligația să ia în considerare o listă neexhaustivă de elemente de care ar trebui să dispună furnizorii terți de servicii TIC. Lista ar trebui să includă elemente legate de reputația comercială a furnizorilor de servicii, de resursele financiare, umane și tehnice ale acestora, de securitatea informațiilor, de structura lor organizațională, inclusiv în ceea ce privește gestionarea riscurilor, precum și de controalele lor interne.

(10) Pentru a se asigura gestionarea solidă a riscurilor în ceea ce privește furnizarea de servicii TIC care sprijină funcții critice sau importante de către furnizorii terți de servicii TIC, politica ar trebui să conțină informații cu privire la punerea în aplicare, monitorizarea și gestionarea acordurilor contractuale, inclusiv la nivel consolidat și subconsolidat, după caz. Acest lucru include cerințe privind clauzele contractuale referitoare la obligațiile reciproce ale entităților financiare și ale furnizorilor terți de servicii TIC, care ar trebui stabilite în scris. Pentru a asigura supravegherea eficientă și a promova reziliența în cazul unor modificări ale modelului de afaceri sau ale mediului de afaceri, politica ar trebui să asigure dreptul entităților financiare sau al părților terțe desemnate și al autorităților competente de a efectua inspecții și de a avea acces la informații și ar trebui să precizeze, totodată, mai în detaliu strategiile de ieșire și procesele de încetare a acordurilor contractuale.

(11) În măsura în care furnizorii terți de servicii TIC prelucrează date cu caracter personal, această politică și orice acorduri contractuale nu aduc atingere obligațiilor prevăzute în Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([2]) și ar trebui să completeze aceste obligații, de exemplu impunerea încheierii unui contract scris care să descrie prelucrarea datelor cu caracter personal, cerința de a asigura securitatea prelucrării datelor cu caracter personal și stabilirea tuturor celorlalte elemente necesare în temeiul regulamentului menționat.

([2]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Comitetul comun al autorităților europene de supraveghere menționat la articolul 54 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([3]), la articolul 54 din Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([4]) și la articolul 54 din Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului ([5]) a efectuat consultări publice deschise cu privire la proiectul de standarde tehnice de reglementare pe care se bazează prezentul regulament, a analizat costurile și beneficiile potențiale ale standardelor propuse și a solicitat avizul Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1093/2010, al Grupului părților interesate din domeniul asigurărilor și reasigurărilor și al Grupului părților interesate din domeniul pensiilor ocupaționale, instituite în conformitate cu articolul 37 din Regulamentul (UE) nr. 1094/2010, precum și al Grupului părților interesate din domeniul valorilor mobiliare și piețelor, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1095/2010.

(13) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]) și a emis un aviz la 24 ianuarie 2024,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Profilul general de risc și complexitatea

Politica privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC („politica") ține seama de dimensiunea și profilul general de risc ale entității financiare, precum și de natura, amploarea și elementele complexității sporite sau reduse a serviciilor, activităților și operațiunilor sale, inclusiv de următoarele elemente:

(a) tipul de servicii TIC incluse în acordul contractual privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC („acordul contractual") dintre entitatea financiară și furnizorul terț de servicii TIC;

(b) locul în care se află furnizorul terț de servicii TIC sau societatea-mamă a acestuia;

(c) dacă serviciile TIC care sprijină funcții critice sau importante sunt furnizate de un furnizor terț de servicii TIC situat într-un stat membru sau într-o țară terță, luând în considerare, de asemenea, locul din care sunt furnizate serviciile TIC și locul în care sunt prelucrate și stocate datele;

(d) natura datelor partajate cu furnizorul terț de servicii TIC;

(e) dacă furnizorul terț de servicii TIC face parte din același grup ca entitatea financiară căreia îi sunt furnizate serviciile;

