

Autoritatea de Supraveghere Financiară - ASF - Normă nr. 33/2020 din 12 august 2020

Norma nr. 33/2020 privind externalizarea către furnizorii de servicii de tip cloud

În vigoare de la 18 august 2020

*Publicat în Monitorul Oficial, Partea I nr. 749 din 18 august 2020. Formă aplicabilă la **20 decembrie 2023**.*

În conformitate cu prevederile art. 2 alin. (1) lit. b), art. 3 alin. (1) lit. b) și art. 6 alin. (2) din Ordonanța de urgență a Guvernului nr. 93/2012 privind înființarea, organizarea și funcționarea Autorității de Supraveghere Financiară, aprobată cu modificări și completări prin Legea nr. 113/2013, cu modificările și completările ulterioare,

în temeiul prevederilor art. 33, art. 173 alin. (1) lit. t) și art. 179 alin. (4) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, cu modificările și completările ulterioare,

în baza prevederilor art. 274 din 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), cu modificările și completările ulterioare,

având în vedere Ghidul EIOPA BoS-20-002 privind externalizarea către furnizorii de servicii de tip cloud,

în urma deliberărilor Consiliului Autorității de Supraveghere Financiară din cadrul ședinței din data de 12 august 2020,

Autoritatea de Supraveghere Financiară emite următoarea normă:

ARTICOLUL 1

Prevederi generale și domeniul de aplicare

- (1)** Prezenta normă reglementează modul în care societățile aplică cerințele referitoare la externalizare prevăzute în Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, cu modificările și completările ulterioare, denumită în continuare Legea nr. 237/2015, și în 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), cu modificările și completările ulterioare, denumit în continuare Regulamentul delegat nr. 35/2015, în contextul externalizării către furnizorii de servicii de tip cloud.

(2) Externalizarea funcțiilor sau activităților operaționale către alți furnizori de servicii care se bazează în mod semnificativ pe infrastructuri de tip cloud intră în sfera de aplicare a prezentei norme.

ARTICOLUL 2

Definiții

Termenii, expresiile și acronimele utilizate în prezenta normă au semnificațiile prevăzute în Legea nr. 237/2015, alte reglementări din domeniul asigurărilor, prevederile legale în vigoare, precum și următoarele semnificații:

1. furnizor de servicii - o entitate terță care realizează un proces, serviciu sau o activitate sau părți din acestea, în baza unui acord de externalizare;
2. furnizor de servicii de tip cloud - furnizor de servicii responsabil de furnizarea serviciilor de tip cloud în cadrul unui acord de externalizare;
3. servicii de tip cloud - servicii furnizate cu ajutorul tehnologiilor de calcul de tip cloud pentru permiterea accesului universal, convenabil, la cerere în rețea la un grup comun de resurse de calcul configurabile, care poate fi rapid pus la dispoziție și lansat cu un efort minim de gestionare sau interacțiune cu furnizorul de servicii;
4. cloud public - infrastructură informatică disponibilă pentru utilizarea liberă de către publicul larg;
5. cloud privat - infrastructură informatică disponibilă pentru utilizare exclusiv de către o singură societate;
6. cloud comunitar - infrastructură informatică disponibilă pentru utilizare exclusiv de către o anumită comunitate de entități din cadrul aceluiași grup;
7. cloud hibrid - infrastructură informatică compusă din două sau mai multe infrastructuri distincte de tip cloud;
8. TIC - tehnologia informației și comunicațiilor.

ARTICOLUL 3

Serviciile cloud și externalizarea

(1) Societățile evaluează dacă un acord cu un furnizor de servicii de tip cloud se încadrează în definiția externalizării prevăzută la art. 1 alin. (2) pct. 14 din Legea nr. 237/2015.

(2) La evaluarea prevăzută la alin. (1) societățile iau în considerare dacă funcția, activitatea operațională externalizată, inclusiv o parte a acesteia:

- a) este efectuată în mod repetat sau continuu;
- b) intră în sfera funcțiilor sau activităților operaționale care în mod normal sunt îndeplinite de societate, chiar dacă acestea nu au fost efectuate în trecut.

(3) În cazul în care acordul cu furnizorul de servicii de tip cloud acoperă mai multe funcții sau activități operaționale, societățile iau în considerare toate aspectele acordului în cadrul evaluării.

