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 21 ianuarie 2021.

În conformitate cu prevederile art. 2 alin. (1) lit. b), art. 3 alin. (1) lit. b) şi art. 6 alin. (2) din Ordonanţa de urgenţă a Guvernului nr. 93/2012 privind înfiinţarea, organizarea şi funcţionarea Autorităţii de Supraveghere Financiară, aprobată cu modificări şi completări prin Legea nr. 113/2013, cu modificările şi completările ulterioare,

în temeiul prevederilor art. 33, art. 173 alin. (1) lit. t) şi art. 179 alin. (4) din Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi reasigurare, cu modificările şi 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 şi a Consiliului privind accesul la activitate şi desfăşurarea activităţii de asigurare şi de reasigurare (Solvabilitate II), cu modificările şi completările ulterioare,

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

în urma deliberărilor Consiliului Autorităţii de Supraveghere Financiară din cadrul şedinţei din data de 12 august 2020,

Autoritatea de Supraveghere Financiară emite următoarea normă:

ARTICOLUL 1
Prevederi generale şi domeniul de aplicare

(1) Prezenta normă reglementează modul în care societăţile aplică cerinţele referitoare la externalizare prevăzute în Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi reasigurare, cu modificările şi completările ulterioare, denumită în continuare Legea nr. 237/2015, şi în Regulamentul delegat (UE) 2015/35 al Comisiei din 10 octombrie 2014 de completare a Directivei 2009/138/CE a Parlamentului European şi a Consiliului privind accesul la activitate şi desfăşurarea activităţii de asigurare şi de reasigurare (Solvabilitate II), cu modificările şi completările ulterioare, denumit în continuare Regulamentul delegat nr. 35/2015, în contextul externalizării către furnizorii de servicii de tip cloud.

(2) Externalizarea funcţiilor sau activităţilor operaţionale către alţi furnizori de servicii care se bazează în mod semnificativ pe infrastructuri de tip cloud intră în sfera de aplicare a prezentei norme.

ARTICOLUL 2
Definiţii

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

1. furnizor de servicii - o entitate terţă care realizează un proces, serviciu sau o activitate sau părţi 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 reţea la un grup comun de resurse de calcul configurabile, care poate fi rapid pus la dispoziţie şi lansat cu un efort minim de gestionare sau interacţiune 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 entităţi din cadrul aceluiaşi grup;

7. cloud hibrid - infrastructură informatică compusă din două sau mai multe infrastructuri distincte de tip cloud;

8. TIC - tehnologia informaţiei şi comunicaţiilor.

ARTICOLUL 3
Serviciile cloud şi externalizarea

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

(2) La evaluarea prevăzută la alin. (1) societăţile iau în considerare dacă funcţia, activitatea operaţională externalizată, inclusiv o parte a acesteia:

a) este efectuată în mod repetat sau continuu;

b) intră în sfera funcţiilor sau activităţilor operaţionale 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 funcţii sau activităţi operaţionale, societăţile 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 funcţie sau activitate operaţională critică sau semnificativă în conformitate cu art. 6;

2. identifică şi evaluează riscurile relevante asociate acordurilor de externalizare în cloud, în conformitate cu art. 7;

3. efectuează o analiză complexă corespunzătoare cu privire la potenţialul furnizor de servicii de tip cloud, în conformitate cu art. 8;

4. identifică şi evaluează conflictele de interese pe care le poate cauza externalizarea, în conformitate cu cerinţele prevăzute la art. 274 alin. (3) lit. b) din Regulamentul delegat nr. 35/2015.

ARTICOLUL 5
Principii generale de guvernanţă 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 funcţii sau activităţi operaţionale critice sau semnificative către furnizorii de servicii de tip cloud se bazează pe o evaluare detaliată a riscurilor aferente acordului şi a cel puţin următoarelor:

a) riscul TIC;

b) riscul privind continuitatea activităţii;

c) riscul juridic;

d) riscul de conformitate;

e) riscul de concentrare;

f) riscul operaţional;

g) riscul asociat fazei de migrare a datelor şi/sau fazei de implementare, după caz.

