Autoritatea de Supraveghere Financiară - ASF

Norma nr. 40/2016
pentru modificarea şi completarea Normei Autorităţii de Supraveghere Financiară nr. 6/2015 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de Autoritatea de Supraveghere Financiară

În vigoare de la 23 decembrie 2016
Publicat în Monitorul Oficial, Partea I nr. 1040 din 23 decembrie 2016.
Nu există modificări până la 28 decembrie 2016.

În urma deliberărilor Consiliului Autorităţii de Supraveghere Financiară din cadrul şedinţei din data de 14 decembrie 2016,

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

Autoritatea de Supraveghere Financiară emite următoarea normă:

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

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

" **Art. 1. -** (1) Prezenta normă stabileşte cerinţele la nivelul entităţilor autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară, denumită în continuare A.S.F., pentru identificarea, prevenirea şi reducerea impactului potenţial negativ al riscurilor operaţionale generate de utilizarea tehnologiei informaţiei şi comunicaţiilor la nivel de oameni, procese, sisteme şi mediu extern, inclusiv de fapte ce ţin de criminalitatea informatică."

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

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

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

" **b)** societăţi de administrare a investiţiilor (SAI), administratori de fonduri de investiţii alternative (AFIA), după cum urmează:".

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

" **f)** Fondul de compensare a investitorilor, Fondul de garantare a asiguraţilor şi Fondul de garantare a drepturilor din sistemul de pensii private;".

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

" (4) Încadrarea, respectiv reîncadrarea entităţilor menţionate 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 entităţilor menţionate la art. 2 lit. d) se realizează în luna ianuarie a fiecărui an calendaristic, în baza activităţii autorizate de A.S.F şi a deţinerii calităţii 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 şi investitorilor lor accesul la platforme electronice de distribuire a titlurilor de participare asigură cel puţin, fără a se limita la:

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

b) mecanisme care să garanteze nerepudierea datelor transmise şi recepţionate;

c) jurnalizarea în timp real a informaţiei despre instrucţiunile investitorilor transmise;

d) mecanisme de nerepudiere a integrităţii înregistrării operaţiunilor de sistem informatic."

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

" (9) Contractul menţionat la alin. (7) trebuie să conţină 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 şi de comunicaţii utilizat de entitate şi care:".

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

" (10) Contractul prevăzut la alin. (7) trebuie să conţină 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 şi va avea următorul cuprins:

" (2) În vederea obţinerii avizului A.S.F., auditorul IT extern depune la A.S.F. o cerere, în care menţionează sectorul/sectoarele în care sunt autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către A.S.F. entităţile pentru care intenţionează să presteze servicii, însoţită de documentaţia care trebuie să cuprindă următoarele, după caz:".

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

" (v) dovada experienţei şi a specializării pe domeniul de audit extern al sistemelor informatice;".

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

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

(iii) copia certificatului de auditor IT, semnată pentru conformitate cu originalul, care dovedeşte experienţa 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 şi va avea următorul cuprins:

" **o)** declaraţia pe propria răspundere a auditorului IT extern cu privire la faptul că acesta nu se află în relaţii cu entitatea auditată, cu membrii structurii de conducere sau cu angajaţii acesteia care ar putea să îi afecteze independenţa sau obiectivitatea activităţii de audit."

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

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

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

" **c)** acte doveditoare în funcţie de tipul serviciului sau activităţii desfăşurate, astfel:

(i) pentru toţi 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 condiţiilor 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 atribuţii de supraveghere a entităţii respective."

17. Articolul 15 se modifică şi va avea următorul cuprins:

" **Art. 15. -** Nerespectarea prevederilor prezentei norme de către entităţile prevăzute la art. 2 constituie contravenţie conform prevederilor art. 39 alin. (2) lit. a) din Legea nr. 32/2000 privind activitatea şi supravegherea intermediarilor în asigurări şi reasigurări, cu modificările şi completările ulterioare, ale art. 163 alin. (1) lit. a) din Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi 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 şi lit. k) pct. 3 din Legea nr. 297/2004, cu modificările şi completările ulterioare, ale art. 141 alin. (1) lit. g) din Legea nr. 411/2004 privind fondurile de pensii administrate privat, cu modificările şi completările ulterioare, respectiv ale art. 121 alin. (1) lit. k) din Legea nr. 204/2006 privind pensiile facultative, cu modificările şi completările ulterioare, în funcţie de tipul entităţii."

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

" (4) Pentru toate entităţile, 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 excepţie de la prevederile alin. (1)-(4), Fondul de garantare a asiguraţilor şi 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 documentaţia pentru avizare înainte de data intrării în vigoare a prezentei norme vor fi avizaţi conform prevederilor normei în vigoare la data depunerii cererii. Auditorii IT externi care sunt avizaţi şi înscrişi în Registrul public al Autorităţii de Supraveghere Financiară (A.S.F.) înainte de data intrării în vigoare a prezentei norme pot să presteze servicii pentru entităţile supravegheate de către A.S.F.

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

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

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

Preşedintele Autorităţii de Supraveghere Financiară,
Mişu Negriţoiu

Bucureşti, 16 decembrie 2016.
Nr. 40.