ARTICOLUL 4

Evaluarea prealabilă externalizării

Înainte de a încheia acordurile cu furnizorii de servicii de tip cloud, societatea:

1. evaluează dacă acordurile de externalizare în cloud se referă la o funcție sau activitate operațională critică sau semnificativă în conformitate cu [art. 6](#);
2. identifică și evaluează riscurile relevante asociate acordurilor de externalizare în cloud, în conformitate cu [art. 7](#);
3. efectuează o analiză complexă corespunzătoare cu privire la potențialul furnizor de servicii de tip cloud, în conformitate cu [art. 8](#);
4. identifică și evaluează conflictele de interese pe care le poate cauza externalizarea, în conformitate cu cerințele prevăzute la art. 274 alin. (3) [lit. b](#)) din Regulamentul delegat nr. 35/2015.

ARTICOLUL 5

Principii generale de guvernanză pentru externalizarea în cloud

- (1) Fără a aduce atingere [art. 274 alin. \(3\)](#) din Regulamentul delegat nr. 35/2015, conducerea se asigură că deciziile de a externaliza funcții sau activități operaționale critice sau semnificative către furnizorii de servicii de tip cloud se bazează pe o evaluare detaliată a riscurilor aferente acordului și a cel puțin următoarelor:
 - a) riscul TIC;
 - b) riscul privind continuitatea activității;
 - c) riscul juridic;
 - d) riscul de conformitate;
 - e) riscul de concentrare;
 - f) riscul operațional;
 - g) riscul asociat fazei de migrare a datelor și/sau fazei de implementare, după caz.
- (2) Societățile țin cont în cadrul ORSA de modificările din profilul de risc asociate acordurilor de externalizare în cloud a funcțiilor sau activităților operaționale critice sau semnificative către furnizorii de servicii de tip cloud.
- (3) Serviciile cloud se utilizează în concordanță cu politicile și procedurile interne ale societății, actualizate atunci când este necesar și ținând cont de cel puțin următoarele:
 - a) strategia TIC;
 - b) strategia de securitate a informațiilor;
 - c) strategia managementului riscului operațional.

ARTICOLUL 6

Evaluarea funcțiilor și activităților operaționale critice sau semnificative

- (1) La efectuarea evaluării menționate la [art. 8 alin. \(1\)](#) societatea analizează dacă acordul are potențialul de a deveni critic sau semnificativ în viitor; de asemenea societatea reevaluează și caracterul critic sau semnificativitatea funcției sau a activității operaționale externalizate anterior către furnizorii de servicii de tip cloud, în cazul în care natura, amploarea și complexitatea riscurilor inerente acordului se modifică semnificativ.
- (2) În cadrul evaluării societatea ține 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 de tip cloud la nivelurile de calitate a serviciilor convenite, asupra:

- (i)** respectării permanente a prevederilor legale;
- (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, riscului juridic, riscului TIC, riscului de conduită și 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 prevederile legale;
- (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 de tip 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) capacitatea de substituire având în vedere posibilitatea, dacă este necesar, de a transfera acordul de externalizare propus către alt furnizor de servicii de tip cloud sau de a reintegra serviciile;

f) protecția datelor comerciale care sunt secrete și/sau sensibile, protecția datelor cu caracter personal și nepersonal și impactul potențial asupra societății, contractanților sau altor subiecți relevanți al unei încălcări a obligației de confidențialitate sau al incapacității de a asigura disponibilitatea și integritatea datelor în conformitate cu prevederile Regulamentului (UE) [2016/679](#) al Parlamentului European și a 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).

ARTICOLUL 7

Evaluarea riscurilor asociate externalizării în cloud

(1) Societatea adoptă o abordare proporțională cu natura, amploarea și complexitatea riscurilor inerente serviciilor externalizate către furnizorii de servicii de tip cloud și include evaluarea impactului potențial al fiecărei externalizări în cloud, în special asupra riscurilor operațional și reputațional.