(2) Societăţile ţin cont în cadrul ORSA de modificările din profilul de risc asociate acordurilor de externalizare în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative către furnizorii de servicii de tip cloud.

(3) Serviciile cloud se utilizează în concordanţă cu politicile şi procedurile interne ale societăţii, actualizate atunci când este necesar şi ţinând cont de cel puţin următoarele:

a) strategia TIC;

b) strategia de securitate a informaţiilor;

c) strategia managementului riscului operaţional.

ARTICOLUL 6
Evaluarea funcţiilor şi activităţilor operaţionale critice sau semnificative

(1) La efectuarea evaluării menţionate la art. 8 alin. (1) societatea analizează dacă acordul are potenţialul de a deveni critic sau semnificativ în viitor; de asemenea societatea reevaluează şi caracterul critic sau semnificativitatea funcţiei sau a activităţii operaţionale externalizate anterior către furnizorii de servicii de tip cloud, în

cazul în care natura, amploarea şi complexitatea riscurilor inerente acordului se modifică semnificativ.

(2) În cadrul evaluării societatea ţine cont, în paralel cu rezultatul evaluării riscurilor, cel puţin de următorii factori:

a) impactul potenţial al perturbărilor semnificative ale funcţiei sau activităţii operaţionale 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) rezilienţei şi viabilităţii din punct de vedere financiar şi al solvabilităţii, pe termen scurt şi lung;

(iii) continuităţii activităţii şi a rezilienţei operaţionale;

(iv) riscului operaţional, riscului juridic, riscului TIC, riscului de conduită şi riscului reputaţional;

b) impactul potenţial al acordului de externalizare în cloud asupra capacităţii societăţii de a:

(i) identifica, monitoriza şi gestiona toate riscurile relevante;

(ii) respecta toate cerinţele juridice şi prevederile legale;

(iii) efectua audituri adecvate asupra funcţiei sau activităţii operaţionale externalizate;

c) expunerea agregată a societăţii şi/sau a grupului, după caz, faţă de acelaşi furnizor de servicii de tip cloud şi potenţialul impact cumulativ al acordurilor de externalizare pentru acelaşi domeniu de activitate;

d) dimensiunea şi complexitatea fiecărui tip de activitate al societăţii, 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) protecţia datelor comerciale care sunt secrete şi/sau sensibile, protecţia datelor cu caracter personal şi nepersonal şi impactul potenţial asupra societăţii, contractanţilor sau altor subiecţi relevanţi al unei încălcări a obligaţiei de confidenţialitate sau al incapacităţii de a asigura disponibilitatea şi integritatea datelor în conformitate cu prevederile Regulamentului (UE) 2016/679 al Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

ARTICOLUL 7

Evaluarea riscurilor asociate externalizării în cloud

(1) Societatea adoptă o abordare proporţională cu natura, amploarea şi complexitatea riscurilor inerente serviciilor externalizate către furnizorii de servicii de tip cloud şi include evaluarea impactului potenţial al fiecărei externalizări în cloud, în special asupra riscurilor operaţional şi reputaţional.

(2) În cazul externalizării unor funcţii sau activităţi operaţionale critice sau semnificative către furnizorii de servicii de tip cloud, societatea:

a) ţine seama de beneficiile şi 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, necesităţile, toate riscurile, precum şi limitările capacităţii de control care decurg din:

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

(ii) migrarea şi/sau implementarea;

(iii) datele şi sistemele aferente activităţilor externalizate sau avute în vedere pentru a fi externalizate, senzitivitatea acestora şi măsurile de securitate necesare;

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

(v) legislaţia în vigoare, inclusiv legislaţia privind protecţia datelor;

(vi) dispoziţiile de aplicare a legii în vigoare;

(vii) dispoziţiile din legislaţia privind insolvenţa care s-ar aplica în cazul incapacităţii unui furnizor de servicii de tip cloud şi impedimentele care ar putea apărea în caz de recuperare urgentă a datelor societăţii;

(viii) riscurile asociate externalizării în lanţ, inclusiv:

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

2. riscul ca lanţurile lungi şi complexe de externalizare să diminueze capacitatea societăţilor de a avea control asupra funcţiilor sau activităţilor operaţionale critice sau semnificative;

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

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

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

2. existenţa mai multor acorduri de externalizare cu acelaşi furnizor de servicii de tip cloud.