([3]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Bancară Europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Europeană de Asigurări și Pensii Ocupaționale), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Europeană pentru Valori Mobiliare și Piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(f) utilizarea furnizorilor terți de servicii TIC care sunt autorizați, înregistrați sau supuși supravegherii sau controlului de către o autoritate competentă dintr-un stat membru sau care fac obiectul cadrului de supraveghere prevăzut în capitolul V secțiunea II din Regulamentul (UE) 2022/2554 și utilizarea furnizorilor terți de servicii TIC care nu sunt;

(g) utilizarea furnizorilor terți de servicii TIC care sunt autorizați, înregistrați sau supuși supravegherii sau controlului de către o autoritate de supraveghere dintr-o țară terță și utilizarea furnizorilor terți de servicii TIC care nu sunt;

(h) dacă furnizarea de servicii TIC care sprijină funcții critice sau importante este concentrată la un singur furnizor terț de servicii TIC sau la un număr mic de astfel de furnizori de servicii;

(i) transferabilitatea serviciilor TIC care sprijină funcții critice sau importante către un alt furnizor terț de servicii TIC, inclusiv ca urmare a particularităților tehnologice;

(j) impactul potențial al perturbărilor în furnizarea serviciilor TIC care sprijină funcții critice sau importante asupra continuității activităților entității financiare și asupra disponibilității serviciilor sale.

Articolul 2

Aplicarea la nivel de grup

În cazul în care prezentul regulament se aplică pe bază subconsolidată sau consolidată, societatea-mamă care este responsabilă cu furnizarea situațiilor financiare consolidate sau subconsolidate pentru grup se asigură că politica este pusă în aplicare în mod consecvent în toate entitățile financiare care fac parte din grup și este adecvată pentru aplicarea efectivă a prezentului regulament la toate nivelurile relevante ale grupului.

Articolul 3

Mecanisme de guvernanță

(1) Organul de conducere revizuiește politica cel puțin o dată pe an și o actualizează dacă este necesar. Modificările aduse politicii trebuie puse în aplicare în timp util și de îndată ce acest lucru este posibil în cadrul acordurilor contractuale relevante. Entitatea financiară documentează calendarul planificat pentru punerea în aplicare.

(2) Politica stabilește sau face trimitere la o metodologie de stabilire a serviciilor TIC care sprijină funcții critice sau importante. Politica specifică, de asemenea, momentul în care această evaluare urmează să fie efectuată și revizuită.

(3) Politica atribuie în mod clar responsabilitățile interne pentru aprobarea, gestionarea, controlul și documentarea acordurilor contractuale relevante și asigură că se mențin competențele, experiența și cunoștințele adecvate în cadrul entității financiare pentru a supraveghea în mod eficace acordurile contractuale relevante, inclusiv serviciile TIC furnizate în temeiul acordurilor respective.

(4) Fără a aduce atingere responsabilității finale a entității financiare de a supraveghea în mod eficace acordurile contractuale relevante, politica impune obligația ca furnizorul terț de servicii TIC să facă obiectul unei evaluări care să ateste că respectivul furnizor dispune de resurse suficiente pentru a garanta că entitatea financiară respectă toate cerințele juridice și de reglementare în ceea ce privește serviciile TIC care sprijină funcțiile critice sau importante furnizate.

(5) Politica identifică în mod clar rolul sau membrul personalului de conducere de nivel superior responsabil cu monitorizarea acordurilor contractuale relevante. Politica specifică modul în care acest rol sau membru al personalului de conducere de nivel superior trebuie să coopereze cu funcțiile de control, cu excepția cazului în care face parte din acestea, și precizează liniile de raportare către organul de conducere, inclusiv natura informațiilor care trebuie raportate și documentele care trebuie furnizate. Politica stabilește, de asemenea, frecvența acestor raportări.