(2) În cazul externalizării unor funcții sau activități operaționale critice sau semnificative către furnizorii de servicii de tip cloud, societatea:

a) ține seama de beneficiile și costurile preconizate ale acordului de externalizare în cloud, inclusiv compararea riscurilor semnificative care pot fi reduse sau cărora li se poate aplica un management mai eficient cu riscurile semnificative care pot apărea ca urmare a acordului de externalizare în cloud;

b) evaluează, după caz, necesitățile, toate riscurile, precum și limitările capacității de control care decurg din:

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

(ii) migrarea și/sau implementarea;

(iii) datele și sistemele aferente activităților externalizate sau avute în vedere pentru a fi externalizate, sensibilitatea acestora și măsurile de securitate necesare;

(iv) stabilitatea politică și situația de securitate a statelor membre din Uniunea Europeană sau a statelor terțe din care sunt sau pot fi furnizate serviciile externalizate și în care datele sunt sau ar putea fi stocate;

(v) legislația în vigoare, inclusiv legislația privind protecția datelor;

(vi) dispozițiile de aplicare a legii în vigoare;

(vii) dispozițiile din legislația privind insolvența care s-ar aplica în cazul incapacității unui furnizor de servicii de tip cloud și impedimentele care ar putea apărea în caz de recuperare urgentă a datelor societății;

(viii) riscurile asociate externalizării în lanț, inclusiv:

1. riscurile suplimentare care pot apărea în cazul în care subcontractantul este situat într-un stat terț sau într-un alt stat decât furnizorul de servicii de tip cloud;

2. riscul ca lanțurile lungi și complexe de externalizare să diminueze capacitatea societăților de a avea control asupra funcțiilor sau activităților operaționale critice sau semnificative;

3. capacitatea Autorității de Supraveghere Financiară (A.S.F.) de supraveghere a acestora;

(ix) riscul de concentrare global al societății din expunerea la același furnizor de servicii de tip cloud, inclusiv:

1. externalizarea către un furnizor de servicii de tip cloud care nu este ușor de substituit;

2. existența mai multor acorduri de externalizare cu același furnizor de servicii de tip cloud.

(3) Atunci când societatea ia cunoștință de deficiențe și/sau modificări semnificative ale serviciilor furnizate sau ale situației furnizorului de servicii de tip cloud, aceasta analizează evaluarea riscurilor sau efectuează o nouă evaluare a riscurilor.

ARTICOLUL 8

Evaluarea complexă a furnizorului de servicii de tip cloud

(1) În efectuarea procesului de selecție și evaluare, societatea se asigură că furnizorul de servicii de tip cloud corespunde criteriilor definite prin politicile și procedurile interne de externalizare.

(2) Evaluarea complexă a furnizorului de servicii de tip cloud se efectuează înainte de externalizarea funcțiilor sau activităților operaționale.

(3) În cazul în care se încheie un al doilea acord cu un furnizor de servicii de tip cloud și care a fost deja evaluat, societatea stabilește, pe baza unei abordări bazate pe riscuri, dacă este necesară o nouă evaluare complexă.

(4) În cazul externalizării în cloud a funcțiilor operaționale critice sau semnificative, evaluarea complexă include o evaluare a adecvării furnizorului de servicii de tip cloud și are în vedere cel puțin următoarele:

- a)** competențe;
- b)** infrastructură;
- c)** situație economică;
- d)** statut corporativ;
- e)** reglementări.

(5) Pentru a putea face dovada de punere în aplicare a **alin. (4)** societatea poate folosi certificări bazate pe standardele internaționale, rapoarte de audit ale unor terți recunoscuți sau rapoarte de audit intern, precum și alte documente care pot să demonstreze efectuarea evaluării complexe.

ARTICOLUL 9

Documentarea

(1) În cadrul sistemului de guvernanță și al managementului riscului, societatea ține evidența acordurilor de externalizare în cloud, sub forma unui registru dedicat și actualizat; societatea menține, pentru o perioadă de doi ani, o evidență a acordurilor de externalizare în cloud încetate.

(2) În cazul externalizării funcțiilor sau activităților operaționale critice sau semnificative, societatea înregistrează următoarele:

- a)** informațiile notificate A.S.F. prevăzute la art. 10 **alin. (2)**;
- b)** în cazul grupurilor, societățile și alte entități care intră în sfera de aplicare a consolidării prudențiale și care utilizează servicii de tip cloud;
- c)** data celor mai recente evaluări a riscurilor și un rezumat succint al principalelor rezultate;
- d)** persoana sau organul din conducerea societății care a aprobat acordul de externalizare în cloud;
- e)** data celui mai recent audit și data următoarelor audituri programate;
- f)** denumirea subcontractanților cărora le sunt externalizate părți semnificative ale unei funcții sau activități operaționale critice sau semnificative, inclusiv statul în care sunt înregistrați subcontractanții, în care se prestează serviciul și locațiile, respectiv statele și regiunile în care sunt stocate datele;
- g)** rezultatul evaluării capacității de substituire a furnizorului de servicii de tip cloud care să indice ușurința, dificultatea sau imposibilitatea substituirii;
- h)** dacă în cadrul funcției sau activității operaționale critice sau semnificative externalizate există 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 de tip cloud.