(3) Atunci când societatea ia cunoştinţă de deficienţe şi/sau modificări semnificative ale serviciilor furnizate sau ale situaţiei 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 selecţie şi evaluare, societatea se asigură că furnizorul de servicii de tip cloud corespunde criteriilor definite prin politicile şi procedurile interne de externalizare.

(2) Evaluarea complexă a furnizorului de servicii de tip cloud se efectuează înainte de externalizarea funcţiilor sau activităţilor operaţionale.

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

(4) În cazul externalizării în cloud a funcţiilor operaţionale critice sau semnificative, evaluarea complexă include o evaluare a adecvării furnizorului de servicii de tip cloud şi are în vedere cel puţin următoarele:

a) competenţe;

b) infrastructură;

c) situaţie 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 internaţionale, rapoarte de audit ale unor terţi recunoscuţi sau rapoarte de audit intern, precum şi alte documente care pot să demonstreze efectuarea evaluării complexe.

ARTICOLUL 9

Documentarea

(1) În cadrul sistemului de guvernanţă şi al managementului riscului, societatea ţine evidenţa acordurilor de externalizare în cloud, sub forma unui registru dedicat şi actualizat; societatea menţine, pentru o perioadă de doi ani, o evidenţă a acordurilor de externalizare în cloud încetate.

(2) În cazul externalizării funcţiilor sau activităţilor operaţionale critice sau semnificative, societatea înregistrează următoarele:

a) informaţiile notificate A.S.F. prevăzute la art. 10 alin. (2);

b) în cazul grupurilor, societăţile şi alte entităţi care intră în sfera de aplicare a consolidării prudenţiale şi care utilizează servicii de tip cloud;

c) data celor mai recente evaluări a riscurilor şi un rezumat succint al principalelor rezultate;

d) persoana sau organul din conducerea societăţii care a aprobat acordul de externalizare în cloud;

e) data celui mai recent audit şi data următoarelor audituri programate;

f) denumirea subcontractanţilor cărora le sunt externalizate părţi semnificative ale unei funcţii sau activităţi operaţionale critice sau semnificative, inclusiv statul în care sunt înregistraţi subcontractanţii, în care se prestează serviciul şi locaţiile, respectiv statele şi regiunile în care sunt stocate datele;

g) rezultatul evaluării capacităţii de substituire a furnizorului de servicii de tip cloud care să indice uşurinţa, dificultatea sau imposibilitatea substituirii;

h) dacă în cadrul funcţiei sau activităţii operaţionale critice sau semnificative externalizate există operaţiuni 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 denunţare de către oricare dintre părţi sau de întrerupere a serviciilor de către furnizorul de servicii de tip cloud.

(3) În cazul externalizării funcţiilor sau activităţilor operaţionale necritice sau nesemnificative, societatea defineşte informaţiile ce se înregistrează în funcţie de natura, amploarea şi complexitatea riscurilor inerente serviciilor oferite de furnizorul de servicii de tip cloud.

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

ARTICOLUL 10

Notificarea scrisă adresată A.S.F.

(1) Cerinţele de notificare scrisă prevăzute la art. 33 alin. (3) din Legea nr. 237/2015 şi detaliate de Norma Autorităţii de Supraveghere Financiară nr. 35/2015 privind cerinţele calitative stabilite de către Autoritatea Europeană de Supraveghere pentru Asigurări şi Pensii Ocupaţionale, denumită în continuare Norma nr. 35/2015, se aplică tuturor acţiunilor de externalizare a funcţiilor şi activităţilor operaţionale critice sau semnificative către furnizorii de servicii de tip cloud; societatea notifică A.S.F. atunci când o funcţie sau activitate operaţională externalizată şi clasificată anterior drept necritică sau nesemnificativă devine critică sau semnificativă.