(6) Politica garantează că acordurile contractuale sunt conforme cu următoarele:

(a) cadrul de gestionare a riscurilor TIC menționat la articolul 6 din Regulamentul (UE) 2022/2554;

(b) politica de securitate a informațiilor menționată la articolul 9 alineatul (4) din Regulamentul (UE) 2022/2554;

(c) politica de continuitate a activității TIC menționată la articolul 11 din Regulamentul (UE) 2022/2554;

(d) cerințele privind raportarea incidentelor prevăzute la articolul 19 din Regulamentul (UE) 2022/2554.

(7) Politica impune obligația ca serviciile TIC care sprijină funcții critice sau importante furnizate de furnizori terți de servicii TIC să facă obiectul unei analize independente și să fie incluse în planul de audit.

(8) Politica specifică în mod explicit că acordurile contractuale trebuie:

(a) să nu exonereze entitatea financiară și organul său de conducere de obligațiile de reglementare și de responsabilitățile față de clienți;

(b) să nu împiedice supravegherea eficace a unei entități financiare și să nu contravină vreunei restricții de supraveghere a serviciilor și activităților;

(c) să impună obligația furnizorilor terți de servicii TIC să coopereze cu autoritățile competente;

(d) să impună obligația ca entitatea financiară, auditorii acesteia și autoritățile competente să aibă acces efectiv la datele și sediile legate de utilizarea serviciilor TIC care sprijină funcții critice sau importante.

Articolul 4

Principalele etape ale ciclului de viață pentru adoptarea și utilizarea acordurilor contractuale

Politica specifică cerințele, inclusiv regulile, responsabilitățile și procesele, pentru fiecare etapă principală a ciclului de viață al acordului contractual, acoperind cel puțin următoarele:

(a) responsabilitățile organului de conducere, inclusiv implicarea acestuia, după caz, în procesul decizional privind utilizarea serviciilor TIC care sprijină funcții critice sau importante furnizate de furnizori terți de servicii TIC;

(b) planificarea acordurilor contractuale, inclusiv evaluarea riscurilor, diligența necesară, astfel cum se prevede la articolele 5 și 6, și procesul de aprobare a noilor acorduri contractuale sau a modificărilor semnificative ale acestora, astfel cum se prevede la articolul 8 alineatul (4);

(c) implicarea unităților operaționale, a controalelor interne și a altor unități relevante în ceea ce privește acordurile contractuale;

(d) punerea în aplicare, monitorizarea și gestionarea acordurilor contractuale, astfel cum se prevede la articolele 7, 8 și 9, inclusiv la nivel consolidat și subconsolidat, după caz;

(e) documentarea și ținerea evidențelor, ținând seama de cerințele privind registrul de informații prevăzute la articolul 28 alineatul (3) din Regulamentul (UE) 2022/2554;

(f) strategiile de ieșire și procesele de încetare a acordurilor contractuale, astfel cum sunt prevăzute la articolul 10.

Articolul 5

Evaluarea *ex ante* a riscurilor

(1) Politica prevede obligația de a defini nevoile operaționale ale entității financiare înainte de încheierea unui acord contractual.

(2) Politica prevede obligația de a efectua o evaluare a riscurilor la nivelul entității financiare și, după caz, la nivel consolidat și subconsolidat înainte de încheierea unui acord contractual.

Evaluarea riscurilor ține seama de toate cerințele relevante prevăzute în Regulamentul (UE) 2022/2554 și în legislația sectorială aplicabilă a Uniunii. Evaluarea riscurilor ia în considerare, în special, impactul furnizării de servicii TIC care sprijină funcții critice sau importante de către furnizori terți de servicii TIC asupra entității financiare și toate riscurile pe care le prezintă furnizarea respectivelor servicii TIC care sprijină funcții critice sau importante de către furnizori terți de servicii TIC, inclusiv următoarele:

(a) riscurile operaționale;

(b) riscurile juridice;

(c) riscurile TIC;

(d) riscurile reputaționale;

(e) riscurile legate de protecția datelor confidențiale sau cu caracter personal;

(f) riscurile legate de disponibilitatea datelor;

(g) riscurile legate de locul în care sunt prelucrate și stocate datele;

(h) riscurile legate de locul în care se află furnizorul terț de servicii TIC;

(i) riscurile de concentrare a serviciilor TIC la nivel de entitate.