(3) În cazul externalizării funcțiilor sau activităților operaționale necritice sau nesemnificative, societatea definește informațiile ce se înregistrează în funcție de natura, amploarea și complexitatea riscurilor inerente serviciilor oferite de furnizorul de servicii de tip cloud.

(4) La cerere, societatea pune la dispoziția A.S.F. toate informațiile necesare derulării procesului de supraveghere, inclusiv o copie a acordului de externalizare.

ARTICOLUL 10

Notificarea scrisă adresată A.S.F.

(1) Cerințele de notificare scrisă prevăzute la art. 33 alin. (3) din Legea nr. 237/2015 și detaliate de Norma Autorității de Supraveghere Financiară nr. 35/2015 privind cerințele calitative stabilite de către Autoritatea Europeană de Supraveghere pentru Asigurări și Pensii Ocupaționale, denumită în continuare Norma nr. 35/2015, se aplică tuturor acțiunilor de externalizare a funcțiilor și activităților operaționale critice sau semnificative către furnizorii de servicii de tip cloud; societatea notifică A.S.F. atunci când o funcție sau activitate operațională externalizată și clasificată anterior drept necritică sau nesemnificativă devine critică sau semnificativă.

(2) Notificarea scrisă include, ținând cont de principiul proporționalității, cel puțin următoarele informații:

- a) scurtă descriere a funcției sau 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 de tip cloud și pentru societate;
- c) legea aplicabilă acordului de externalizare în cloud;
- d) denumirea furnizorului de servicii de tip cloud, numărul de înregistrare, codul privind identificatorul persoanei juridice, dacă este disponibil, adresa înregistrată și alte date de contact relevante, precum și denumirea societății-mamă, dacă există, iar în cazul grupurilor, dacă furnizorul de servicii de tip cloud face parte sau nu din grup;
- e) serviciile de tip cloud și modelele publice/private/hibride/comunitare de implementare, precum și natura specifică a datelor ce urmează a fi deținute și locațiile unde sunt stocate datele respective;
- f) un scurt rezumat al motivelor pentru care funcția sau activitatea operațională externalizată este considerată critică sau semnificativă;
- g) data celei mai recente evaluări a caracterului critic sau a semnificativității funcției sau activității operaționale externalizate.

ARTICOLUL 11

Actualizarea politicii scrise de externalizare

În cazul externalizării către furnizorii de servicii de tip cloud, societățile actualizează atât politicile și procedurile aferente externalizării cât și politicile și procedurile relevante cum ar fi cele privind securitatea informațiilor, luând în considerare cel puțin următoarele:

- a) rolurile și responsabilitățile funcțiilor implicate din cadrul societăților, în special:
 - (i) conducerea;
 - (ii) funcția responsabilă de TIC;
 - (iii) funcția responsabilă de securitatea informațiilor;

- (iv) funcția de conformitate;
- (v) funcția de managementul riscului;
- (vi) funcția de 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 semnificative;
- 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 de tip cloud, inclusiv frecvența evaluării riscurilor;
 - (ii) mecanisme de monitorizare și de management;
 - (iii) standarde și mecanisme de securitate;
- d) cerințele contractuale prevăzute la [art. 12](#) în cazul externalizării în cloud a funcțiilor sau activităților operaționale critice sau semnificative;
- e) documentarea și notificarea scrisă către A.S.F. cu privire la externalizarea în cloud a funcțiilor sau activităților critice sau semnificative;
- f) strategia de încetare a acordului, în cazul funcțiilor sau activităților operaționale critice sau semnificative, documentată și, dacă este cazul, suficient testată care să fie proporțională cu natura, amploarea și complexitatea riscurilor inerente serviciilor furnizate;
- g) procesele de denunțare, inclusiv, dar fără a se limita la întreruperea, reintegrarea sau transferul serviciilor incluse în acordul de externalizarea în cloud.