(2) Notificarea scrisă include, ţinând cont de principiul proporţionalităţii, cel puţin următoarele informaţii:

a) scurtă descriere a funcţiei sau activităţii operaţionale externalizate;

b) data de începere şi, după caz, următoarea dată de reînnoire a contractului, data de încetare şi/sau perioadele de preaviz pentru furnizorul de servicii de tip cloud şi 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 şi alte date de contact relevante, precum şi denumirea societăţii-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 şi modelele publice/private/hibride/comunitare de implementare, precum şi natura specifică a datelor ce urmează a fi deţinute şi locaţiile unde sunt stocate datele respective;

f) un scurt rezumat al motivelor pentru care funcţia sau activitatea operaţională externalizată este considerată critică sau semnificativă;

g) data celei mai recente evaluări a caracterului critic sau a semnificativităţii funcţiei sau activităţii operaţionale externalizate.

ARTICOLUL 11

Actualizarea politicii scrise de externalizare

În cazul externalizării către furnizorii de servicii de tip cloud, societăţile actualizează atât politicile şi procedurile aferente externalizării cât şi politicile şi procedurile relevante cum ar fi cele privind securitatea informaţiilor, luând în considerare cel puţin următoarele:

a) rolurile şi responsabilităţile funcţiilor implicate din cadrul societăţilor, în special:

(i) conducerea;

(ii) funcţia responsabilă de TIC;
(iii) funcţia responsabilă de securitatea informaţiilor;
(iv) funcţia de conformitate;
(v) funcţia de managementul riscului;
(vi) funcţia de audit intern;

b) procesele şi procedurile de raportare necesare pentru aprobarea, punerea în aplicare, monitorizarea, managementul şi reînnoirea, după caz, a acordurilor de externalizare în cloud asociate funcţiilor sau activităţilor operaţionale critice sau semnificative;

c) controlul asupra serviciilor cloud, proporţional cu natura, amploarea şi complexitatea riscurilor inerente serviciilor furnizate, inclusiv:

(i) evaluarea riscurilor asociate acordurilor de externalizare în cloud şi evaluarea complexă a furnizorilor de servicii de tip cloud, inclusiv frecvenţa evaluării riscurilor;
(ii) mecanisme de monitorizare şi de management;
(iii) standarde şi mecanisme de securitate;

d) cerinţele contractuale prevăzute la art. 12 în cazul externalizării în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative;

e) documentarea şi notificarea scrisă către A.S.F. cu privire la externalizarea în cloud a funcţiilor sau activităţilor critice sau semnificative;

f) strategia de încetare a acordului, în cazul funcţiilor sau activităţilor operaţionale critice sau semnificative, documentată şi, dacă este cazul, suficient testată care să fie proporţională cu natura, amploarea şi complexitatea riscurilor inerente serviciilor furnizate;

g) procesele de denunţare, inclusiv, dar fără a se limita la întreruperea, reintegrarea sau transferul serviciilor incluse în acordul de externalizarea în cloud.

ARTICOLUL 12
Cerinţe contractuale

(1) Drepturile şi obligaţiile ce le revin societăţii şi 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 funcţii sau activităţi operaţionale critice sau semnificative către un furnizor de servicii de tip cloud, acordul scris dintre societate şi furnizorul de servicii cloud cuprinde cel puţin următoarele:

a) o descriere clară a funcţiei externalizate care urmează să fie furnizată şi tipul serviciilor de asistenţă;

b) data de începere şi data de încetare a acordului, după caz;

c) perioadele de preaviz pentru furnizorul de servicii de tip cloud şi pentru societate;

d) jurisdicţia instanţei şi legea aplicabilă acordului;

e) obligaţiile financiare ale celor două părţi;

f) dacă este permisă externalizarea în lanţ a unei funcţii sau activităţi operaţionale critice sau semnificative sau a unor părţi semnificative din aceasta, inclusiv condiţiile la care este supusă externalizarea în lanţ semnificativă şi cele ale art. 15;

g) locaţia sau locaţiile centrelor de date, cu precizarea regiunii, a statului sau a statelor unde sunt stocate şi prelucrate date relevante, inclusiv:

(i) condiţiile care trebuie îndeplinite;

(ii) cerinţa de a notifica societatea în cazul în care furnizorul de servicii propune schimbarea locaţiei sau a locaţiilor;

h) prevederile specificate la art. 14, precum şi următoarele informaţii:

(i) accesibilitate;

(ii) disponibilitate;

(iii) integritate;

(iv) confidenţialitate;

(v) caracterul privat şi siguranţa datelor relevante;

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

(i) obiective de performanţă cantitative şi calitative clare;

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

j) obligaţiile de raportare ale furnizorului de servicii de tip cloud către societate, inclusiv, dacă este cazul, obligaţiile de transmitere a rapoartelor relevante pentru funcţia de securitate şi funcţiile-cheie ale societăţii, 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 activităţii, prin intermediul unui plan de urgenţă pentru administrarea situaţiei de criză şi testarea acestuia;

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

(i) toate sediile operaţionale relevante, cum ar fi sedii centrale şi centre operaţionale;

(ii) întreaga gamă de dispozitive, sisteme, reţele, informaţii şi date relevante utilizate pentru furnizarea funcţiei externalizate;

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

(iv) drepturi nelimitate de control şi de audit legate de acordul de externalizare, denumite drepturi de audit, pentru a se permite monitorizarea acordului de externalizare şi pentru a asigura respectarea tuturor cerinţelor contractuale şi de reglementare aplicabile;

n) clauze prin care se garantează faptul că datele care aparţin societăţii pot fi recuperate rapid de aceasta în cazul insolvenţei, al rezoluţiei sau al întreruperii operaţiunilor realizate de furnizorul de servicii de tip cloud.

ARTICOLUL 13

Drepturi de acces şi de audit

(1) În vederea respectării obligaţiilor 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 şi opţiunile de control asupra serviciilor de tip cloud.

(2) Societatea îşi exercită drepturile de acces şi de audit, stabileşte frecvenţa misiunilor de audit, precum şi domeniile şi serviciile care urmează să fie auditate, adoptând o abordare bazată pe riscuri în conformitate cu cerinţele Normei nr. 35/2015.

(3) La stabilirea frecvenţei şi sferei de exercitare a drepturilor de acces sau de audit, societatea ţine cont de cel puţin următoarele:

a) dacă externalizarea în cloud este asociată sau nu unei funcţii sau activităţi operaţionale critice sau semnificative;

b) de natura şi amploarea riscului;

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

(4) În situaţia 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 şi/sau pentru un alt client al acestuia, cum ar fi impactul asupra nivelului calităţii serviciilor, a disponibilităţii datelor sau a aspectelor de confidenţialitate, societatea şi furnizorul de servicii de tip cloud impun mecanisme de control specifice, care pot fi testate, astfel încât să fie asigurate modalităţi alternative de calitate a serviciilor.

(5) Fără a aduce atingere responsabilităţii finale a societăţilor cu privire la activităţile desfăşurate de furnizorii de servicii de tip cloud, pentru a utiliza mai eficient resursele de audit şi pentru a reduce dificultăţile de ordin organizatoric pentru furnizorul de servicii de tip cloud şi pentru clienţii acestuia, se utilizează următoarele:

a) certificări de la terţi şi rapoarte de audit intern sau efectuate de terţi, puse la dispoziţie de furnizorul de servicii de tip cloud;

b) audituri centralizate cum ar fi auditurile organizate în comun cu alţi clienţi ai aceluiaşi furnizor de servicii de tip cloud sau audituri centralizate efectuate de un terţ numit de aceştia.