Articolul 6

Diligența necesară

(1) Politica stabilește un proces adecvat și proporțional pentru selectarea și evaluarea potențialilor furnizori terți de servicii TIC, ținând seama de apartenența sau nu a furnizorului terț de servicii TIC la furnizorii intragrup de servicii TIC, și impune obligația ca entitatea financiară să evalueze, înainte de a încheia un acord contractual, dacă furnizorul terț de servicii TIC:

(a) are o reputație comercială, capacități suficiente, expertiză și resurse financiare, umane și tehnice adecvate, standarde de securitate a informațiilor, o structură organizațională, o gestionare a riscurilor și controale interne adecvate și, după caz, autorizațiile sau înregistrările necesare pentru a furniza servicii TIC care sprijină funcția critică sau importantă într-un mod fiabil și profesionist;

(b) are capacitatea de a monitoriza evoluțiile tehnologice relevante și de a identifica cele mai bune practici în materie de securitate TIC și de a le pune în aplicare atunci când este cazul pentru a dispune de un cadru eficace și solid de reziliență operațională digitală;

(c) utilizează sau intenționează să utilizeze subcontractanți TIC pentru a presta servicii TIC care sprijină funcții critice sau importante sau părți semnificative ale acestora;

(d) este localizat, prelucrează sau stochează datele într-o țară terță și, în caz afirmativ, dacă această practică afectează nivelul riscurilor operaționale sau reputaționale sau riscul de a fi afectat de măsuri restrictive, inclusiv embargouri și sancțiuni, care pot avea impact asupra capacității furnizorului terț de servicii TIC de a furniza serviciile TIC sau a entității financiare de a beneficia de respectivele servicii TIC;

(e) aprobă acordurile contractuale care asigură faptul că este posibil în mod efectiv să se efectueze audituri la furnizorul terț de servicii TIC, inclusiv la fața locului, de către entitatea financiară însăși, de către părțile terțe desemnate și de către autoritățile competente;

(f) acționează într-un mod etic și responsabil din punct de vedere social, respectă drepturile omului și drepturile copiilor, inclusiv interdicția privind munca copiilor, respectă principiile aplicabile privind protecția mediului și asigură condiții de muncă adecvate.

(2) Politica specifică nivelul necesar de asigurare în ceea ce privește eficacitatea cadrului de gestionare a riscurilor al furnizorilor terți de servicii TIC pentru serviciile TIC care sprijină funcții critice sau importante care urmează să fie furnizate de un furnizor terț de servicii TIC. Politica prevede obligația de a include în procesul de diligență evaluarea existenței măsurilor de atenuare a riscurilor și de asigurare a continuității activității, precum și a modului în care este asigurată funcționarea acestora în cadrul furnizorului terț de servicii TIC.

(3) Politica stabilește procesul de diligență pentru selectarea și evaluarea potențialilor furnizori terți de servicii TIC și precizează care dintre următoarele elemente urmează să fie utilizate pentru atingerea nivelului necesar de asigurare cu privire la performanța furnizorului terț de servicii TIC:

(a) audituri sau evaluări independente efectuate de entitatea financiară sau în numele acesteia;

(b) utilizarea rapoartelor de audit independente întocmite la cererea furnizorului terț de servicii TIC;

(c) utilizarea rapoartelor de audit întocmite de funcția de audit intern a furnizorului terț de servicii TIC;

(d) utilizarea certificărilor adecvate ale terților;

(e) utilizarea altor informații relevante aflate la dispoziția entității financiare sau a altor informații furnizate de furnizorul terț de servicii TIC.

(4) Entitățile financiare trebuie să garanteze un nivel adecvat de asigurare cu privire la performanța furnizorului terț de servicii TIC, ținând seama de elementele enumerate la alineatul (3) literele (a)-(e). După caz, se utilizează mai multe dintre elementele enumerate la literele respective.