ARTICOLUL 12

Cerințe contractuale

- (1) Drepturile și obligațiile ce le revin societății și furnizorului de servicii de tip cloud sunt stabilite prin acord scris.
- (2) Fără a aduce atingere [art. 274](#) din Regulamentul delegat nr. 35/2015, în cazul externalizării unor funcții sau activități operaționale critice sau semnificative către un furnizor de servicii de tip cloud, acordul scris dintre societate și furnizorul de servicii cloud cuprinde cel puțin următoarele:
 - a) o descriere clară a funcției externalizate care urmează să fie furnizată și tipul serviciilor de asistență;
 - b) data de începere și data de încetare a acordului, după caz;
 - c) perioadele de preaviz pentru furnizorul de servicii de tip cloud și pentru societate;
 - d) jurisdicția instanței și legea aplicabilă acordului;
 - e) obligațiile financiare ale celor două părți;
 - f) dacă este permisă externalizarea în lanț a unei funcții sau activități operaționale critice sau semnificative sau a unor părți semnificative din aceasta, inclusiv condițiile la care este supusă externalizarea în lanț semnificativă și cele ale [art. 15](#);

g) locația sau locațiile centrelor de date, cu precizarea regiunii, a statului sau a statelor unde sunt stocate și prelucrate date relevante, inclusiv:

(i) condițiile care trebuie îndeplinite;

(ii) cerința de a notifica societatea în cazul în care furnizorul de servicii propune schimbarea locației sau a locațiilor;

h) prevederile specificate la [art. 14](#), precum și următoarele informații:

(i) accesibilitate;

(ii) disponibilitate;

(iii) integritate;

(iv) confidențialitate;

(v) caracterul privat și siguranța datelor relevante;

i) dreptul societății de a monitoriza în mod regulat activitatea furnizorului de servicii de tip cloud, nivelurile convenite de calitate a serviciilor, cu includerea a cel puțin următoarelor:

(i) obiective de performanță cantitative și calitative clare;

(ii) măsuri corective adecvate în situația în care nu sunt respectate nivelurile convenite de calitate a serviciilor, fără întârzieri nejustificate;

j) obligațiile de raportare ale furnizorului de servicii de tip cloud către societate, inclusiv, dacă este cazul, obligațiile de transmitere a rapoartelor relevante pentru funcția de securitate și funcțiile-cheie ale societății, cum ar fi rapoarte de audit intern a furnizorului de servicii de tip cloud;

k) posibilitatea de a impune furnizorului de servicii de tip cloud de a încheia o asigurare obligatorie împotriva anumitor riscuri, cu precizarea, după caz, a sumei asigurate;

l) planul de continuare a activității, prin intermediul unui plan de urgență pentru administrarea situației de criză și testarea acestuia;

m) acordarea accesului societății, A.S.F. și altor persoane desemnate de acestea, de către furnizorul de servicii de tip cloud, la:

(i) toate sediile operaționale relevante, cum ar fi sedii centrale și centre operaționale;

(ii) întreaga gamă de dispozitive, sisteme, rețele, informații și date relevante utilizate pentru furnizarea funcției externalizate;

(iii) informații de natură financiară, despre personal și despre auditorii externi ai furnizorului de servicii de tip cloud;

(iv) drepturi nelimitate de control și de audit legate de acordul de externalizare, denumite drepturi de audit, pentru a se permite monitorizarea acordului 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 de tip cloud.

ARTICOLUL 13

Drepturi de acces și de audit

(1) În vederea respectării obligațiilor prevăzute de prevederile legale, acordul de externalizare a serviciilor de tip cloud oferă posibilitatea ca societatea să

exercite efectiv drepturile de acces, drepturile de audit și opțiunile de control asupra serviciilor de tip cloud.

(2) Societatea își exercită drepturile de acces și de audit, stabilește frecvența misiunilor de audit, precum și domeniile și serviciile care urmează să fie auditate, adoptând o abordare bazată pe riscuri în conformitate cu cerințele Normei nr. 35/2015.

(3) La stabilirea frecvenței și sferei de exercitare a drepturilor de acces sau de audit, societatea ține cont de cel puțin următoarele:

a) dacă externalizarea în cloud este asociată sau nu unei funcții sau activități operaționale critice sau semnificative;

b) de natura și amploarea riscului;

c) de impactul acordurilor de externalizare în cloud asupra societății.