(6) În cazul externalizării în cloud a unor funcţii sau activităţi operaţionale critice sau semnificative, societăţile utilizează metoda menţionată la alin. (5) lit. a) numai dacă acestea:

a) se asigură că obiectul certificării sau al raportului de audit acoperă sistemele, procesele, aplicaţiile, infrastructura, centrele de date şi mecanismele de control identificate şi evaluează respectarea cerinţelor de reglementare relevante;

b) evaluează temeinic şi periodic conţinutul noilor certificări sau rapoarte de audit şi verifică caducitatea acestora;

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

d) sunt mulţumite de calitatea activităţii entităţii care realizează certificarea sau auditul cu privire la cel puţin următoarele aspecte ale dosarului de audit analizat:

(i) rotaţia entităţii de certificare sau de audit;

(ii) calificările şi expertiza;

(iii) reefectuarea şi/sau verificarea dovezilor;

e) sunt mulţumite de faptul că emiterea certificărilor şi efectuarea auditurilor sunt realizate conform unor standarde corespunzătoare şi includ un test de eficacitate operaţională 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 şi mecanisme de control relevante; numărul şi frecvenţa acestor cereri de modificare a domeniului de aplicare sunt rezonabile şi legitime din perspectiva managementului riscului;

g) păstrează dreptul contractual de a efectua audituri individuale la sediul furnizorului, la aprecierea proprie, în ceea ce priveşte externalizarea în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative; acest drept este exercitat în funcţie de necesităţile specifice şi în cazul în care nu este posibil prin intermediul altor tipuri de interacţiuni cu furnizorul de servicii de tip cloud.

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

(8) Înainte de un control planificat la sediu, societatea, auditorul sau terţii care acţionează în numele societăţii, dacă nu este posibil să transmită o notificare prealabilă din cauza unei situaţii de urgenţă sau de criză, transmite/transmit într-un timp rezonabil un aviz care include cel puţin următoarele:

a) locaţia;

b) scopul controlului;

c) personalul care va efectua controlul.

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

ARTICOLUL 14

Securitatea datelor şi a sistemelor

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

(2) În cazul externalizării unor funcţii sau activităţi operaţionale critice sau semnificative către furnizori de servicii de tip cloud, societatea prevede în acordul de externalizare inclusiv cerinţe specifice de securitate a informaţiilor şi monitorizează periodic respectarea acestor cerinţe.

(3) În vederea respectării alin. (2), societatea ţine cont de responsabilităţile sale şi de cele ale furnizorului de servicii de tip cloud, iar prin abordarea bazată pe riscuri:

a) convine asupra repartizării clare a rolurilor şi responsabilităţilor între furnizorul de servicii de tip cloud şi societate în legătură cu funcţiile sau activităţile operaţionale afectate de externalizarea în cloud;

b) stabileşte şi decide asupra nivelului adecvat de protecţie a datelor confidenţiale, asupra continuităţii activităţilor externalizate şi asupra integrităţii şi trasabilităţii datelor şi 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 şi datele în repaus, cum ar fi utilizarea tehnologiilor de criptare în combinaţie cu o arhitectură de management adecvat al cheilor;

d) ia în considerare mecanismele de integrare a serviciilor cloud în sistemele proprii, de exemplu, interfeţele de programare a aplicaţiilor şi un proces adecvat de management al accesului şi utilizatorilor;

e) asigură contractual că disponibilitatea traficului de reţea şi capacitatea preconizată îndeplinesc cerinţe stricte în ceea ce priveşte continuitatea, dacă sunt aplicabile şi fezabile;

f) defineşte şi introduce cerinţe corespunzătoare în ceea ce priveşte continuitatea, asigurând niveluri adecvate de calitate la fiecare nivel al lanţului tehnologic, dacă este cazul;

g) asigură un proces adecvat şi bine documentat de management al incidentelor, cu responsabilităţile aferente, de exemplu, prin elaborarea unui model de cooperare în caz de incidente reale sau preconizate;

h) adoptă o abordare bazată pe riscuri privind locaţia/locaţiile de stocare şi de prelucrare a datelor, cum ar fi statul sau regiunea, incluzând consideraţii privind securitatea informaţiilor;

i) monitorizează respectarea cerinţelor referitoare la aplicarea efectivă şi 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 lanţ a funcţiilor şi activităţilor operaţionale critice sau semnificative

