

Autoritatea de Supraveghere Financiară - ASF

Norma nr. 40/2016 pentru modificarea și completarea Normei Autorității de Supraveghere Financiară nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate și/sau supravegheate de Autoritatea de Supraveghere Financiară

În vigoare de la 23.12.2016

Publicat în Monitorul Oficial, Partea I nr. 1040 din 23.12.2016.

Tipărit de **Rada Craciun**

În urma deliberărilor Consiliului Autorității de Supraveghere Financiară din cadrul ședinței din data de 14 decembrie 2016,

în temeiul prevederilor art. 3 alin. (1) lit. b), art. 5, art. 6 alin. (2) și ale art. 14 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,

Autoritatea de Supraveghere Financiară emite următoarea normă:

**Art. I.** Norma Autorității de Supraveghere Financiară nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate și/sau supravegheate de Autoritatea de Supraveghere Financiară, publicată în Monitorul Oficial al României, Partea I, nr. 227 din 3 aprilie 2015, se modifică și se completează după cum urmează:

1. La articolul 1, alineatul (1) se modifică și va avea următorul cuprins:

" **Art. 1. (1)** Prezenta normă stabilește cerințele la nivelul entităților autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară, denumită în continuare A.S.F., pentru identificarea, prevenirea și reducerea impactului potențial negativ al riscurilor operaționale generate de utilizarea tehnologiei informației și comunicațiilor la nivel de oameni, procese, sisteme și mediu extern, inclusiv de fapte ce țin de criminalitatea informatică."

2. La articolul 2, partea introductivă se modifică și va avea următorul cuprins:

" **Art. 2.** Prezenta normă se aplică următoarelor categorii de entități autorizate/avizate/înregistrate, reglementate și/sau supravegheate de A.S.F., denumite în continuare entități:"

3. La articolul 2, partea introductivă a literei b) se modifică și va avea următorul cuprins:

" **b)** societăți de administrare a investițiilor (SAI), administratori de fonduri de investiții alternative (AFIA), după cum urmează:"

4. La articolul 2, litera f) se modifică și va avea următorul cuprins:

" **f)** Fondul de compensare a investitorilor, Fondul de garantare a asiguraților și Fondul de garantare a drepturilor din sistemul de pensii private;"

5. La articolul 6, alineatele (4) și (5) se modifică și vor avea următorul cuprins:

" **(4)** Încadrarea, respectiv reîncadrarea entităților menționate la art. 2 lit. b) se realizează în luna ianuarie a fiecărui an calendaristic, în baza valorii totale a activelor în portofoliu/administrate din ultima zi lucrătoare a anului anterior.

**(5)** Încadrarea, respectiv reîncadrarea entităților menționate la art. 2 lit. d) se realizează în luna ianuarie a fiecărui an calendaristic, în baza activității autorizate de A.S.F și a deținerii calității de market maker/furnizor de lichiditate în ultima zi lucrătoare a anului anterior."

6. La articolul 8, după alineatul (2) se introduce un nou alineat, alineatul (3), cu următorul cuprins:

" **(3)** Sistemele informatice care oferă SAI/AFIA și investitorilor lor accesul la platforme electronice de distribuire a titlurilor de participare asigură cel puțin, fără a se limita la:

a) securitatea și integritatea datelor procesate prin folosirea unei modalități de securizare, asupra datelor trimise către platformele electronice de distribuire a titlurilor de participare;

b) mecanisme care să garanteze nerepudierea datelor transmise și recepționate;

c) jurnalizarea în timp real a informației despre instrucțiunile investitorilor transmise;

d) mecanisme de nerepudiere a integrității înregistrării operațiunilor de sistem informatic."

7. La articolul 9, partea introductivă a alineatului (9) se modifică și va avea următorul cuprins:

" **(9)** Contractul menționat la alin. (7) trebuie să conțină o clauză expresă prin care auditorul se obligă să notifice în scris A.S.F. în cel mai scurt timp posibil, dar nu mai târziu de 10 zile de la constatare, cu privire la orice fapt sau act în legătură cu sistemul informatic și de comunicații utilizat de entitate și care:"

8. La articolul 9, partea introductivă a alineatului (10) se modifică și va avea următorul cuprins:

" **(10)** Contractul prevăzut la alin. (7) trebuie să conțină o clauză expresă prin care, la solicitarea scrisă a A.S.F., auditorul se obligă să prezinte A.S.F. în maximum 10 zile de la solicitare:"

9. La **articolul 10**, partea introductivă a **alineatului (2)** se modifică și va avea următorul cuprins:

" **(2)** În vederea obținerii avizului A.S.F., auditorul IT extern depune la A.S.F. o cerere, în care menționează sectorul/sectoarele în care sunt autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către A.S.F. entitățile pentru care intenționează să presteze servicii, însoțită de documentația care trebuie să cuprindă următoarele, după caz:"

10. La articolul 10 alineatul (2), **punctul (v)** al literei a) se modifică și va avea următorul cuprins:

" **(v)** dovada experienței și a specializării pe domeniul de audit extern al sistemelor informatice;"

11. La articolul 10 alineatul (2), **punctele (ii) și (iii)** ale literei b) se modifică și vor avea următorul cuprins:

" **(ii)** curriculum vitae al auditorului IT, datat și semnat, cu prezentarea experienței profesionale în auditarea externă a sistemelor informatice;

**(iii)** copia certificatului de auditor IT, semnată pentru conformitate cu originalul, care dovedește experiența în domeniul de audit extern al sistemelor informatice;"

12. La articolul 10 alineatul (9), după **punctul (vii)** al literei j), se introduce un nou punct, **punctul (viii)**, cu următorul cuprins:

" **(viii)** descrierea modului prin care s-a efectuat auditarea evaluării prevăzute la art. 5 alin. (1)."

