EIOPA-BoS-20-002

Ghid privind externalizarea către furnizorii de servicii cloud

Cuprins

Introducere

1. În conformitate cu articolul 16 din Regulamentul (UE) nr. 1094/2010[1], EIOPA emite ghiduri care oferă recomandări societăților de asigurare și reasigurare cu privire la modul în care ar trebui aplicate dispozițiile referitoare la externalizare prevăzute în Directiva 2009/138/CE[2] („Directiva Solvabilitate II") și în Regulamentul delegat al Comisiei (UE) nr. 2015/35[3] („Regulamentul delegat") în cazul externalizării către furnizori de servicii cloud.
2. Prezentul ghid se bazează pe articolul 13 alineatul (28), articolele 38 și 49 din Directiva Solvabilitate II și pe articolul 274 din Regulamentul delegat. Mai mult, el se bazează și pe recomandările prevăzute de Ghidul EIOPA privind sistemul de guvernanță (EIOPA-BoS-14/253).
3. Prezentul ghid se adresează autorităților competente pentru a oferi îndrumări cu privire la modul în care societățile de asigurare și reasigurare (denumite colectiv „societăți") ar trebui să aplice cerințele referitoare la externalizare prevăzute în actele juridice menționate mai sus, în contextul externalizării către furnizorii de servicii cloud.
4. Prezentul ghid se aplică atât societăților individuale, cât și *mutatis mutandis* grupurilor[4].

   Entitățile care se supun altor cerințe sectoriale și care fac parte dintr-un grup sunt excluse din sfera de aplicare a prezentului ghid la nivel individual, deoarece ar trebui să respecte cerințele sectoriale specifice, precum și îndrumările relevante emise de Autoritatea Europeană pentru Valori Mobiliare și Piețe și de Autoritatea Bancară Europeană.
5. În cazul externalizării intragrup și al externalizării în lanț către furnizori de servicii cloud, acest ghid ar trebui aplicat împreună cu prevederile din Ghidul EIOPA privind sistemul de guvernanță referitoare la externalizarea intragrup.
6. Societățile și autoritățile competente ar trebui să țină seama de principiul proporționalității[5], atunci când respectă sau supraveghează respectarea acestui ghid, precum și de caracterul critic sau importanța serviciului externalizat către furnizorii de servicii cloud. Principiul proporționalității ar trebui să garanteze că mecanismele de guvernanță, inclusiv cele legate de externalizarea către furnizorii de servicii cloud, sunt proporționale cu natura, amploarea și complexitatea riscurilor subiacente.
7. Acest ghid ar trebui citit în paralel cu Ghidul EIOPA privind sistemul de guvernanță și fără a aduce atingere acestuia și obligațiilor prevăzute de reglementările enumerate la punctul 1.

Definiții

8. Termenii care nu sunt definiți în prezentul ghid au sensul definit în actele juridice menționate în introducere.

---

[1] Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru 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).

[2] Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1).

[3] Regulamentul delegat (UE) 2015/35 al Comisiei din 10 octombrie 2014 de completare a Directivei 2009/138/CE a Parlamentului European și a Consiliului privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 12, 17.1.2015, p. 1).

[4] Articolul 212 alineatul (1) din Directiva Solvabilitate II.

[5] Articolul 29 alineatul (3) din Directiva Solvabilitate II.

9. În plus, în sensul prezentului ghid, se aplică următoarele definiții:

Furnizor de servicii	O entitate terță care realizează un proces, serviciu sau activitate, sau părți din acestea, în baza unui acord de externalizare.
Furnizor de servicii cloud	Un furnizor de servicii, astfel cum este definit mai sus, responsabil de furnizarea de servicii cloud în cadrul unui acord de externalizare.
Servicii cloud	Servicii furnizate cu ajutorul tehnologiilor de calcul de tip cloud, și anume un model pentru permiterea accesului universal, convenabil, la cerere în rețea la un grup comun de resurse de calcul configurabile (de exemplu rețele, servere, soluții de stocare, aplicații și servicii), care poate fi rapid pus la dispoziție și lansat cu un efort minim de gestionare sau interacțiune cu furnizorul serviciului.
Cloud public	Infrastructură de tip cloud disponibilă pentru utilizare liberă de către publicul larg.
Cloud privat	Infrastructură de tip cloud disponibilă pentru utilizare exclusivă de către o singură societate.
Cloud comunitar	Infrastructură de tip cloud disponibilă pentru utilizare exclusivă de către o anumită comunitate de entități , de exemplu, mai multe entități dintr-un singur grup.
Cloud hibrid	Infrastructură de tip cloud compusă din două sau mai multe infrastructuri distincte de tip cloud.

Data aplicării

10. Prezentul ghid se aplică de la 1 ianuarie 2021 tuturor acordurilor de externalizare în cloud încheiate sau modificate la această dată sau ulterior.

11. Societățile ar trebui să revizuiască și să modifice în mod corespunzător acordurile existente de externalizare asociate unor funcții sau activități operaționale critice sau importante, pentru a asigura respectarea acestui ghid până la 31 decembrie 2022.

12. În cazul în care revizuirea acordurilor de externalizare a serviciilor cloud asociate funcțiilor sau activităților operaționale critice sau importante nu este finalizată până la data de 31 decembrie 2022, societatea ar trebui să informeze autoritatea de supraveghere[6] cu privire la acest aspect, precizând inclusiv măsurile avute în vedere pentru a finaliza revizuirea sau posibila strategie de încetare a acordurilor. Autoritatea de supraveghere poate conveni cu societatea prelungirea termenului pentru finalizarea revizuirii, dacă este cazul.

13. Actualizarea (acolo unde este necesar) a politicilor și proceselor interne ale societății ar trebui efectuată până la 1 ianuarie 2021, iar cerințele privind documentarea pentru acordurile de externalizare în cloud asociate funcțiilor sau activităților operaționale critice sau importante ar trebui puse în aplicare până la 31 decembrie 2022.

[6] Articolul 13 alineatul (10) din Directiva Solvabilitate II.

Recomandarea 1 - Serviciile cloud și externalizarea

14. Societatea ar trebui să stabilească dacă un acord cu un furnizor de servicii cloud se încadrează în definiția externalizării în conformitate cu Directiva Solvabilitate II. În cadrul evaluării, ar trebui avut în vedere:

a. dacă funcția sau activitatea operațională externalizată (sau o parte a acesteia) este efectuată în mod repetat sau continuu; și

b. dacă această funcție sau activitate operațională (sau o parte a acesteia) ar intra, în mod normal, în sfera funcțiilor sau activităților operaționale care vor fi sau ar putea fi îndeplinite de societate în cadrul activităților comerciale obișnuite, chiar dacă societatea nu a efectuat această funcție sau activitate operațională în trecut.

15. În cazul în care un acord cu un furnizor de servicii acoperă mai multe funcții sau activități operaționale, societatea ar trebui să ia în considerare toate aspectele acordului în cadrul evaluării.

16. În cazurile în care societatea externalizează funcții sau activități operaționale către furnizori de servicii care nu sunt furnizori de servicii cloud, dar care se bazează în mod semnificativ pe infrastructuri de tip cloud pentru furnizarea serviciilor (de exemplu, când furnizorul de servicii cloud face parte dintr-un lanț de externalizare), acordul pentru o astfel de externalizare intră în sfera de aplicare a prezentului ghid.

Recomandarea 2 – Principii generale de guvernanță pentru externalizarea în cloud

17. Fără a aduce atingere articolului 274 alineatul (3) din Regulamentul delegat, organul administrativ, de conducere sau de control („AMSB”) al societății ar trebui să se asigure că deciziile de a externaliza funcții sau activități operaționale critice sau importante către furnizori de servicii cloud se bazează pe o evaluare detaliată a riscurilor, care are în vedere toate riscurile relevante aferente acordului, cum ar fi cele legate de tehnologia informației și comunicațiilor („TIC”), de continuitatea activității, riscul juridic, riscul de conformitate, riscul de concentrare și alte riscuri operaționale, precum și riscurile asociate fazei de migrare a datelor și/sau fazei de implementare, după caz.

18. În cazul externalizării către furnizorii de servicii cloud a funcțiilor sau activităților operaționale critice sau importante, societatea ar trebui, după caz, să țină cont în autoevaluarea riscurilor și a solvabilității („ORSA”), de modificările din profilul de risc asociate acordurilor de externalizare în cloud.

19. Utilizarea serviciilor cloud ar trebui să fie în concordanță cu strategiile societății (de exemplu, strategia TIC, strategia de securitate a informațiilor, strategia de management al riscului operațional) și cu politicile și procesele interne, care ar trebui actualizatecând este necesar.

Recomandarea 3 – Actualizarea politicii scrise de externalizare

20. În cazul externalizării către furnizorii de servicii cloud, societatea ar trebui să actualizeze politica de externalizare scrisă (de exemplu, prin revizuire, prin adăugare de anexe sau elaborare de noi politici dedicate) și celelalte politici interne relevante (de exemplu, securitatea informațiilor), luând în considerare anumite specificități ale externalizării în cloud cel puțin în ceea ce privește:

a. rolurile și responsabilitățile funcțiilor implicate din societăți, în special AMSB, și funcțiile responsabile de TIC, securitatea informațiilor, conformitate, managementul riscului și audit intern;

b. procesele și procedurile de raportare necesare pentru aprobarea, punerea în aplicare, monitorizarea, managementul și reînnoirea, după caz, a acordurilor de externalizare în cloud asociate funcțiilor sau activităților operaționale critice sau importante;

c. controlul asupra serviciilor cloud, proporțional cu natura, amploarea și complexitatea riscurilor inerente serviciilor furnizate, inclusiv (i) evaluarea riscurilor asociate acordurilor de externalizare în cloud și evaluarea complexă a furnizorilor de servicii cloud, inclusiv frecvența evaluării riscurilor; (ii) mecanisme de monitorizare și de management (de exemplu, verificarea acordului privind nivelul calității serviciilor); (iii) standarde și mecanisme de securitate;

d. în ceea ce privește externalizarea în cloud a funcțiilor sau activităților operaționale critice sau importante, ar trebui aplicate cerințele contractuale descrise la Recomandarea 10;

e. cerințele de documentare și notificarea scrisă către autoritatea de supraveghere cu privire la externalizarea în cloud a funcțiilor sau activităților operaționale critice sau importante;

f. în ceea ce privește fiecare acord de externalizare în cloud care acoperă funcții sau activități operaționale critice sau importante, cerințele privind „strategia de încetare a acordului" documentată și, dacă este cazul, suficient testată, care să fie proporțională cu natura, amploarea și complexitatea riscurilor inerente serviciilor furnizate. Strategia de încetare a acordului poate implica o serie de procese de denunțare, inclusiv (dar nu neapărat limitat la), întreruperea, reintegrarea sau transferul serviciilor incluse în acordul de externalizare în cloud.

Recomandarea 4 – Notificarea scrisă adresată autorității de supraveghere

21. Cerințele de notificare scrisă stabilite la articolul 49 alineatul (3) din Directiva Solvabilitate II și detaliate de Ghidul EIOPA privind sistemul de guvernanță sunt aplicabile tuturor acțiunilor de externalizare a funcțiilor și activităților operaționale critice sau importante către furnizorii de servicii cloud. În cazul în care o funcție sau o activitate operațională externalizată, clasificată anterior drept necritică sau neimportantă, devine critică sau importantă, societatea ar trebui să notifice autoritatea de supraveghere.

22. Notificarea scrisă a societății ar trebui să includă, ținând cont de principiul proporționalității, cel puțin următoarele informații:

a. o scurtă descriere a funcției sau a activității operaționale externalizate;

b. data de începere și, după caz, următoarea dată de reînnoire a contractului, data de încetare și/sau perioadele de preaviz pentru furnizorul de servicii cloud și pentru societate;

c. legea aplicabilă acordului de externalizare în cloud;

d. denumirea furnizorului de servicii cloud, numărul de înregistrare al societății, identificatorul persoanei juridice (dacă este disponibil), adresa înregistrată și alte date de contact relevante, precum și denumirea societății-mamă (dacă există); în cazul grupurilor, dacă furnizorul de servicii cloud face parte sau nu din grup;

e. serviciile cloud și modelele de implementare (adică, publice/private/hibride/comunitare, precum și natura specifică a datelor care

urmează să fie deținute și locațiile (și anume, țări sau regiuni) unde sunt stocate datele respective;

f. un scurt rezumat al motivelor pentru care funcția sau activitatea operațională externalizată este considerată critică sau importantă;

g. data celei mai recente evaluări a caracterului critic sau a importanței funcției sau activității operaționale externalizate.

Recomandarea 5 – Cerințe privind documentarea

23. În cadrul sistemului de guvernanță și de management al riscului, societatea ar trebui să țină evidența acordurilor de externalizare în cloud, de exemplu, sub forma unui registru dedicat, actualizat în timp. De asemenea, societatea ar trebui să mențină, pentru o perioadă adecvată, sub rezerva reglementării naționale, o evidență a acordurilor denunțate de externalizare în cloud.

24. În cazul externalizării funcțiilor sau activităților operaționale critice sau importante, societatea ar trebui să înregistreze toate informațiile următoare:

a. informațiile care sunt notificate autorității de supraveghere, menționate în Recomandarea 4;

b. în cazul grupurilor, societățile de asigurare sau de reasigurare și alte entități care intră în sfera de aplicare a consolidării prudențiale și care utilizează servicii cloud;

c. data celei mai recente evaluări a riscurilor și un rezumat succint al principalelor rezultate;

d. persoana fizică sau organul de decizie (de exemplu, AMSB) din societate care a aprobat acordul de externalizare în cloud;

e. data celui mai recent audit și data următoarelor audituri programate, dacă este cazul;

f. denumirea subcontractanților cărora le sunt externalizate părți semnificative ale unei funcții sau activități operaționale critice sau importante, inclusiv țara în care sunt înregistrați subcontractanții, în care se prestează serviciul și, dacă este cazul, locațiile (și anume, țările sau regiunile) în care sunt stocate datele;

g. rezultatul evaluării capacității de substituire a furnizorului de servicii cloud (de exemplu, ușor, dificil sau imposibil de substituit);

h. dacă pe funcția sau activitatea operațională critică sau importantă externalizată se bazează operațiuni care sunt necesare în momente critice;

i. cheltuieli bugetare anuale estimate;

j. dacă societatea dispune de o strategie de încetare a acordului în caz de denunțare de către oricare dintre părți sau de întrerupere a serviciilor de către furnizorul de servicii cloud;

25. În cazul externalizării funcțiilor sau activităților operaționale necritice sau neimportante, societatea ar trebui să definească informațiile care trebuie înregistrate în funcție de natura, amploarea și complexitatea riscurilor inerente serviciilor oferite de furnizorul de servicii cloud.

26. Societatea ar trebui să pună la dispoziția autorității de supraveghere, la cerere, toate informațiile necesare care-i permit acesteia din urmă să efectueze supravegherea societății, inclusiv o copie a acordului de externalizare.

Recomandarea 6 – Evaluarea prealabilă externalizării

27. Înainte de a încheia acordurile cu furnizorii de servicii cloud, societatea ar trebui:

a. să evalueze dacă acordurile de externalizare în cloud se referă la o funcție sau activitate operațională critică sau importantă în conformitate cu Recomandarea 7;

b. să identifice și să evalueze toate riscurile relevante asociate acordurilor de externalizare în cloud, în conformitate cu Recomandarea 8;

c. să efectueze analiza complexă corespunzătoare cu privire la furnizorul de servicii cloud potențial, în conformitate cu Recomandarea 9;

d. să identifice și să evalueze conflictele de interese pe care le poate cauza externalizarea, în conformitate cu cerințele prevăzute la articolul 274 alineatul (3) litera (b) din Regulamentul delegat.

Recomandarea 7 – Evaluarea funcțiilor și activităților operaționale critice sau importante

28. Înainte de a încheia un acord de externalizare cu furnizorii de servicii cloud, societatea ar trebui să evalueze dacă acordul de externalizare în cloud se referă la o funcție sau activitate operațională care este critică sau importantă. La efectuarea acestei evaluări, atunci când este cazul, societatea ar trebui să aibă în vedere dacă acordul are potențialul de a deveni critic sau important în viitor. De asemenea, societatea ar trebui să reevalueze și caracterul critic sau importanța funcției sau a activității operaționale externalizate anterior către furnizorii de servicii cloud, în cazul în care natura, amploarea și complexitatea riscurilor inerente acordului se modifică semnificativ.

29. În cadrul evaluării, societatea ar trebui să țină cont, în paralel cu rezultatul evaluării riscurilor, cel puțin de următorii factori:

a. impactul potențial al perturbărilor semnificative ale funcției sau activității operaționale externalizate sau al nefurnizării serviciilor de către furnizorul de servicii cloud la nivelurile de calitate a serviciilor convenite, asupra:

   i. respectării permanente a obligațiilor prevăzute de reglementări;

   ii. rezilienței și viabilității din punct de vedere financiar și al solvabilității, pe termen scurt și lung;

   iii. continuității activității și a rezilienței operaționale;

   iv. riscului operațional, inclusiv riscul juridic, riscul TIC și riscul de conduită;

   v. riscului reputațional.

b. impactul potențial al acordului de externalizare în cloud asupra capacității societății de a:

   i. identifica, monitoriza și gestiona toate riscurile relevante;

   ii. respecta toate cerințele juridice și de reglementare;

   iii. efectua audituri adecvate asupra funcției sau activității operaționale externalizate.

c. expunerea agregată a societății (și/sau a grupului, după caz) față de același furnizor de servicii cloud și potențialul impact cumulativ al acordurilor de externalizare pentru același domeniu de activitate;

d. dimensiunea și complexitatea fiecărui tip de activitate al societății, afectate de acordul de externalizare în cloud;

e. posibilitatea, dacă este necesar sau de dorit, de a transfera acordul de externalizare propus către alt furnizor de servicii cloud sau de a reintegra serviciile („capacitatea de substituire”);

f. protecția datelor cu caracter personal și nepersonal și impactul potențial asupra societății, deținătorilor de polițe sau altor subiecți relevanți al unei încălcări a obligației de confidențialitate sau al incapacității de a asigura disponibilitatea și integritatea datelor pe baza, printre altele, a Regulamentului (UE) 2016/679[7]. Societatea ar trebui să țină seama, în special, de datele comerciale care sunt secrete și/sau sensibile (de exemplu, datele medicale ale deținătorilor de polițe).

Recomandarea 8 – Evaluarea riscurilor asociate externalizării în cloud

30. În general, societatea ar trebui să adopte o abordare proporțională cu natura, amploarea și complexitatea riscurilor inerente serviciilor externalizate către furnizorii de servicii cloud. Aceasta include evaluarea impactului potențial al fiecărei externalizări în cloud, în special, asupra riscurilor operațional și reputațional.

31. În cazul externalizării unor funcții sau activități operaționale critice sau importante către furnizorii de servicii cloud, societatea ar trebui:

a. să țină seama de beneficiile și costurile preconizate ale acordului de externalizare în cloud propus, inclusiv compararea riscurilor semnificative care pot fi reduse sau cărora li se poate aplica un management mai eficientcu riscurile semnificative care pot apărea ca urmare a acordului de externalizare în cloud propus;

b. să evalueze, după caz și necesități, riscurile, inclusiv riscurile juridic, TIC, de neconformitate și reputațional, precum și limitările capacității de control care decurg din:

   i. serviciul cloud selectat și modelele de implementare propuse (adică public/privat/hibrid/comunitar);

   ii. migrarea și/sau implementarea;

   iii. datele și sistemele aferente activităților avute în vedere pentru a fi externalizate (sau care au fost externalizate), senzitivitatea acestora și măsurile de securitate necesare;

   iv. stabilitatea politică și situația de securitate a țărilor (din UE sau din afara UE) din care sunt sau pot fi furnizate serviciile externalizate și în care datele sunt sau ar putea fi stocate. Evaluarea ar trebui să ia în considerare:

      1. legislația în vigoare, inclusiv legislația privind protecția datelor;

      2. dispozițiile de aplicare a legii în vigoare;

      3. dispozițiile din legislația privind insolvența care s-ar aplica în cazul incapacității unui furnizor de servicii și impedimentele

[7] 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).

care ar putea apărea în caz de recuperare urgentă a datelor societății;

v. riscurile asociate externalizării în lanț, inclusiv riscurile suplimentare care pot apărea în cazul în care subcontractantul este situat într-o țară terță sau într-o altă țară decât furnizorul de servicii cloud și riscul ca lanțurile lungi și complexe de externalizare să diminueze capacitatea societății de a avea control asupra funcțiilor sau activităților operaționale critice sau importante și capacitatea autorităților de supraveghere de a le supraveghea în mod eficace;

vi. riscul de concentrare global al societății din expunerea la același furnizor de servicii cloud, inclusiv externalizarea către un furnizor de servicii cloud care nu este ușor de substituit sau existența mai multor acorduri de externalizare cu același furnizor de servicii cloud. Atunci când evaluează riscul de concentrare, societatea (și/sau grupul, dacă este cazul) ar trebui să țină seama de toate acordurile de externalizare în cloud cu respectivul furnizor de servicii cloud.

32. Evaluarea riscurilor ar trebui efectuată înainte de a încheia un acord de externalizare în cloud. Dacă societatea ia cunoștință de deficiențe semnificative și/sau modificări semnificative ale serviciilor furnizate sau ale situației furnizorului de servicii cloud, evaluarea riscurilor ar trebui imediat analizată sau efectuată din nou. În cazul reînnoirii unui acord de externalizare în cloud în ceea ce privește conținutul și sfera de aplicare a acestuia (de exemplu, extinderea domeniului de aplicare sau includerea unor funcții operaționale critice sau importante care nu erau incluse anterior), evaluarea riscurilor ar trebui efectuată din nou.

Recomandarea 9 – Evaluarea complexă a furnizorului de servicii cloud

33. În procesul de selecție și evaluare, societatea ar trebui să se asigure că furnizorul de servicii cloud corespunde criteriilor definite prin politica de externalizare scrisă.

34. Evaluarea complexă a furnizorului de servicii cloud ar trebui efectuată înainte de externalizarea funcțiilor sau activităților operaționale. În cazul în care societatea încheie un al doilea acord cu un furnizor de servicii cloud care a fost deja evaluat, societatea ar trebui să stabilească, pe baza unei abordări bazate pe riscuri, dacă este necesară o nouă evaluare complexă. Dacă societatea ia cunoștință de deficiențe semnificative și/sau modificări semnificative ale serviciilor furnizate sau ale situației furnizorului de servicii cloud, evaluarea complexă ar trebui imediat analizată sau efectuată din nou.

35. În cazul externalizăriiîn cloud a funcțiilor operaționale critice sau importante, evaluarea complexă ar trebui să includă o evaluare a adecvării furnizorului de servicii cloud (de exemplu, competențe, infrastructură, situație economică, statut corporativ și din punct de vedere al reglementărilor). Dacă este cazul, societatea poate folosi, pentru a susține dovada că s-a efectuat evaluarea complexă, certificări bazate pe standardele internaționale, rapoarte de audit ale unor terți recunoscuți sau rapoarte de audit intern.

Recomandarea 10 – Cerințe contractuale

36. Drepturile și obligațiile care le revin societății și furnizorului de servicii cloud ar trebui să fie clar atribuite și definite printr-un acord scris.

37. Fără a aduce atingere cerințelor menționate la articolul 274 din Regulamentul delegat, în cazul externalizării unor funcții sau activități operaționale critice sau

importante către un furnizor de servicii cloud, acordul scris dintre societate și furnizorul de servicii cloud ar trebui să prevadă:

a. o descriere clară a funcției externalizate care urmează să fie furnizată (servicii cloud, inclusiv tipul serviciilor de asistență);

b. data de începere și data de încetare a acordului, după caz, și perioadele de preaviz pentru furnizorul de servicii cloud și pentru societate;

c. jurisdicția instanței și legea aplicabilă acordului;

d. obligațiile financiare ale părților;

e. dacă este permisă externalizarea în lanț a unei funcții sau activități operaționale critice sau importante (sau a unor părți semnificative din aceasta) și, în caz afirmativ, condițiile la care este supusă externalizarea în lanț semnificativă (vezi Recomandarea 13);

f. locația (locațiile) (și anume, regiunile sau țările) unde sunt stocate și prelucrate date relevante (locația centrelor de date), condițiile care trebuie îndeplinite, inclusiv cerința de a notifica societatea în cazul în care furnizorul de servicii propune schimbarea locației (locațiilor);

g. prevederi referitoare la accesibilitatea, disponibilitatea, integritatea, confidențialitatea, caracterul privat și siguranța datelor relevante, ținând cont de specificațiile din Recomandarea 12;

h. dreptul societății de a monitoriza în mod regulat activitatea furnizorului de servicii cloud;

i. nivelurile convenite de calitate a serviciilor, care ar trebui să includă obiective de performanță cantitative și calitative precise, pentru a permite o monitorizare în timp util, astfel încât, dacă nu sunt respectate nivelurile convenite de calitate a serviciilor, să se poată lua măsuri corective adecvate, fără întârzieri nejustificate;

j. obligațiile de raportare ale furnizorului de servicii cloud către societate, inclusiv, după caz, obligațiile de a transmite rapoarte relevante pentru funcția de securitate și funcțiile-cheie ale societății, precum rapoarte ale funcției de audit intern a furnizorului de servicii cloud;

k. dacă prestatorul de servicii cloud trebuie să încheie o asigurare obligatorie împotriva anumitor riscuri și, dacă este cazul, nivelul necesar al asigurării;

l. cerințele de punere în aplicare și de testare a planurilor de urgență pentru continuitatea activității;

m. cerința ca furnizorul de servicii cloud să acorde societății, autorităților de supraveghere și altor persoane desemnate de societate sau de autoritățile de supraveghere, următoarele:

    i. acces deplin la toate sediile operaționale relevante (sedii centrale și centre operaționale), inclusiv la întreaga gamă de dispozitive, sisteme, rețele, informații și date relevante utilizate pentru furnizarea funcției externalizate și la informații asociate acestora, de natură financiară, despre personal și despre auditorii externi ai furnizorului de servicii cloud („drepturi de acces”);

    ii. drepturi nelimitate de control și de audit legate de acordul de externalizare („drepturi de audit”), pentru a le permite să monitorizeze acordul de externalizare și pentru a asigura respectarea tuturor cerințelor contractuale și de reglementare aplicabile;

n. clauze prin care se garantează faptul că datele care aparțin societății pot fi recuperate rapid de aceasta în cazul insolvenței, al rezoluției sau al întreruperii operațiunilor realizate de furnizorul de servicii cloud.

Recomandarea 11 – Drepturi de acces și de audit

38. Pentru a se respecta obligațiile prevăzute de reglementări, acordul de externalizare a serviciilor cloud nu ar trebui să limiteze posibilitatea ca societatea să exercite efectiv drepturile de acces, drepturile de audit și opțiunile de control asupra serviciilor cloud.

39. Societatea ar trebui să-și exercite drepturile de acces și de audit, să stabilească frecvența misiunilor de audit, precum și domeniile și serviciile care urmează să fie auditate, adoptând o abordare bazată pe riscuri în conformitate cu secțiunea 8 din Ghidul EIOPA privind sistemul de guvernanță.

40. La stabilirea frecvenței și sferei de exercitare a drepturilor de acces sau de audit, societatea ar trebui să aibă în vedere dacă externalizarea în cloud este asociată sau nu unei funcții sau activități operaționale critice sau importante și să țină seama de natura și amploarea riscului și a impactului acordurilor de externalizare în cloud asupra societății.

41. Dacă exercitarea drepturilor de acces, a drepturilor de audit sau utilizarea anumitor tehnici de audit creează un risc pentru mediul de afaceri al furnizorului de servicii cloud și/sau pentru un alt client al furnizorului de servicii cloud (de exemplu, impactul asupra nivelului calității serviciilor, disponibilității datelor, aspectelor de confidențialitate), societatea și furnizorul de servicii cloud ar trebui să convină asupra unor modalități alternative de a oferi societății un nivel similar de asigurare și de calitate a serviciilor [de exemplu, includerea unor mecanisme de control specifice care să fie testate într-un raport specific/certificare specifică elaborat(ă) de furnizorul de servicii cloud].

42. Fără a aduce atingere responsabilității finale a societăților cu privire la activitățile desfășurate de furnizorii de servicii cloud, pentru a utiliza mai eficient resursele de audit și pentru a reduce dificultățile de ordin organizatoric pentru furnizorul de servicii cloud și pentru clienții săi, acestea pot utiliza:

a. certificări de la terți și rapoarte de audit intern sau efectuate de terți, puse la dispoziție de furnizorul de servicii cloud;

b. audituri centralizate (adică organizate în comun cu alți clienți ai aceluiași furnizor de servicii cloud) sau audituri centralizate efectuate de un terț numit de aceștia.

43. În cazul externalizării în cloud a unor funcții sau activități operaționale critice sau importante, societățile ar trebui să utilizeze metoda menționată la punctul 42 litera (a) numai dacă acestea:

a. se asigură că obiectul certificării sau al raportului de audit acoperă sistemele (de exemplu, procesele, aplicațiile, infrastructura, centrele de date etc.) și mecanismele de control identificate și evaluează respectarea cerințelor de reglementare relevante;

b. evaluează temeinic și periodic conținutul noilor certificări sau rapoarte de audit și verifică să nu fie caduce rapoartele sau certificările;

c. se asigură că sistemele-cheie și mecanimele de control principale sunt incluse în viitoarele versiuni ale certificării sau ale raportului de audit;

d. sunt mulțumite de calitățile părții care realizează certificarea sau auditul (de exemplu, cu privire la rotația entității de certificare sau de audit, calificările, expertiza, reefectuarea/verificarea dovezilor din dosarul de audit analizat);

e. sunt mulțumite că certificările sunt emise și auditurile sunt efectuate conform unor standarde corespunzătoare și că includ un test de eficacitate operațională a mecanismelor de control importante implementate;

f. au dreptul contractual de a solicita extinderea domeniului de aplicare al certificărilor sau al rapoartelor de audit la alte sisteme și mecanisme de control relevante; numărul și frecvența acestor cereri de modificare a domeniului de aplicare ar trebui să fie rezonabile și legitime din perspectiva managementului riscului;

g. păstrează dreptul contractual de a efectua audituri individuale la sediul furnizorului, la aprecierea proprie, în ceea ce privește externalizarea în cloud a funcțiilor sau activităților operaționale critice sau importante; acest drept ar trebui să fie exercitat în funcție de necesitățile specifice și în cazul în care nu este posibil prin intermediul altor tipuri de interacțiuni cu furnizorul de servicii cloud.

44. Pentru externalizarea unor funcții operaționale critice sau importante către furnizori de servicii cloud, societatea ar trebui să evalueze dacă certificările și rapoartele terților menționate la punctul 42 litera (a) sunt adecvate și suficiente pentru a respecta obligațiile prevăzute de reglementări și, aplicând o abordare bazată pe riscuri, nu ar trebui să se bazeze exclusiv pe aceste rapoarte și certificări de-a lungul timpului.

45. Înainte de un control la sediu planificat, partea care exercită dreptul de acces (societatea, auditorul sau terții care acționează în numele societății) ar trebui să transmită un aviz într-o perioadă de timp rezonabilă, dacă nu este posibil să transmită o notificare prealabilă din cauza unei situații de urgență sau de criză. Avizul ar trebui să includă locația, scopul controlului și personalul care va efectua controlul.

46. Având în vedere că soluțiile de tip cloud au un nivel ridicat de complexitate tehnică, societatea ar trebui să verifice dacă personalul care efectuează auditul – care poate consta din auditorii săi interni, din grupul de auditori care acționează în numele său sau din auditorii desemnați ai furnizorului de servicii cloud – sau, după caz, personalul care revizuiește certificarea realizată de o terță parte sau rapoartele de audit ale furnizorului de servicii are aptitudinile și cunoștințele adecvate pentru a efectua audituri și/sau evaluări relevante.

Recomandarea 12 – Securitatea datelor și a sistemelor

47. Societatea ar trebui să se asigure că furnizorii de servicii cloud respectă reglementările europene și naționale, precum și standardele corespunzătoare de securitate TIC.

48. În cazul externalizării unor funcții sau activități operaționale critice sau importante către furnizori de servicii cloud, în plus, societatea ar trebui să prevadă în acordul de externalizare cerințe specifice de securitate a informațiilor și să monitorizeze periodic respectarea acestor cerințe.

49. În sensul punctului 48, în cazul externalizării unor funcții sau activități operaționale critice sau importante către furnizori de servicii cloud, societatea, aplicând o abordare bazată pe riscuri și ținând cont de responsabilitățile sale și de cele ale furnizorului de servicii cloud, ar trebui:

a. să convină asupra rolurilor și responsabilităților clare între furnizorul de servicii cloud și societate în legătură cu funcțiile sau activitățile operaționale afectate de externalizarea în cloud, care ar trebui să fie clar repartizate;

b. să stabilească și să decidă asupra nivelului adecvat de protecție a datelor confidențiale, asupra continuității activităților externalizate și asupra integrității și trasabilității datelor și sistemelor în contextul externalizării în cloud vizate;

c. să ia în considerare măsuri specifice atunci când este necesar pentru datele aflate în tranzit, datele din memorie și datele în repaus, cum ar fi utilizarea tehnologiilor de criptare în combinație cu o arhitectură de management adecvat al cheilor;

d. să ia în considerare mecanismele de integrare a serviciilor cloud în sistemele proprii, de exemplu, interfețele de programare a aplicațiilor și un proces adecvat de management al accesului și utilizatorilor;

e. să se asigure contractual că disponibilitatea traficului de rețea și capacitatea preconizată îndeplinesc cerințe stricte în ceea ce privește continuitatea, dacă sunt aplicabile și fezabile;

f. să definească și să introducă cerințe corespunzătoare în ceea ce privește continuitatea, asigurând niveluri adecvate de calitate la fiecare nivel al lanțului tehnologic, dacă este cazul;

g. să asigure un proces adecvat și bine documentat de management al incidentelor, cu responsabilitățile aferente, de exemplu, prin elaborarea unui model de cooperare în caz de incidente reale sau preconizate;

h. să adopte o abordare bazată pe riscuri privind locația (locațiile) de stocare și de prelucrare a datelor (adică țara sau regiunea), incluzând considerații privind securitatea informațiilor;

i. să monitorizeze respectarea cerințelor referitoare la aplicarea efectivă și eficientă a mecanismelor de control implementate de furnizorul de servicii cloud care ar minimiza riscurile legate de serviciile furnizate.

Recomandarea 13 – Externalizarea în lanț a funcțiilor și activităților operaționale critice sau importante

50. Dacă este permisă externalizarea în lanț a funcțiilor operaționale critice sau importante (sau a unei părți din acestea), acordul de externalizare în cloud dintre societate și furnizorul de servicii cloud ar trebui:

a. să precizeze tipurile de activități care sunt excluse de la potențiala externalizare în lanț;

b. să indice condițiile care ar trebui respectate în cazul subcontractării în lanț (de exemplu, faptul că și subcontractantul va respecta pe deplin obligațiile relevante care revin furnizorului de servicii cloud). Aceste obligații includ drepturile de audit și de acces și securitatea datelor și a sistemelor;

c. să indice faptul că furnizorul de servicii cloud păstrează responsabilitatea deplină și asigură un control complet asupra serviciilor externalizate în lanț;

d. să includă pentru furnizorul de servicii cloud obligația de a informa societatea despre modificările semnificative planificate la nivel de subcontractanți sau de servicii externalizate în lanț care ar putea afecta capacitatea furnizorului de servicii de a-și îndeplini obligațiile asumate prin acordul de externalizare în cloud. Perioada de notificare a acestor modificări ar trebui să permită societății, cel puțin, să efectueze o evaluare a riscurilor în ceea ce privește efectele

modificărilor propuse înainte ca modificarea efectivă a subcontractanților și a serviciilor subcontractate să intre în vigoare;

e. să se asigure, în cazurile în care un furnizor de servicii cloud intenționează schimbe subcontractantul sau serviciile externalizatesubcontractate, ceea ce ar avea un efect negativ asupra evaluării riscurilor serviciilor convenite, că are dreptul să se opună acestor modificări și/sau dreptul de a rezilia sau denunța contractul.

Recomandarea 14 – Monitorizarea acordurilor de externalizare în cloud și controlul asupra acestora

51. Societatea ar trebui să monitorizeze periodic desfășurarea activităților, măsurile de securitate și respectarea nivelului convenit al calității serviciilor de către furnizorii de servicii cloud, printr-o abordare bazată pe riscuri. Atenția principală ar trebui concentrată pe externalizarea în cloud a funcțiilor operaționale critice și importante.

52. Pentru a realiza acest lucru, societatea ar trebui să instituie mecanisme de monitorizare și de control care ar trebui să țină seama, dacă este posibil și adecvat, de externalizarea în lanț a unor funcții operaționale critice sau importante sau a unei părți din acestea.

53. AMSB ar trebui informat periodic în ceea ce privește riscurile identificate asociate externalizării în cloud a funcțiilor sau activităților operaționale critice sau importante.

54. Pentru a asigura monitorizarea adecvată și un control adecvat asupra acordurilor de externalizare în cloud, societățile ar trebui să utilizeze suficiente resurse cu abilități și cunoștințe adecvate pentru a putea monitoriza serviciile externalizate în cloud. Personalul societății care se ocupă de aceste activități ar trebui să aibă cunoștințele necesare atât din domeniul TIC, cât și despre domeniul de afaceri.

Recomandarea 15 – Drepturi de reziliere și strategii de încetare a acordului

55. În cazul externalizării în cloud a unor funcții sau activități operaționale critice sau importante, în cadrul acordului de externalizare în cloud ar trebui să se prevadă o clauză clar definită privind strategia de încetare a acordului, prin care să asigure faptul că societatea are capacitatea să denunțe acordul, dacă este necesar. Denunțarea ar trebui să fie posibilă fără a aduce atingere continuității și calității furnizării serviciilor către deținătorii de polițe. În acest scop, societatea ar trebui:

a. să elaboreze planuri de încetare a acordului care să fie cuprinzătoare, în funcție de servicii, documentate și testate suficient (de exemplu, realizând o analiză a costurilor potențiale, a impactului, a resurselor și a implicațiilor în timp ale diverselor opțiuni potențiale de încetare a acordului);

b. să identifice soluții alternative și să elaboreze planuri de tranziție adecvate și fezabile pentru a permite societății să elimine și să transfere activitățile și datele existente de la furnizorul de servicii cloud către alți furnizorii de servicii sau înapoi la societate. Aceste soluții ar trebui definite în raport cu problemele care pot apărea din cauza locației datelor, luând măsurile necesare pentru a asigura continuitatea activității în faza de tranziție;

c. să se asigure că furnizorul de servicii cloud acordă asistență adecvată societății atunci când transferă datele, sistemele sau aplicațiile externalizate către un alt furnizor de servicii sau direct către societate;

d. să convină cu furnizorul de servicii cloud că, odată retransferate către societate, datele vor fi șterse complet și în siguranță de către furnizorul de servicii cloud, în toate regiunile.

56. La elaborarea strategiilor de încetare a acordului, societatea ar trebui să ia în considerare următoarele:

a. să stabilească obiectivele strategiei de încetare a acordului;

b. să stabilească evenimentele declanșatoare (de exemplu, indicatori-cheie de risc care raportează un nivel inacceptabil de calitate a serviciilor) care ar putea activa strategia de încetare a acordului;

c. să efectueze o analiză a impactului economic proporțională cu activitățile externalizate pentru a identifica ce resurse umane și de altă natură ar fi necesare pentru a implementa planul de încetare a acordurilor și de cât timp ar fi nevoie;

d. să aloce roluri și responsabilități pentru managementul planurilor de încetare a acordului și a activităților de tranziție;

e. să stabilească criteriile care asigură o tranziție eficientă.

Recomandarea 16 – Supravegherea acordurilor de externalizare în cloud de către autoritățile de supraveghere

57. Autoritățile de supraveghere ar trebui să efectueze analiza impactului acordurilor de externalizare în cloud ale societăților în cadrul procesului de supraveghere. Analiza impactului ar trebui să se concentreze, în special, asupra acordurilor de externalizare a funcțiilor sau activităților operaționale critice sau importante.

58. Autoritățile de supraveghere ar trebui să ia în considerare următoarele riscuri la supravegherea acordurilor de externalizare în cloud ale societăților:

a. riscurile TIC;

b. alte riscuri operaționale (inclusiv riscul juridic, riscul de neconformitate, riscul de externalizare și riscul de management al relației cu terții);

c. riscul reputațional;

d. riscul de concentrare, inclusiv la nivel de țară/sectorial.

59. În evaluarea realizată, autoritățile de supraveghere ar trebui să includă următoarele aspecte, aplicând o abordare bazată pe riscuri:

a. adecvarea și eficiența proceselor operaționale și de guvernanță ale societății legate de aprobarea, implementarea, monitorizarea, managementul și reînnoirea acordurilor de externalizare în cloud;

b. dacă societatea are sau nu resurse suficiente cu competențe și cunoștințe adecvate pentru a monitoriza serviciile externalizate în cloud;

c. dacă societatea identifică și asigură managementul tutror riscurilor evidențiate în prezentul ghid.

60. În cazul grupurilor, supraveghetorul grupului ar trebui să se asigure că impactul externalizării în cloud a funcțiilor sau activităților operaționale critice sau importante sunt reflectate în evaluarea pentru supraveghere a riscurilor la nivel de grup, ținând cont de cerințele enumerate la punctele 58 și59 și de caracteristicile individuale operaționale și de guvernanță ale grupului.

61. Dacă externalizarea în cloud a funcțiilor sau activităților operaționale critice sau importante implică mai multe societăți din diferite state membre și managementul acesteia este asigurat centralizat de societatea-mamă sau de o filială a grupului (de exemplu, o societate sau o societate de servicii de grup, cum ar fi furnizorul TIC de grup), autoritatea de supraveghere a grupului și/sau autoritățile de supraveghere relevante ale societăților implicate în externalizarea serviciilor cloud ar trebui să discute în cadrul colegiului de supraveghetori, după caz, impactul externalizării în cloud asupra profilului de risc al grupului.

62. În cazul în care se identifică aspecte care conduc la concluzia că societatea nu mai are instituite mecanisme adecvate de guvernanță sau nu mai respectă cerințele de reglementare, autoritățile de supraveghere ar trebui să ia măsuri corespunzătoare, care pot cuprinde, de exemplu, obligarea societății de a-și îmbunătăți sistemul de guvernanță, limitarea sau restrângerea numărului funcțiilor externalizate sau impunerea încetării unuia sau mai multor acorduri de externalizare. În special, ținând cont de necesitatea asigurării continuității funcționării societății, anularea contractelor ar putea fi prevăzută dacă supravegherea și impunerea cerințelor de reglementare nu pot fi asigurate prin alte măsuri.

Reguli de conformitate și raportare

63. Prezentul document cuprinde recomandări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1094/2010. În conformitate cu articolul 16 alineatul (3) din același regulament, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile pentru a respecta recomandările din prezentul ghid.

64. Autoritățile competente care respectă sau intenționează să respecte prezentul ghid ar trebui să îl includă în mod corespunzător în cadrul de reglementare sau de supraveghere.

65. Autoritățile competente trebuie să transmită la EIOPA confirmarea respectării sau a intenției de a respecta prezentul ghid, prezentând motivele în cazul neconformității, în termen de două luni de la publicarea versiunilor traduse.

66. În lipsa unui răspuns până la împlinirea acestui termen, se va considera că autoritățile competente nu respectă cerințele de raportare și vor fi raportate ca atare.

Prevedere finală cu privire la revizuire

67. Prezentul Ghid va fi supus unei revizuiri de către EIOPA.