În situaţia în care externalizarea în lanţ a funcţiilor operaţionale critice sau semnificative, inclusiv a unei părţi din acestea, este permisă, acordul de externalizare în cloud dintre societate şi furnizorul de servicii de tip cloud stipulează cel puţin următoarele:

a) tipurile de activităţi care sunt excluse de la potenţiala externalizare în lanţ;

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

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

d) obligaţia furnizorului de servicii de tip cloud de a informa societatea despre modificările semnificative planificate la nivel de subcontractanţi sau de servicii externalizate în lanţ care ar putea afecta capacitatea furnizorului de servicii de a-şi îndeplini obligaţiile asumate prin acordul de externalizare în cloud; perioada de notificare a acestor modificări permite societăţii, cel puţin, să efectueze o evaluare a riscurilor în ceea ce priveşte efectele modificărilor propuse înainte ca modificarea efectivă a subcontractanţilor şi a serviciilor subcontractate să intre în vigoare;

e) dreptul de a se opune modificărilor şi/sau dreptul de a rezilia sau denunţa contractul în cazul în care un furnizor de servicii de tip cloud intenţionează să schimbe subcontractantul sau serviciile externalizate subcontractate, dacă acestea ar avea un potenţial efect negativ asupra evaluării riscurilor serviciilor convenite.

ARTICOLUL 16

Monitorizarea şi controlul acordurilor de externalizare în cloud

(1) Societatea, printr-o abordare bazată pe riscuri, monitorizează periodic desfăşurarea activităţilor, măsurile de securitate şi respectarea nivelului convenit al calităţii serviciilor oferite de către furnizorii de servicii de tip cloud, în special externalizarea în cloud a funcţiilor operaţionale critice sau semnificative.

(2) În vederea respectării prevederilor alin. (1), societatea instituie mecanisme de monitorizare şi de control care să ţină seama, dacă este posibil şi adecvat, de externalizarea în lanţ a unor funcţii operaţionale critice sau semnificative sau a unei părţi din acestea.

(3) Conducerea este informată periodic cu privire la riscurile identificate asociate externalizării în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative.

(4) Pentru a asigura monitorizarea adecvată şi un control adecvat asupra acordurilor de externalizare în cloud, societăţile utilizează suficiente resurse cu abilităţi şi cunoştinţe adecvate pentru a putea monitoriza serviciile externalizate în cloud; personalul societăţii care se ocupă de aceste activităţi deţine cunoştinţele necesare atât din domeniul TIC, cât şi despre domeniul de afaceri.

ARTICOLUL 17

Drepturi de reziliere şi strategii de încetare a acordului

(1) În cazul externalizării în cloud a unor funcţii sau activităţi operaţionale 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 denunţe acordul, dacă este necesar, fără a aduce atingere continuităţii şi calităţii furnizării serviciilor către contractanţi, astfel:

a) elaborează planuri de încetare a acordului care să fie cuprinzătoare, în funcţie de servicii, documentate şi testate suficient, cum ar fi efectuarea unei analize a costurilor potenţiale, a impactului, a resurselor şi a implicaţiilor în timp ale diverselor opţiuni potenţiale de încetare a acordului;

b) identifică soluţii alternative şi elaborează planuri de tranziţie adecvate şi fezabile pentru a permite societăţii să elimine şi să transfere activităţile şi datele existente de la furnizorul de servicii de tip cloud către alţi furnizori de servicii sau înapoi la societate; aceste soluţii sunt definite în raport cu problemele care pot apărea din cauza locaţiei datelor, luând măsurile necesare pentru a asigura continuitatea activităţii în faza de tranziţie;

c) se asigură că furnizorul de servicii de tip cloud acordă asistenţă adecvată societăţii atunci când transferă datele, sistemele sau aplicaţiile externalizate către un alt furnizor de servicii sau direct către societate;

d) stabileşte cu furnizorul de servicii de tip cloud că, odată retransferate către societate, datele vor fi şterse complet şi în siguranţă de către furnizorul de servicii de tip cloud, în toate regiunile.