13. La articolul 10 alineatul (9), **litera o)** se modifică și va avea următorul cuprins:

" **o)** declarația pe propria răspundere a auditorului IT extern cu privire la faptul că acesta nu se află în relații cu entitatea auditată, cu membrii structurii de conducere sau cu angajații acesteia care ar putea să îi afecteze independența sau obiectivitatea activității de audit."

14. La articolul 11 alineatul (1), **litera a)** se modifică și va avea următorul cuprins:

" **a)** permit respectarea de către entitate a prevederilor prezentei norme, astfel încât, prin externalizarea activităților, să nu se înregistreze nicio evitare a conformării cu prevederile normei;"

15. La articolul 11 **alineatul (4)**, partea introductivă și **punctele (i) și (iv)** ale literei c) se modifică și vor avea următorul cuprins:

" **c)** acte doveditoare în funcție de tipul serviciului sau activității desfășurate, astfel:

**(i)** pentru toți furnizorii - SR ISO/IEC 27001 sau certificări pentru standarde echivalente;

.....

**(iv)** pentru furnizarea de servicii de găzduire sau externalizare prin intermediul centrelor de date - respectarea condițiilor tehnice conform TIA-942 nivel 2 sau echivalent;"

16. La **articolul 14**, după **alineatul (5)** se introduce un nou alineat, **alineatul (6)**, cu următorul cuprins:

" **(6)** Rapoartele prevăzute la alin. (3) se depun la A.S.F. conform sistemului de raportare comunicat de fiecare structură organizatorică din cadrul A.S.F. cu atribuții de supraveghere a entității respective."

17. **Articolul 15** se modifică și va avea următorul cuprins:

" **Art. 15.** Nerespectarea prevederilor prezentei norme de către entitățile prevăzute la art. 2 constituie contravenție conform prevederilor art. 39 alin. (2) lit. a) din Legea nr. 32/2000 privind activitatea și supravegherea intermediarilor în asigurări și reasigurări, cu modificările și completările ulterioare, ale art. 163 alin. (1) lit. a) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, ale art. 272 alin. (1) lit. a) pct. 6, lit. b) pct. 5, lit. c) pct. 4, lit. d) pct. 4, lit. e) pct. 7, lit. f) pct. 3, lit. h) pct. 8, lit. i) pct. 3, lit. j) pct. 17 și lit. k) pct. 3 din Legea nr. 297/2004, cu modificările și completările ulterioare, ale art. 141 alin. (1) lit. g) din Legea nr. 411/2004 privind fondurile de pensii administrate privat, cu modificările și completările ulterioare, respectiv ale art. 121 alin. (1) lit. k) din Legea nr. 204/2006 privind pensiile facultative, cu modificările și completările ulterioare, în funcție de tipul entității."

18. La articolul 16, **alineatul (4)** se modifică și va avea următorul cuprins:

" **(4)** Pentru toate entitățile, prima auditare IT se realizează astfel încât raportul auditorului IT extern să fie transmis către A.S.F. cel mai târziu până la data de 31 decembrie 2016."

19. La **articolul 16**, după **alineatul (4)** se introduce un nou alineat, **alineatul (5)**, cu următorul cuprins:

" **(5)** Prin excepție de la prevederile alin. (1)-(4), Fondul de garantare a asiguraților și Fondul de garantare a drepturilor din sistemul de pensii private efectuează primele raportări începând cu anul 2018, pentru anul 2017, în termenele prevăzute la art. 14."

**Art. II. (1)** Auditorii IT externi care au depus documentația pentru avizare înainte de data intrării în vigoare a prezentei norme vor fi avizați conform prevederilor normei în vigoare la data depunerii cererii. Auditorii IT externi care sunt avizați și înscriși în Registrul public al Autorității de Supraveghere Financiară (A.S.F.)

înainte de data intrării în vigoare a prezentei norme pot să presteze servicii pentru entitățile supravegheate de către A.S.F.

(2) Auditorul IT extern care este avizat de către A.S.F. și își manifestă intenția de a presta servicii și pentru entități din cadrul altui/altor sector/sectoare decât cel/cele pentru care este înscris în Registrul public al A.S.F. are obligația să transmită o notificare către A.S.F. în care să menționeze sectorul/sectoarele în care sunt autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către A.S.F. respectivele entități.

(3) În baza notificării menționate la alin. (2) auditorul IT extern va putea presta servicii numai după înscrierea acestuia în Registrul public al A.S.F. în secțiunea aferentă sectorului/sectoarelor menționat/menționate în notificare.

**Art. III.** Prezenta normă se publică în Monitorul Oficial al României, Partea I, precum și în Buletinul A.S.F., și intră în vigoare la data publicării acesteia.

Președintele Autorității de Supraveghere  
Financiară,  
Mișu Negrițoiu

București, 16 decembrie 2016.

Nr. 40.