(4) În situația în care, în urma exercitării drepturilor de acces, a drepturilor de audit sau ca urmare a utilizării anumitor tehnici de audit se creează un risc pentru mediul de afaceri al furnizorului de servicii de tip cloud și/sau pentru un alt client al acestuia, cum ar fi impactul asupra nivelului calității serviciilor, a disponibilității datelor sau a aspectelor de confidențialitate, societatea și furnizorul de servicii de tip cloud impun mecanisme de control specifice, care pot fi testate, astfel încât să fie asigurate modalități alternative de calitate a serviciilor.

(5) Fără a aduce atingere responsabilității finale a societăților cu privire la activitățile desfășurate de furnizorii de servicii de tip cloud, pentru a utiliza mai eficient resursele de audit și pentru a reduce dificultățile de ordin organizatoric pentru furnizorul de servicii de tip cloud și pentru clienții acestuia, se utilizează următoarele:

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

b) audituri centralizate cum ar fi auditurile organizate în comun cu alți clienți ai aceluiași furnizor de servicii de tip cloud sau audituri centralizate efectuate de un terț numit de aceștia.

(6) În cazul externalizării în cloud a unor funcții sau activități operaționale critice sau semnificative, societățile utilizează metoda menționată la alin. (5) lit. a) numai dacă acestea:

a) se asigură că obiectul certificării sau al raportului de audit acoperă sistemele, procesele, aplicațiile, infrastructura, centrele de date 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 caducitatea acestora;

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

d) sunt mulțumite de calitatea activității entității care realizează certificarea sau auditul cu privire la cel puțin următoarele aspecte ale dosarului de audit analizat:

(i) rotația entității de certificare sau de audit;

(ii) calificările și expertiza;

(iii) reeefectuarea și/sau verificarea dovezilor;

e) sunt mulțumite de faptul că emiterea certificărilor și efectuarea auditurilor sunt realizate conform unor standarde corespunzătoare și 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 sunt 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 semnificative; acest drept este exercitat în funcție de necesitățile specifice și în cazul în care nu este posibil prin intermediul altor tipuri de interacțiuni cu furnizorul de servicii de tip cloud.

(7) În vederea externalizării unor funcții operaționale critice sau semnificative către furnizori de servicii de tip cloud, societatea evaluează dacă certificările și rapoartele terților menționate la alin. (5) lit. a) sunt adecvate și suficiente pentru a respecta obligațiile prevederilor legale; societatea aplică o abordare bazată pe risc fără a se limita la aceste rapoarte și certificări de-a lungul timpului.

(8) Înainte de un control planificat la sediu, societatea, auditorul sau terții care acționează în numele societății, dacă nu este posibil să transmită o notificare prealabilă din cauza unei situații de urgență sau de criză, transmite/transmit într-un timp rezonabil un aviz care include cel puțin următoarele:

a) locația;

b) scopul controlului;

c) personalul care va efectua controlul.

(9) Având în vedere faptul că soluțiile de tip cloud au un nivel ridicat de complexitate tehnică, societatea verifică dacă personalul care efectuează auditul are aptitudinile și cunoștințele adecvate pentru a efectua audituri și/sau evaluări relevante; personalul poate fi din cadrul auditorilor săi interni, din grupul de auditori care acționează în numele său, din auditorii desemnați ai furnizorului de servicii de tip cloud sau, după caz, personalul care revizuieste certificarea realizată de o terță parte sau rapoartele de audit ale furnizorului de servicii.

ARTICOLUL 14

Securitatea datelor și a sistemelor

(1) Societatea se asigură că furnizorii de servicii de tip cloud respectă prevederile legale, precum și standardele corespunzătoare de securitate TIC.

(2) În cazul externalizării unor funcții sau activități operaționale critice sau semnificative către furnizori de servicii de tip cloud, societatea prevede în acordul de externalizare inclusiv cerințe specifice de securitate a informațiilor și monitorizează periodic respectarea acestor cerințe.

(3) În vederea respectării **alin. (2)**, societatea ține cont de responsabilitățile sale și de cele ale furnizorului de servicii de tip cloud, iar prin abordarea bazată pe riscuri:

a) convine asupra repartizării clare a rolurilor și responsabilităților între furnizorul de servicii de tip cloud și societate în legătură cu funcțiile sau activitățile operaționale afectate de externalizarea în cloud;

b) stabilește și decide 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) 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) 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) asigură contractual că disponibilitatea traficului de rețea și capacitatea preconizată îndeplinesc cerințe stricte în ceea ce privește continuitatea, dacă sunt aplicabile și fezabile;

f) definește și introduce cerințe corespunzătoare în ceea ce privește continuitatea, asigurând niveluri adecvate de calitate la fiecare nivel al lanțului tehnologic, dacă este cazul;

g) asigură 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) adoptă o abordare bazată pe riscuri privind locația/locațiile de stocare și de prelucrare a datelor, cum ar fi statul sau regiunea, incluzând considerații privind securitatea informațiilor;

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

ARTICOLUL 15

Externalizarea în lanț a funcțiilor și activităților operaționale critice sau semnificative

În situația în care externalizarea în lanț a funcțiilor operaționale critice sau semnificative, inclusiv a unei părți din acestea, este permisă, acordul de externalizare în cloud dintre societate și furnizorul de servicii de tip cloud stipulează cel puțin următoarele:

a) tipurile de activități care sunt excluse de la potențiala externalizare în lanț;

b) condițiile care ar trebui respectate în cazul subcontractării în lanț, cum ar fi, dar fără a ne limita la acestea, respectarea pe deplin a subcontractantului a obligațiilor relevante ce revin furnizorului de servicii de tip cloud; aceste obligații includ drepturile de audit și de acces și securitatea datelor și a sistemelor;

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

d) obligația furnizorului de servicii de tip cloud 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 permite 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) dreptul de a se opune modificărilor și/sau dreptul de a rezilia sau denunța contractul în cazul în care un furnizor de servicii de tip cloud intenționează să schimbe subcontractantul sau serviciile externalizate subcontractate, dacă acestea ar avea un potențial efect negativ asupra evaluării riscurilor serviciilor convenite.

ARTICOLUL 16

Monitorizarea și controlul acordurilor de externalizare în cloud

(1) Societatea, printr-o abordare bazată pe riscuri, monitorizează periodic desfășurarea activităților, măsurile de securitate și respectarea nivelului convenit al calității serviciilor oferite de către furnizorii de servicii de tip cloud, în special externalizarea în cloud a funcțiilor operaționale critice sau semnificative.

(2) În vederea respectării prevederilor alin. (1), societatea instituie mecanisme de monitorizare și de control care să țină seama, dacă este posibil și adecvat, de externalizarea în lanț a unor funcții operaționale critice sau semnificative sau a unei părți din acestea.

(3) Conducerea este informată periodic cu privire la riscurile identificate asociate externalizării în cloud a funcțiilor sau activităților operaționale critice sau semnificative.

(4) Pentru a asigura monitorizarea adecvată și un control adecvat asupra acordurilor de externalizare în cloud, societățile utilizează suficiente resurse cu abilități și cunoștințe adecvate pentru a putea monitoriza serviciile externalizate în cloud; personalul societății care se ocupă de aceste activități deține cunoștințele necesare atât din domeniul TIC, cât și despre domeniul de afaceri.

ARTICOLUL 17

Drepturi de reziliere și strategii de încetare a acordului

(1) În cazul externalizării în cloud a unor funcții sau activități operaționale critice sau semnificative, acordul prevede o clauză clar definită privind strategia de încetare a acestuia, prin care să asigure faptul că societatea are capacitatea să denunțe acordul, dacă este necesar, fără a aduce atingere continuității și calității furnizării serviciilor către contractanți, astfel:

a) elaborează planuri de încetare a acordului care să fie cuprinzătoare, în funcție de servicii, documentate și testate suficient, cum ar fi efectuarea unei

analize a costurilor potențiale, a impactului, a resurselor și a implicațiilor în timp ale diverselor opțiuni potențiale de încetare a acordului;

b) identifică soluții alternative și elaborează planuri de tranziție adecvate și fezabile pentru a permite societății să elimine și să transfere activitățile și datele existente de la furnizorul de servicii de tip cloud către alți furnizori de servicii sau înapoi la societate; aceste soluții sunt 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) se asigură că furnizorul de servicii de tip cloud acordă asistență adecvată societății atunci când transferă datele, sistemele sau aplicațiile externalizate către un alt furnizor de servicii sau direct către societate;

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

(2) La elaborarea strategiilor de încetare a acordului, societatea ia în considerare cel puțin următoarele:

a) stabilirea obiectivelor strategiei de încetare a acordului;

b) stabilirea evenimentelor declanșatoare cum ar fi indicatori-cheie de risc care raportează un nivel inacceptabil de calitate a serviciilor, care ar putea activa strategia de încetare a acordului;

c) analiza 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) alocarea rolurilor și responsabilităților pentru managementul planurilor de încetare a acordului și a activităților de tranziție;

e) stabilirea criteriilor care asigură o tranziție eficientă.

ARTICOLUL 18

Supravegherea acordurilor de externalizare în cloud de către A.S.F.

(1) A.S.F. poate efectua analiza impactului acordurilor de externalizare în cloud ale societăților în cadrul procesului de supraveghere, în special, asupra acordurilor de externalizare a funcțiilor sau activităților operaționale critice sau semnificative.

(2) A.S.F. poate lua 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.

(3) În evaluarea realizată, A.S.F. poate include 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 tuturor riscurilor evidențiate în prezentul ghid.

(4) În cazul grupurilor, A.S.F., în calitate de supraveghetor al grupului, se asigură că impactul externalizării în cloud a funcțiilor sau activităților operaționale critice sau semnificative este reflectat în evaluarea pentru supraveghere a riscurilor la nivel de grup, ținând cont de cerințele enumerate la [alin. \(2\)](#) și [\(3\)](#) și de caracteristicile individuale operaționale și de guvernanță ale grupului.

(5) Dacă externalizarea în cloud a funcțiilor sau activităților operaționale critice sau semnificative implică mai multe societăți din diferite state membre și managementul acestora este asigurat centralizat de societatea-mamă sau de o filială a grupului cum ar fi o societate sau o societate de servicii de grup, cum ar fi furnizorul TIC de grup, A.S.F., în calitate de supraveghetor al grupului, și/sau autoritățile de supraveghere relevante ale societăților implicate în externalizarea serviciilor de tip cloud discută în cadrul colegiului de supraveghetori cu autoritățile de supraveghere relevante ale societăților implicate în externalizarea serviciilor cloud, după caz, impactul externalizării în cloud asupra profilului de risc al grupului.

(6) În cazul în care sunt identificate aspecte care conduc la concluzia că societatea nu mai are instituite mecanisme adecvate de guvernanță sau încalcă prevederile legale, aceasta respectă măsurile impuse de A.S.F., precum:

a) îmbunătățirea sistemului de guvernanță;

b) limitarea sau restrângerea numărului funcțiilor externalizate;

c) încetarea unuia sau mai multor acorduri de externalizare;

d) alte măsuri necesare.

(7) Ținând cont de necesitatea asigurării continuității activității societății, măsura prevăzută la [alin. \(6\) lit. c\)](#) se impune în cazul nerespectării sau aplicării deficitare a celorlalte măsuri adoptate de A.S.F.

ARTICOLUL 19

Prevederi finale

(1) Nerespectarea prevederilor prezentei norme se sancționează în conformitate cu [art. 163](#) din Legea nr. 237/2015.

(2) Prezenta normă se publică în Monitorul Oficial al României, Partea I, intră în vigoare la data publicării și se aplică de la data de 1 ianuarie 2021 tuturor acordurilor de externalizare în cloud încheiate sau modificate începând cu această dată.

(3) Societățile revizuiesc și modifică în mod corespunzător acordurile existente de externalizare asociate unor funcții sau activități operaționale critice sau semnificative, pentru a asigura respectarea prezentei norme, până cel târziu la 31 decembrie 2022.

(4) Societățile dispun încetarea acordurilor de externalizare a serviciilor cloud asociate funcțiilor sau activităților operaționale critice sau semnificative

până cel târziu la data de 31 decembrie 2022, dacă până la această dată revizuirea acestor acorduri nu poate fi finalizată; societățile notifică A.S.F. încetarea acordurilor în termen de 10 zile lucrătoare de la data încetării acestora.

(5) Actualizarea, acolo unde este necesar, a politicilor și procedurilor societății se efectuează până la data de 1 ianuarie 2021, iar cerințele privind documentarea pentru acordurile de externalizare în cloud asociate funcțiilor sau activităților operaționale critice sau semnificative sunt puse în aplicare până la data de 31 decembrie 2022.

Președintele Autorității de Supraveghere Financiară,
Nicu Marcu

București, 12 august 2020.
Nr. 33.