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

a) stabilirea obiectivelor strategiei de încetare a acordului;

b) stabilirea evenimentelor declanşatoare 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, proporţională cu activităţile externalizate pentru a identifica ce resurse umane şi de altă natură ar fi necesare pentru a implementa planul de încetare a acordurilor şi de cât timp ar fi nevoie;

d) alocarea rolurilor şi responsabilităţilor pentru managementul planurilor de încetare a acordului şi a activităţilor de tranziţie;

e) stabilirea criteriilor care asigură o tranziţie 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 societăţilor în cadrul procesului de supraveghere, în special, asupra acordurilor de externalizare a funcţiilor sau activităţilor operaţionale critice sau semnificative.

(2) A.S.F. poate lua în considerare următoarele riscuri la supravegherea acordurilor de externalizare în cloud ale societăţilor:

a) riscurile TIC;

b) alte riscuri operaţionale, inclusiv riscul juridic, riscul de neconformitate, riscul de externalizare şi riscul de management al relaţiei cu terţii;

c) riscul reputaţional;

d) riscul de concentrare, inclusiv la nivel de ţară/sectorial.

(3) În evaluarea realizată, A.S.F. poate include următoarele aspecte, aplicând o abordare bazată pe riscuri:

a) adecvarea şi eficienţa proceselor operaţionale şi de guvernanţă ale societăţii legate de aprobarea, implementarea, monitorizarea, managementul şi reînnoirea acordurilor de externalizare în cloud;

b) dacă societatea are sau nu resurse suficiente cu competenţe şi cunoştinţe adecvate pentru a monitoriza serviciile externalizate în cloud;

c) dacă societatea identifică şi asigură managementul tuturor riscurilor evidenţiate în prezentul ghid.

(4) În cazul grupurilor, A.S.F., în calitate de supraveghetor al grupului, se asigură că impactul externalizării în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative este reflectat în evaluarea pentru supraveghere a riscurilor la nivel de grup, ţinând cont de cerinţele enumerate la alin. (2) şi (3) şi de caracteristicile individuale operaţionale şi de guvernanţă ale grupului.

(5) Dacă externalizarea în cloud a funcţiilor sau activităţilor operaţionale critice sau semnificative implică mai multe societăţi din diferite state membre şi managementul acesteia 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, şi/sau autorităţile de supraveghere relevante ale societăţilor implicate în externalizarea serviciilor de tip cloud discută în cadrul colegiului de supraveghetori cu autorităţile de supraveghere relevante ale societăţilor 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 guvernanţă sau încalcă prevederile legale, aceasta respectă măsurile impuse de A.S.F., precum:

a) îmbunătăţirea sistemului de guvernanţă;

b) limitarea sau restrângerea numărului funcţiilor externalizate;

c) încetarea unuia sau mai multor acorduri de externalizare;

d) alte măsuri necesare.

(7) Ţinând cont de necesitatea asigurării continuităţii activităţii societăţii, 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 sancţionează 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 şi se aplică de la data de 1 ianuarie 2021 tuturor acordurilor de externalizare în cloud încheiate sau modificate începând cu această dată.

(3) Societăţile revizuiesc şi modifică în mod corespunzător acordurile existente de externalizare asociate unor funcţii sau activităţi operaţionale critice sau semnificative, pentru a asigura respectarea prezentei norme, până cel târziu la 31 decembrie 2022.

(4) Societăţile dispun încetarea acordurilor de externalizare a serviciilor cloud asociate funcţiilor sau activităţilor operaţionale critice sau semnificative până cel târziu la data de 31 decembrie 2022, dacă până la această dată revizuirea acestor acorduri nu poate fi finalizată; societăţile 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 şi procedurilor societăţii se efectuează până la data de 1 ianuarie 2021, iar cerinţele privind documentarea pentru acordurile de externalizare în cloud asociate funcţiilor sau activităţilor operaţionale critice sau semnificative sunt puse în aplicare până la data de 31 decembrie 2022.

Preşedintele Autorităţii de Supraveghere Financiară,
Nicu Marcu

Bucureşti, 12 august 2020.
Nr. 33.