Articolul 7

Conflicte de interese

(1) Politica specifică măsurile adecvate pentru identificarea, prevenirea și gestionarea conflictelor de interese reale sau potențiale care decurg din utilizarea furnizorilor terți de servicii TIC care trebuie luate înainte de a încheia acordurile contractuale relevante și prevede o monitorizare continuă a acestor conflicte de interese.

(2) În cazul în care serviciile TIC care sprijină funcții critice sau importante sunt furnizate de furnizori de servicii TIC intragrup, politica specifică faptul că deciziile privind condițiile, inclusiv condițiile financiare, legate de serviciile TIC trebuie luate în mod obiectiv.

Articolul 8

Clauze contractuale

(1) Politica specifică faptul că acordul contractual relevant trebuie să fie în formă scrisă și să includă toate elementele menționate la articolul 30 alineatele (2) și (3) din Regulamentul (UE) 2022/2554. Politica include, de asemenea, elemente privind cerințele menționate la articolul 1 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, precum și alte acte legislative relevante ale Uniunii și naționale, după caz.

(2) Politica specifică faptul că acordurile contractuale relevante trebuie să includă dreptul entității financiare de a avea acces la informații, de a efectua inspecții și audituri și de a efectua teste cu privire la TIC. În acest scop, politica impune ca entitatea financiară să utilizeze următoarele metode, fără a aduce atingere responsabilității finale a entității financiare:

(a) propriul audit intern sau un audit efectuat de un terț desemnat;

(b) după caz, audituri grupate și testare TIC grupată, inclusiv teste de penetrare bazate pe amenințări, care sunt organizate în comun cu alte entități financiare sau firme contractante care utilizează serviciile TIC ale aceluiași furnizor terț de servicii TIC și care sunt efectuate de respectivele entități financiare sau firme contractante sau de o parte terță desemnată de acestea;

(c) după caz, certificări acordate de terți;

(d) după caz, rapoartele de audit intern sau rapoartele de audit efectuate de terți puse la dispoziție de furnizorul terț de servicii TIC.

(3) Entitatea financiară nu trebuie să se bazeze, în timp, numai pe certificările menționate la alineatul (2) litera (c) sau pe rapoartele de audit menționate la litera (d) de la alineatul respectiv. Politica permite utilizarea metodelor menționate la alineatul (2) literele (c) și (d) numai în cazul în care entitatea financiară:

(a) este convinsă de planul de audit al furnizorului terț de servicii TIC pentru acordurile contractuale relevante;

(b) se asigură că domeniul de aplicare al certificărilor sau al rapoartelor de audit acoperă sistemele și controalele-cheie identificate de aceasta și asigură conformitatea cu cerințele de reglementare relevante;

(c) evaluează în detaliu și în permanență conținutul certificărilor sau al rapoartelor de audit și verifică dacă rapoartele sau certificările respective nu sunt caduce;

(d) se asigură că sistemele și controalele-cheie sunt incluse în versiunile viitoare ale certificării sau ale raportului de audit;

(e) este convinsă de aptitudinile părții care efectuează certificarea sau auditarea;

(f) este convinsă de faptul că certificările sunt emise și auditurile sunt efectuate cu respectarea standardelor profesionale relevante recunoscute pe scară largă și includ un test al eficacității operaționale a controalelor-cheie instituite;

(g) are dreptul contractual de a solicita, cu o frecvență rezonabilă și legitimă din perspectiva gestionării riscurilor, modificări ale domeniului de aplicare al certificărilor sau al rapoartelor de audit pentru a include alte sisteme și controale relevante;

(h) are dreptul contractual de a efectua audituri individuale și grupate, după cum consideră oportun, cu privire la acordurile contractuale și de a exercita aceste drepturi cu frecvența convenită.

(4) Politica garantează că modificările semnificative ale acordurilor contractuale sunt formalizate într-un document scris datat și semnat de toate părțile și specifică procesul de reînnoire a acordurilor contractuale.

Articolul 9

Monitorizarea acordurilor contractuale

(1) Politica prevede obligația ca acordurile contractuale să specifice măsurile și indicatorii-cheie pentru monitorizarea continuă a performanței furnizorilor terți de servicii TIC, inclusiv măsurile de monitorizare a conformității cu cerințele privind confidențialitatea, disponibilitatea, integritatea și autenticitatea datelor și informațiilor, precum și conformitatea furnizorilor terți de servicii TIC cu politicile și procedurile relevante ale entității financiare. Politica specifică, de asemenea, măsurile care se aplică atunci când nu sunt îndeplinite acordurile privind nivelul serviciilor, inclusiv sancțiunile contractuale, dacă este cazul.

(2) Politica specifică modul în care entitatea financiară trebuie să evalueze dacă furnizorii terți de servicii TIC utilizați pentru serviciile TIC care sprijină funcții critice sau importante respectă standarde de performanță și de calitate adecvate, în conformitate cu acordul contractual și cu propriile politici ale entității financiare. Politica asigură în special următoarele:

(a) faptul că furnizorii terți de servicii TIC furnizează entității financiare rapoarte adecvate cu privire la activitățile și serviciile lor, inclusiv rapoarte periodice, rapoarte privind incidentele, rapoarte privind furnizarea de servicii, rapoarte privind securitatea TIC și rapoarte privind măsurile și testele de asigurare a continuității activității;

(b) faptul că performanța furnizorilor terți de servicii TIC este evaluată pe baza indicatorilor-cheie de performanță, a indicatorilor-cheie de control, a auditurilor, a autocertificărilor și a analizelor independente conform cadrului de gestionare a riscurilor TIC al entității financiare;

(c) faptul că entitatea financiară primește alte informații relevante de la furnizorii terți de servicii TIC;

(d) faptul că entitatea financiară este notificată, dacă este cazul, cu privire la incidentele legate de TIC și la incidentele operaționale sau de securitate legate de plăți;

(e) faptul că se efectuează o analiză independentă și audituri pentru verificarea conformității cu cerințele și politicile legale și de reglementare.

(3) Politica specifică faptul că evaluarea menționată la alineatul (2) trebuie să fie documentată, iar rezultatele acesteia trebuie utilizate pentru a actualiza evaluarea riscurilor efectuată de entitatea financiară, astfel cum este menționată la articolul 6.

(4) Politica stabilește măsurile adecvate pe care entitatea financiară trebuie să le adopte în cazul în care identifică deficiențe ale furnizorilor terți de servicii TIC, inclusiv incidente legate de TIC și incidente operaționale sau de securitate legate de plăți, în furnizarea serviciilor TIC care sprijină funcții critice sau importante sau în ceea ce privește conformitatea cu acordurile contractuale sau cu cerințele legale. Politica specifică, de asemenea, modul în care trebuie monitorizată punerea în aplicare a unor astfel de măsuri pentru a se asigura că acestea sunt respectate efectiv într-un interval de timp definit, ținând seama de importanța deficiențelor.

Articolul 10

Retragerea din acordurile contractuale și încetarea acordurilor contractuale

Politica conține cerințe referitoare la un plan de ieșire documentat pentru fiecare acord contractual și la revizuirea și testarea periodică a planului de ieșire documentat. La stabilirea planului de ieșire se iau în considerare următoarele:

(a) întreruperi neprevăzute și persistente ale serviciului;

(b) furnizarea necorespunzătoare sau defectuoasă a serviciilor;

(c) încetarea neașteptată a acordului contractual.

Planul de ieșire trebuie să fie realist, fezabil, bazat pe scenarii plauzibile și pe ipoteze rezonabile și să aibă un calendar planificat de punere în aplicare compatibil cu condițiile de ieșire și de încetare stabilite în acordurile contractuale.

Articolul 11

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 13 martie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN