



MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 194 (XXXVIII) — Nr. 11

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Luni, 12 ianuarie 2026

SUMAR

<u>Nr.</u>	<u>Pagina</u>
DECIZII ALE CURȚII CONSTITUȚIONALE	
Decizia nr. 194 din 8 aprilie 2025 referitoare la excepția de neconstituționalitate a dispozițiilor art. 396 alin. (10) din Codul de procedură penală	2–4
HOTĂRĂRI ALE GUVERNULUI ROMÂNIEI	
1.172/2025. — Hotărâre privind actualizarea denumirii, codului de clasificare și valorilor de inventar, după caz, pentru bunurile imobile aflate în domeniul public al statului și în administrarea Stațiunii de Cercetare-Dezvoltare pentru Cartof Târgu Secuiesc din subordinea Academiei de Științe Agricole și Silvicultură „Gheorghe Ionescu Șişești”	4–5
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE	
3.360/2025. — Decizie a președintelui Agenției Naționale Pentru Mediu și Aree Protejate privind aprobarea Planului de management al sitului Natura 2000 ROSCI0345 Pajiștea Cenad	6
ACTE ALE AUTORITĂȚII DE SUPRAVEGHERE FINANCIARĂ	
26/2025. — Normă pentru aplicarea Ghidului privind externalizarea către furnizorii de servicii cloud	7–13
ACTE ALE AUTORITĂȚII ELECTORALE PERMANENTE	
18.197/2025. — Raport privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul Câmpina Curată	14
18.550/2025. — Raport privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul Republican Conservator în anul 2025	14
20.000/2025. — Raport privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul Arădenilor în anul 2025	15
20.042/2025. — Raport privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul România în Acțiune	15
20.791/2025. — Raport privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul SOS România în anii 2023 și 2024	16

DECIZII ALE CURȚII CONSTITUȚIONALE

CURTEA CONSTITUȚIONALĂ

DECIZIA Nr. 194

din 8 aprilie 2025

referitoare la excepția de neconstituționalitate a dispozițiilor art. 396 alin. (10) din Codul de procedură penală

Marian Enache	— președinte
Mihaela Ciochină	— judecător
Cristian Deliorga	— judecător
Dimitrie-Bogdan Licu	— judecător
Laura-Iuliana Scânteii	— judecător
Gheorghe Stan	— judecător
Livia Doina Stanciu	— judecător
Elena-Simina Tănăsescu	— judecător
Varga Attila	— judecător
Daniela Ramona Marițiu	— magistrat-asistent

Cu participarea reprezentantei Ministerului Public, procuror Nicoleta-Ecaterina Eucarie.

1. Pe rol se află soluționarea excepției de neconstituționalitate a dispozițiilor art. 396 alin. (10) din Codul de procedură penală, excepție ridicată de Iulian Constantin Siminiceanu în Dosarul nr. 3.516/62/2020 al Tribunalului Brașov — Secția penală. Excepția formează obiectul Dosarului Curții Constituționale nr. 1.663D/2021.

2. La apelul nominal se constată lipsa părților. Procedura de înștiințare este legal îndeplinită. Magistratul-asistent referă asupra cererii depuse la dosar de către autorul excepției prin care acesta solicită judecarea în lipsă.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantei Ministerului Public, care pune concluzii de respingere, ca inadmisibilă, a excepției de neconstituționalitate. Arată că autorul acesteia nu formulează o veritabilă critică, ci este nemulțumit de modul de interpretare și aplicare a normelor criticate. În subsidiar, invocând Decizia nr. 775 din 18 noiembrie 2021, solicită respingerea, ca neîntemeiată, a excepției de neconstituționalitate.

CURTEA,

având în vedere actele și lucrările dosarului, reține următoarele:

4. Prin Încheierea din 27 aprilie 2021, pronunțată în Dosarul nr. 3.516/62/2020, **Tribunalul Brașov — Secția penală a sesizat Curtea Constituțională cu excepția de neconstituționalitate a dispozițiilor art. 396 alin. (10) din Codul de procedură penală**, excepție ridicată de Iulian Constantin Siminiceanu, într-o cauză penală în care s-a solicitat aplicarea procedurii simplificate de judecată.

5. În **motivarea excepției de neconstituționalitate**, autorul acesteia susține că dispozițiile criticate instituie un tratament penal mai favorabil — reducerea limitelor de pedeapsă prevăzute de lege — inculpaților trimiși în judecată pentru săvârșirea unor infracțiuni care, prin declarațiile furnizate în fața instanței, recunosc comiterea faptelor de care sunt acuzați. Astfel, dispoziția de lege criticată este aplicabilă numai inculpaților care, chiar dacă nu doresc să recunoască în

integralitate acuzațiile, formulează, în mod formal, o cerere de judecare a cauzei în procedura simplificată. Inculpatul care formulează cu rea-credință o cerere vădit inadmisibilă, doar pentru a-și asigura posibilitatea accesării unei norme ce îi poate aduce beneficii sub forma reducerii limitelor de pedeapsă, beneficiază de un tratament preferențial față de inculpatul care are o conduită procesuală onestă și dorește o recunoaștere parțială.

6. Apreciază că instanța de contencios constituțional trebuie să admită excepția de neconstituționalitate și să stabilească că textul de lege criticat este constituțional în măsura în care reducerea limitelor de pedeapsă se aplică atunci când starea de fapt reținută de instanță în urma cercetării judecătorești este cea recunoscută de inculpat, indiferent de formularea în mod expres a unei cereri de judecare potrivit procedurii recunoașterii învinuirii de către acesta și de soluția dată asupra acestei cereri.

7. **Tribunalul Brașov — Secția penală** apreciază că reducerea limitelor speciale de pedeapsă ca urmare a recunoașterii învinuirii nu poate fi convertită într-un drept fundamental, ci reprezintă un beneficiu acordat de legiuitor, potrivit politicii sale penale, în anumite condiții, printre care se numără și recunoașterea în totalitate a faptelor reținute în sarcina inculpatului, tocmai caracterul integral al recunoașterii învinuirii fiind cel care face inutilă efectuarea cercetării judecătorești, așa cum aceasta este reglementată de dispozițiile art. 374 alin. (5)-(10) din Codul de procedură penală. Instanța judecătorească arată că de beneficiul reducerii limitelor de pedeapsă se bucură și inculpatul căruia i-a fost respinsă cererea de parcurgere a procedurii simplificate, dar, în urma cercetării judecătorești, instanța reține aceeași situație de fapt cu cea descrisă de inculpat. Cu privire la critica referitoare la încălcarea prevederilor art. 16 din Constituție, instanța judecătorească apreciază că, potrivit jurisprudenței Curții Constituționale, principiul egalității în drepturi presupune instituirea unui tratament egal pentru situații care, în funcție de scopul urmărit, nu sunt diferite. Așa fiind, situația procesuală descrisă de inculpat poate crea oportunități de discriminare între cei care solicită formal parcurgerea procedurii simplificate (dar în declarația dată în fața instanței nu recunosc în totalitate situația de fapt așa cum a fost descrisă în rechizitoriu și prezintă propria versiune, astfel că cererea este respinsă) și cei care, *ab initio*, declară că nu recunosc situația de fapt descrisă în rechizitoriu, ci prezintă o versiune proprie, care este însoțită de instanță în urma cercetării judecătorești. Scopul reducerii cu o treime a limitelor de pedeapsă în prima ipoteză este acela de a valorifica poziția procesuală de recunoaștere parțială, recunoaștere confirmată de ansamblul probatoriu administrat, finalitate care ar trebui cuantificată cu aceeași măsură procesuală și în cazul în

care inculpatul, constatând că nu este de acord cu toate acuzațiile formulate în actul de sesizare, declară că nu dorește să parcurgă procedura simplificată, instanța reținând la final situația de fapt expusă de inculpat. În concluzie, instanța judecătorească apreciază că un tratament diferit nu poate fi doar expresia aprecierii exclusive a legiuitorului, ci trebuie să se justifice rațional, în respectul principiului egalității cetățenilor în fața legii și a autorităților publice.

8. Potrivit prevederilor art. 30 alin. (1) din Legea nr. 47/1992, încheierea de sesizare a fost comunicată președinților celor două Camere ale Parlamentului, Guvernului și Avocatului Poporului, pentru a-și exprima punctele de vedere asupra excepției de neconstituționalitate.

9. **Președinții celor două Camere ale Parlamentului, Guvernul și Avocatul Poporului** nu au comunicat punctele lor de vedere asupra excepției de neconstituționalitate.

CURTEA,

examinând încheierea de sesizare, raportul întocmit de judecătorul-raportor, concluziile procurorului, dispozițiile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

10. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art. 146 lit. d) din Constituție, precum și ale art. 1 alin. (2), ale art. 2, 3, 10 și 29 din Legea nr. 47/1992, să soluționeze excepția de neconstituționalitate.

11. **Obiectul excepției de neconstituționalitate** îl constituie dispozițiile art. 396 alin. (10) din Codul de procedură penală, cu următorul conținut: *„Când judecata s-a desfășurat în condițiile art. 375 alin. (1), (1¹) și (2), când cererea inculpatului ca judecata să aibă loc în aceste condiții a fost respinsă sau când cercetarea judecătorească a avut loc în condițiile art. 377 alin. (5) ori art. 395 alin. (2), iar instanța reține aceeași situație de fapt ca cea recunoscută de către inculpat, în caz de condamnare sau amânare a aplicării pedepsei, limitele de pedeapsă prevăzute de lege în cazul pedepsei închisorii se reduc cu o treime, iar în cazul pedepsei amenzii, cu o pătrime. Pentru inculpații minori, instanța va avea în vedere aceste aspecte la alegerea măsurii educative; în cazul măsurilor educative privative de libertate, limitele perioadelor pe care se dispun aceste măsuri, prevăzute de lege, se reduc cu o treime.”*

12. Autorul excepției susține că textul criticat contravine prevederilor constituționale cuprinse în art. 1 alin. (5) referitor la cerințele de calitate a legii și art. 16 alin. (1) și (2) referitor la egalitatea în drepturi.

13. Examinând excepția de neconstituționalitate Curtea reține că s-a mai pronunțat asupra constituționalității dispozițiilor de lege criticate, dintr-o perspectivă identică, de exemplu, prin Decizia nr. 220 din 17 aprilie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 523 din 26 iunie 2018, Decizia nr. 484 din 23 iunie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 603 din 10 august 2015, Decizia nr. 726 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 887 din 26 noiembrie 2015, Decizia nr. 753 din 13 decembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 95 din 2 februarie 2017, și Decizia nr. 723 din 6 decembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 263 din 13 aprilie 2017.

14. Cu acele prilejuri, Curtea a reținut că procedura simplificată de judecată în cazul recunoașterii învinuirii nu constituie o noutate în materie procesual penală, fiind reglementată pentru prima dată de dispozițiile art. 320¹ din vechiul Cod de procedură penală — introduse prin Legea nr. 202/2010 privind unele măsuri pentru accelerarea soluționării proceselor —, cu titlul de derogare de la dreptul comun, ce presupune soluționarea cu celeritate a unor cauze penale pentru care cercetarea judecătorească propriu-zisă devine redundantă, întrucât în faza de urmărire penală au fost dezlegate toate aspectele legate de existența infracțiunii și de vinovăția inculpatului.

15. Curtea a statuat că reducerea limitelor speciale de pedeapsă ca urmare a recunoașterii învinuirii nu poate fi convertită într-un drept fundamental, ci reprezintă un beneficiu acordat de legiuitor, potrivit politicii sale penale, în anumite condiții, printre care se numără și recunoașterea în totalitate a faptelor reținute în sarcina inculpatului, tocmai caracterul integral al recunoașterii învinuirii fiind cel care face inutilă efectuarea cercetării judecătorești, așa cum este reglementată aceasta de dispozițiile art. 374 alin. (5)-(10) din actualul Cod de procedură penală. Având în vedere efectele procedurii de judecată simplificate, instanța poate respinge, în baza unor criterii obiective și rezonabile, cererea formulată de inculpat, întrucât, indiferent că recunoașterea învinuirii este totală sau parțială, ceea ce prevalează este existența unui proces echitabil, despre care nu se poate vorbi în măsura în care se neagă principiul aflării adevărului. Prin urmare, nu simpla recunoaștere a învinuirii, chiar și integrală, este determinantă pentru a se da eficiență unui proces echitabil desfășurat în limitele legalității și imparțialității, aceasta constituind doar o condiție procedurală, ci stabilirea vinovăției inculpatului cu privire la faptele reținute în sarcina sa.

16. De altfel, având în vedere tocmai riscul exercitării de presiuni asupra inculpatului spre a-și recunoaște vinovăția și cu privire la fapte pe care nu le-a săvârșit, posibilitatea instanței de a respinge cererea de judecare a cauzei potrivit procedurii simplificate constituie o garanție a dreptului la un proces echitabil, consacrat de art. 21 alin. (3) din Constituție și de art. 6 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale. Judecătorul nu este obligat, în absența convingerii cu privire la sinceritatea inculpatului — chiar dacă acesta recunoaște în totalitate faptele reținute în sarcina sa —, să admită cererea formulată de inculpat, ceea ce reprezintă o materializare a principiului constituțional al înfăptuirii justiției de către instanțele judecătorești, consacrat de art. 124 din Legea fundamentală. Prin urmare, instanța are posibilitatea să respingă cererea inculpatului, chiar și în condițiile unei recunoașteri totale a faptelor reținute în sarcina sa, atunci când nu este lămurită asupra împrejurărilor de fapt ale cauzei și consideră că judecata nu poate avea loc numai în baza probelor administrate în faza de urmărire penală, ci trebuie să se facă potrivit dreptului comun.

17. Întrucât nu au intervenit elemente noi, de natură să justifice reconsiderarea jurisprudenței în materie, Curtea apreciază că soluțiile și considerentele mai sus amintite își păstrează valabilitatea și în prezenta cauză.

18. Pentru considerentele expuse mai sus, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, precum și al art. 1-3, al art. 11 alin. (1) lit. A.d) și al art. 29 din Legea nr. 47/1992, cu unanimitate de voturi,

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Respinge, ca neîntemeiată, excepția de neconstituționalitate ridicată de Iulian Constantin Siminiceanu în Dosarul nr. 3.516/62/2020 al Tribunalului Brașov — Secția penală și constată că dispozițiile art. 396 alin. (10) din Codul de procedură penală sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Tribunalului Brașov — Secția penală și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 8 aprilie 2025.

PREȘEDINTELE CURȚII CONSTITUȚIONALE

pentru **MARIAN ENACHE**,

în temeiul art. 426 alin. (4)

din Codul de procedură civilă coroborat

cu art. 14 din Legea nr. 47/1992

privind organizarea și funcționarea Curții Constituționale,

semnează

ELENA-SIMINA TĂNĂSESCU

Magistrat-asistent,

Daniela Ramona Marițiu

HOTĂRÂRI ALE GUVERNULUI ROMÂNIEI

GUVERNUL ROMÂNIEI

HOTĂRÂRE

privind actualizarea denumirii, codului de clasificare și valorilor de inventar, după caz, pentru bunurile imobile aflate în domeniul public al statului și în administrarea Stațiunii de Cercetare-Dezvoltare pentru Cartof Târgu Secuiesc din subordinea Academiei de Științe Agricole și Silvicultură „Gheorghe Ionescu Șişești”

Având în vedere art. 21 și 22 din Ordonanța Guvernului nr. 81/2003 privind reevaluarea și amortizarea activelor fixe aflate în patrimoniul instituțiilor publice, aprobată prin Legea nr. 493/2003, cu modificările și completările ulterioare,

în temeiul art. 108 din Constituția României, republicată, și al art. 288 alin. (1) din Ordonanța de urgență a Guvernului nr. 57/2019 privind Codul administrativ, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. 1. — Se aprobă actualizarea denumirii, codului de clasificare și valorilor de inventar, după caz, pentru bunurile imobile aflate în domeniul public al statului și în administrarea Stațiunii de Cercetare-Dezvoltare pentru Cartof Târgu Secuiesc din subordinea Academiei de Științe Agricole și Silvicultură „Gheorghe Ionescu Șişești”, potrivit anexei care face parte integrantă din prezenta hotărâre.

Art. 2. — Ministerul Agriculturii și Dezvoltării Rurale, împreună cu Ministerul Finanțelor, va opera în mod corespunzător datele din anexa nr. 3 la Hotărârea Guvernului nr. 1.705/2006 pentru aprobarea inventarului centralizat al bunurilor din domeniul public al statului, cu modificările și completările ulterioare.

PRIM-MINISTRU

ILIE-GAVRIL BOLOJAN

Contrasemnează:

Viceprim-ministru,

Marian Neacșu

Ministrul agriculturii și dezvoltării rurale,

Florin-Ionuț Barbu

p. Ministrul finanțelor,

Mihai Diaconu,

secretar de stat

DATELE DE IDENTIFICARE

ale bunurilor aflate în domeniul public al statului și în administrarea Stațiunii de Cercetare-Dezvoltare pentru Cartof Târgu Secuiesc, pentru care se modifică denumirea, codul de clasificare și valoarea de inventar, după caz

Nr. crt.	Nr. MF	Codul de clasificare	Denumirea	Elementele-cadru de descriere tehnică	Adresa	Valoarea de inventar (lei)	Data la care bunul este înregistrat cu valoarea de inventar din col. 6 în evidența financiar-contabilă	Titularul dreptului de administrare și ordonatorul principal de credite (denumirea și codul fiscal)
0	1	2	3	4	5	6	7	8
1	102098	8.28.13	Atelier mecanic	Suprafața construită = 229 mp; suprafața desfășurată = 273 mp; regimul de înălțime = P + 1E; CF = 29642-C16	Țara: România; județul Covasna; municipiul Târgu Secuiesc; DN 11 km 5	358.010	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
2	102105	8.28.13	Magazie materiale, unelte	Suprafață construită = 395 mp; suprafața desfășurată = 395 mp; regimul de înălțime = parter; CF = 29642-C6	Țara: România; județul Covasna; municipiul Târgu Secuiesc; DN 11 km 5	463.195	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
3	102111	8.29.08	Sediu administrativ	Suprafața construită = 296 mp; suprafața desfășurată = 592 mp; regimul de înălțime = P + 1E; CF = 29641-C1	Țara: România; județul Covasna; municipiul Târgu Secuiesc; str. Orbán Balazs nr. 15	1.049.702	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
4	102119	8.28.10	Magazie pentru cereale și alte produse	Suprafața construită = 246 mp; suprafața desfășurată = 246 mp; regimul de înălțime = parter; CF = 29642-C17	Țara: România; județul Covasna; municipiul Târgu Secuiesc; DN 11, km 5	18.746	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
5	102121	8.28.03	Laborator cercetare	Suprafața construită = 552 mp; suprafața desfășurată = 552 mp; regimul de înălțime = parter; CF = 29644-C1	Țara: România; județul Covasna; municipiul Târgu Secuiesc; str. Orbán Balazs nr. 15	2.604.291	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
6	102122	8.27.01	Depozit de cartof pentru cercetare	Suprafața construită = 390 mp; suprafața desfășurată = 390 mp; regimul de înălțime = parter; CF = 29645-C1	Țara: România; județul Covasna; municipiul Târgu Secuiesc; str. Budai Nagy Antal	406.393	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
7	102126	8.05.03	Suprafață totală de teren	Suprafețe = 3650852 mp; CF = 24476, 26641, 29639, 29640, 29641, 29642, 29643, 29644, 29645, 29646, 29654, 29655, 29734, 29735, 29736, 29737	Țara: România; județul Covasna; municipiul Târgu Secuiesc	36.210.603	1.01.2025	Denumire unitate: SCDC Târgu Secuiesc CUI 14829298 Ministerul Agriculturii și Dezvoltării Rurale CUI 4221187
TOTAL						41.110.940		

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

AGENȚIA NAȚIONALĂ PENTRU MEDIU ȘI ARII PROTEJATE

DECIZIE

privind aprobarea Planului de management al sitului Natura 2000 ROSCI0345 Pajiștea Cenad

Având în vedere Referatul de aprobare nr. 60 din 3.12.2025 al Direcției generale arii naturale, biodiversitate și conservarea naturii, Serviciul arii naturale protejate și emitere avize,

ținând cont de Decizia etapei de încadrare nr. 113 din 14.08.2025, emisă de către Direcția Județeană de Mediu Timiș, reconfirmată prin Adresa nr. 5.755/AAA/633/BANP din 11.11.2025, emisă de către Direcția Județeană de Mediu Timiș,

în temeiul prevederilor art. 2 alin. (5) din Hotărârea Guvernului nr. 311/2025 privind organizarea și funcționarea Agenției Naționale pentru Mediu și Arii Protejate, precum și ale art. 21 alin. (2) din Ordonanța de urgență a Guvernului nr. 57/2007 privind regimul ariilor naturale protejate, conservarea habitatelor naturale, a florei și faunei sălbatice, aprobată cu modificări și completări prin Legea nr. 49/2011, cu modificările și completările ulterioare,

președintele Agenției Naționale pentru Mediu și Arii Protejate emite prezenta decizie.

Art. 1. — Se aprobă Planul de management al sitului Natura 2000 ROSCI0345 Pajiștea Cenad, prevăzut în anexa*) care face parte integrantă din prezenta decizie.

Art. 2. — Prezenta decizie se publică în Monitorul Oficial al României, Partea I.

Președintele Agenției Naționale Pentru Mediu și Arii Protejate,
Raluca Giorgiana Dumitrescu

București, 5 decembrie 2025.

Nr. 3.360.

*) Anexa se publică în Monitorul Oficial al României, Partea I, nr. 11 bis, care se poate achiziționa de la Centrul pentru relații cu publicul din șos. Panduri nr. 1, bloc P33, parter, sectorul 5, București.

ACTE ALE AUTORITĂȚII DE SUPRAVEGHERE FINANCIARĂ

AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

NORMĂ

pentru aplicarea Ghidului privind externalizarea către furnizorii de servicii cloud

În temeiul prevederilor art. 2 alin. (1) lit. a) și d) și alin. (5), art. 3 alin. (1) lit. b), 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, potrivit deliberărilor din ședința Consiliului Autorității de Supraveghere Financiară din data de 3.12.2025,

Autoritatea de Supraveghere Financiară emite prezenta normă.

Art. 1. — Autoritatea de Supraveghere Financiară, denumită în continuare A.S.F., aplică Ghidul privind externalizarea către furnizorii de servicii cloud (ESMA65-294529287-4737), denumit în continuare *Ghidul ESMA*, prevăzut în anexa care face parte integrantă din prezenta normă.

Art. 2. — Entitățile prevăzute la punctul 1.1. din Ghidul ESMA care intră în competența de autorizare/avizare, reglementare, supraveghere și control a A.S.F. respectă prevederile prezentei norme.

Art. 3. — Entitățile prevăzute la pct. 1.1 din Ghidul Esma notifică A.S.F., în scris, informații referitoare la:

a) angajamentul planificat de externalizare în cloud care vizează o funcție critică sau importantă, în termen de 5 zile de la data planificării;

b) angajamentele de externalizare în cloud care privesc o funcție care anterior a fost clasificată ca fiind necritică sau neimportantă, în termen de 5 zile de la data încheierii acestora.

Art. 4. — În cazul în care informațiile și/sau documentele prezentate de entitățile prevăzute la pct. 1.1 din Ghidul Esma nu sunt suficiente sau relevante pentru realizarea evaluării riscurilor care decurg din angajamentele de externalizare în cloud, A.S.F. poate solicita orice informații sau documente suplimentare în cadrul procesului de supraveghere.

Art. 5. — (1) Prelucrarea datelor cu caracter personal de către A.S.F./entitățile prevăzute la pct. 1.1 din Ghidul Esma se realizează în conformitate cu prevederile prezentei norme, ale Regulamentului (U.E.) nr. 679/2016 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția

datelor) și ale altor prevederi legale în vigoare în domeniul protecției datelor cu caracter personal.

(2) A.S.F. cooperează cu Autoritatea Europeană pentru Valori Mobiliare și Piețe/alte autorități competente, cu respectarea legislației aplicabile referitoare la prelucrarea datelor cu caracter personal și libera circulație a acestor date, în legătură cu schimbul de informații pe care le deține sau pe care solicită să le primească în scopul evaluării modului de conformare cu prevederile prezentei norme.

Art. 6. — În situația în care informațiile și documentele prevăzute de prezenta normă se transmit A.S.F. doar în format electronic, acestea sunt semnate cu semnătura electronică calificată a reprezentantului legal al entității.

Art. 7. — Nerespectarea prevederilor prezentei norme se sancționează potrivit dispozițiilor titlului I cap. VII din Ordonanța de urgență a Guvernului nr. 32/2012 privind organismele de plasament colectiv în valori mobiliare și societățile de administrare a investițiilor, precum și pentru modificarea și completarea Legii nr. 297/2004 privind piața de capital, aprobată cu modificări și completări prin Legea nr. 10/2015, cu modificările și completările ulterioare, ale art. 51-57 din Legea nr. 74/2015 privind administratorii de fonduri de investiții alternative, cu modificările și completările ulterioare, sau potrivit prevederilor titlului III din Legea nr. 243/2019 privind reglementarea fondurilor de investiții alternative și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare, după caz.

Art. 8. — (1) Prezenta normă se publică în Monitorul Oficial al României, Partea I, și intră în vigoare la data publicării acesteia.

(2) La data intrării în vigoare a prezentei norme se abrogă Norma Autorității de Supraveghere Financiară nr. 21/2021 pentru aplicarea Ghidului privind externalizarea către furnizorii de servicii cloud, publicată în Monitorul Oficial al României, Partea I, nr. 869 din 10 septembrie 2021.

Președintele Autorității de Supraveghere Financiară,

Alexandru Petrescu

București, 18 decembrie 2025.

Nr. 26.

ANEXĂ

G H I D

privind externalizarea către furnizorii de servicii cloud

1. Domeniul de aplicare

Cui i se adresează?

1. Prezentul ghid se aplică autorităților competente și (i) depozitarilor fondurilor de investiții alternative (FIA) menționați la art. 21 alin. (3) lit. (c) și la art. 21 alin. (3) al treilea paragraf din Directiva AFIA, în cazul în care aceștia nu sunt entități financiare cărora li se aplică DORA, și (ii) depozitarilor organismelor de plasament colectiv în valori mobiliare (OPCVM) menționați la

art. 23 alin. (2) lit. (c) din Directiva OPCVM, în cazul în care aceștia nu sunt entități financiare cărora li se aplică DORA.¹

Ce se aplică?

2. Prezentele orientări se aplică în legătură cu următoarele dispoziții:

a) în ceea ce privește depozitarii FIA: art. 21 din Directiva AFIA; art. 98 din Regulamentul delegat (UE) 2013/231 al Comisiei;

¹ În ceea ce privește acordurile de externalizare în cloud, entitățile financiare definite la art. 2 alin. (1) și (2) din Regulamentul (UE) 2022/2.554 al Parlamentului European și al Consiliului privind reziliența operațională digitală pentru sectorul financiar și de modificare a Regulamentelor (CE) nr. 1.060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1.011 (Regulamentul DORA) sunt supuse normelor specifice prevăzute în Regulamentul DORA și în regulamentele delegate și de punere în aplicare ale Comisiei.

b) în ceea ce privește depozitarii OPCVM-urilor: art. 22, 22a și 23 alin. (2) din Directiva OPCVM; art. 32 din Directiva 2010/43/UE a Comisiei; art. 2 alin. (2) lit. (j), art. 3 alin. (1), art. 13 alin. (2), art. 15, 16 și 22 din Regulamentul delegat (UE) 2016/438 al Comisiei.

Când se aplică?

3. Prezentul ghid se aplică de la data publicării sale pe site-ul ESMA în toate limbile oficiale ale UE și tuturor acordurilor de externalizare în cloud încheiate, reînnoite sau modificate la sau după această dată.

4. Având în vedere aplicarea DORA, Orientările anterioare ale ESMA privind externalizarea către furnizorii de servicii de cloud încetează să se aplice entităților financiare care fac obiectul DORA menționate la art. 2 din același regulament. Pentru depozitarii FIA și pentru depozitarii OPCVM-urilor menționați la pct. 1.1, Ghidul ESMA anterior privind externalizarea către furnizorii de servicii de cloud va continua să se aplice până la data publicării prezentului ghid pe site-ul ESMA în toate limbile oficiale ale UE.

2. Referințe legislative, abrevieri și definiții

2.1. Referințe legislative

<i>Regulamentul ESMA</i>	— Regulamentul (UE) nr. 1.095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei ² ;
<i>DAFIA</i>	— Directiva 2011/61/UE a Parlamentului European și a Consiliului din 8 iunie 2011 privind administratorii fondurilor de investiții alternative și de modificare a Directivelor 2003/41/CE și 2009/65/CE și a Regulamentelor (CE) nr. 1.060/2009 și (UE) nr. 1.095/2010 ³ ;
<i>Regulamentul delegat (UE) nr. 231/2013 al Comisiei</i>	— Regulamentul delegat (UE) nr. 231/2013 al Comisiei din 19 decembrie 2012 de completare a Directivei 2011/61/UE a Parlamentului European și a Consiliului în ceea ce privește derogările, condițiile generale de operare, depozitarii, efectul de levier, transparența și supravegherea ⁴ ;
<i>Directiva OPCVM</i>	— Directiva 2009/65/CE a Parlamentului European și a Consiliului din 13 iulie 2009 de coordonare a actelor cu putere de lege și a actelor administrative privind organismele de plasament colectiv în valori mobiliare (OPCVM) ⁵ ;
<i>Directiva 2010/43/UE a Comisiei</i>	— Directiva 2010/43/UE a Comisiei din 1 iulie 2010 de punere în aplicare a Directivei 2009/65/CE a Parlamentului European și a Consiliului în ceea ce privește cerințele organizatorice, conflictele de interese, regulile de conduită, administrarea riscului și conținutul acordului dintre depozitar și societatea de administrare ⁶ ;
<i>DORA</i>	— Regulamentul (UE) 2022/2.554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1.060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1.0117;
<i>RGPD</i>	— Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE ⁸ .

2.2. Abrevieri

<i>FSC</i>	— furnizor de servicii cloud
<i>ESMA</i>	— Autoritatea Europeană pentru Valori Mobiliare și Piețe
<i>UE</i>	— Uniunea Europeană

2.3. Definiții

<i>funcție</i>	— orice procese, servicii sau activități;
<i>funcție critică sau importantă</i>	— orice funcție a cărei anomalie sau deficiență în îndeplinirea sa ar compromite considerabil: a) respectarea de către societate a obligațiilor sale în temeiul legislației aplicabile; b) performanța financiară a unei societăți; sau c) viabilitatea sau continuitatea principalelor servicii și activități ale unei societăți;
<i>servicii cloud</i>	— servicii furnizate utilizând cloud computing;
<i>cloud computing sau cloud⁹</i>	— o paradigmă care permite accesul în rețea la un bazin scalabil și elastic de resurse fizice sau virtuale care pot fi partajate (de exemplu, servere, sisteme de operare, rețele, software, aplicații și echipamente de stocare) cu funcție de autoservice și de administrare la cerere;

² JO L 331, 15.12.2010, p. 84.

³ JO L 174, 1.07.2011, p. 1.

⁴ JO L 83, 22.03.2013, p. 1.

⁵ JO L 302, 17.11.2009, p. 32.

⁶ JO L 176, 10.07.2010, p. 42.

⁷ JO L 333, 27.12.2022, p. 1-79.

⁸ JO L 119, 4.05.2016, p. 1-88.

⁹ Cloud computing este adesea abreviat în „cloud”. Termenul „cloud” este utilizat în restul documentului pentru a facilita lectura.

<i>furnizor de servicii cloud</i>	— un terț care furnizează servicii cloud în cadrul unui angajament de externalizare în cloud;
<i>angajament de externalizare în cloud</i>	— un angajament sub orice formă, inclusiv acorduri de delegare, între: (i) o societate și un FSC prin care respectivul FSC îndeplinește o funcție care altfel ar fi asumată de societatea înseși; sau (ii) o societate și un terț care nu este un FSC, dar care se bazează în mod semnificativ pe un FSC pentru a îndeplini o funcție care altfel ar fi asumată de societatea înseși. În acest caz, o trimitere la un „FSC” în acest ghid trebuie interpretată ca referindu-se la un astfel de terț;
<i>subcontractare a serviciilor externalizate</i>	— o situație în care FSC transferă mai departe funcția externalizată (sau o parte a acestei funcții) către un alt furnizor de servicii în cadrul unui angajament de externalizare;
<i>model de implementare în cloud</i>	— modul în care cloudul poate fi organizat pe baza controlului și partajării resurselor fizice sau virtuale. Modelele de implementare în cloud includ cloudul comunitar ¹⁰ , hibrid ¹¹ , privat ¹² și public ¹³ ;
<i>societăți</i>	— a) depozitarii menționați la art. 21 alin. (3) lit. (c) și la art. 21 alin. (3) al treilea paragraf din Directiva AFIA („depozitari de fonduri de investiții alternative (FIA)”); b) depozitarii menționați la art. 23 alin. (2) lit. (c) din Directiva OPCVM („depozitarii OPCVM-urilor”).

3. Scop

5. Ghidul este elaborat în temeiul art. 16 alin. (1) din Regulamentul ESMA. Obiectivele prezentului ghid sunt de a stabili practici de supraveghere coerente, eficiente și eficace în cadrul Sistemului european de supraveghere financiară (SESF) și de a asigura aplicarea comună, uniformă și consecventă a cerințelor menționate în secțiunea 1.1. de la rubrica „Ce se aplică?” atunci când societățile externalizează către FSC-uri. În special, aceste ghiduri au scopul de a ajuta societățile și autoritățile competente să identifice, să abordeze și să monitorizeze riscurile și provocările care decurg din angajamentele de externalizare în cloud, de la luarea deciziei de externalizare, selectarea unui furnizor de servicii cloud, monitorizarea activităților externalizate până la furnizarea de strategii de ieșire.

4. Conformitate și obligații de raportare

4.1. Statutul orientărilor

6. Conform art. 16 alin. (3) din Regulamentul ESMA, autoritățile competente și societățile trebuie să depună toate eforturile necesare pentru a respecta ghidul.

7. Autoritățile competente cărora li se aplică prezentul ghid trebuie să se conformeze prin includerea lui în cadrele lor juridice și/sau de supraveghere naționale, după caz, inclusiv în cazul în care ghiduri specifice vizează, în principal, societățile. În acest caz, autoritățile competente trebuie să asigure, prin activități de supraveghere, respectarea ghidului de către societăți.

4.2. Cerințe de raportare

8. În termen de două luni de la data publicării ghidului pe site-ul ESMA în toate limbile oficiale ale UE, autoritățile competente cărora li se aplică prezentul ghid trebuie să informeze ESMA (i) dacă respectă ghidul, (ii) dacă nu respectă, dar intenționează să respecte ghidul sau (iii) dacă nu respectă și nu intenționează să respecte ghidul.

9. În caz de neconformitate, autoritățile competente trebuie, de asemenea, să informeze ESMA în termen de două luni de la data publicării ghidului pe site-ul ESMA în toate limbile oficiale ale UE cu privire la motivele de neconformare cu ghidul. Pe site-ul ESMA este disponibil un model de notificare. Odată ce a fost completat, modelul va fi transmis la ESMA.

10. Societățile nu sunt obligate să raporteze dacă respectă sau nu prezentul ghid.

¹⁰ Un model de implementare în cloud în care serviciile cloud acceptă și sunt partajate exclusiv printr-un grup specific de clienți ai serviciilor cloud care au cerințe comune și o relație de reciprocitate și unde resursele sunt controlate de cel puțin un membru al acestui grup.

¹¹ Un model de implementare în cloud care utilizează cel puțin două modele diferite de implementare în cloud.

¹² Un model de implementare în cloud în care serviciile cloud sunt utilizate exclusiv de un singur client de servicii cloud, iar resursele sunt controlate de respectivul client de servicii cloud.

¹³ Un model de implementare în cloud în care serviciile cloud sunt potențial disponibile pentru orice client de servicii cloud, iar resursele sunt controlate de furnizorul de servicii cloud.

5. Ghid privind externalizarea către furnizorii de servicii cloud

Orientarea 1. Guvernanță, supraveghere și documentare

11. O societate trebuie să aibă o strategie de externalizare în cloud definită și actualizată, care să fie compatibilă cu strategiile relevante și cu politicile și procesele interne ale societății, inclusiv în ceea ce privește tehnologia informației și comunicațiilor, securitatea informațiilor și gestionarea riscurilor operaționale.

12. O societate trebuie:

a) să atribuie clar responsabilitățile în cadrul organizației pentru documentarea, gestionarea și controlul angajamentelor de externalizare în cloud;

b) să aloce resurse suficiente pentru a asigura respectarea acestui ghid și a tuturor cerințelor legale aplicabile angajamentelor sale de externalizare în cloud;

c) să instituie o funcție de supraveghere a externalizării în cloud sau să desemneze membri ai personalului de nivel superior care să se afle în directă subordine a organului de conducere și să răspundă de gestionarea și supravegherea riscurilor aranjamentelor de externalizare în cloud. Atunci când respectă acest ghid, societățile trebuie să țină seama de natura, amploarea și complexitatea activității lor, inclusiv în ceea ce privește riscul pentru sistemul financiar și riscurile inerente funcțiilor externalizate, și să se asigure că organul lor de conducere deține competențele tehnice relevante pentru a înțelege riscurile pe care le presupun angajamentele de externalizare în cloud. Societățile mici și mai puțin complexe trebuie să asigure cel puțin o repartizare clară a sarcinilor și responsabilităților pentru gestionarea și supravegherea angajamentelor de externalizare în cloud.

13. O societate trebuie să monitorizeze performanța activităților, măsurile de securitate și respectarea de către FSC-urile sale a nivelurilor de servicii convenite. Această monitorizare trebuie să se bazeze pe riscuri, acordând o atenție deosebită funcțiilor critice sau importante care au fost externalizate.

14. O societate trebuie să reevalueze dacă aranjamentele sale de externalizare în cloud vizează o funcție critică sau importantă, periodic și ori de câte ori riscul, natura sau amploarea unei funcții externalizate s-a modificat substanțial.

15. O societate trebuie să mențină un registru actualizat de informații cu privire la toate angajamentele sale de externalizare în cloud, făcând distincție între externalizarea funcțiilor critice sau importante și alte angajamente de externalizare. Atunci când face distincția între externalizarea funcțiilor critice sau importante și alte angajamente de externalizare, aceasta trebuie să furnizeze un scurt rezumat al motivelor pentru care funcția externalizată este sau nu este considerată critică sau importantă. Ținând seama de legislația națională, o societate trebuie să țină, de asemenea, o evidență a angajamentelor de externalizare în cloud reziliate, pentru o perioadă de timp adecvată.

16. În cazul angajamentelor de externalizare în cloud care vizează funcții critice sau importante, registrul trebuie să conțină cel puțin următoarele informații pentru fiecare angajament de externalizare:

- a) un număr de referință;
- b) data de începere și, după caz, următoarea dată de reînnoire a contractului, data de încetare și/sau perioadele de preaviz pentru FSC și pentru societate;
- c) o scurtă descriere a funcției externalizate, inclusiv datele externalizate și dacă aceste date conțin date cu caracter personal (de exemplu, prin furnizarea unui răspuns de tip „Da” sau „Nu” într-un câmp de date separat);
- d) o categorie atribuită de societate care reflectă natura funcției externalizate (de exemplu, funcția de tehnologia informației, funcția de control), care trebuie să faciliteze identificarea diferitelor tipuri de angajamente de externalizare în cloud;
- e) dacă funcția externalizată sprijină operațiuni de afaceri care sunt critice din punctul de vedere al timpului;
- f) numele și numele de marcă (dacă este cazul) ale FSC, țara sa de înregistrare, numărul de înregistrare, identificatorul entității juridice (dacă este disponibil), adresa sa înregistrată, datele sale de contact relevante, precum și denumirea societății-mamă (dacă este cazul);
- g) legea de reglementare a angajamentului de externalizare în cloud și, dacă există, alegerea jurisdicției;
- h) tipul de servicii cloud și modele de implementare și natura specifică a datelor care trebuie păstrate și locațiile (și anume regiunile sau țările) în care pot fi stocate aceste date;
- i) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate și data următoarei evaluări planificate;
- j) data celei mai recente evaluări a riscului/celui mai recent audit al FSC, împreună cu un scurt rezumat al principalelor rezultate, și data următoarei evaluări planificate/următorului audit planificat;
- k) persoana fizică sau organul de decizie din cadrul societății care a aprobat angajamentul de externalizare în cloud;
- l) dacă este cazul, numele oricărui subcontractant căruia îi este externalizată în lanț o funcție critică sau importantă (sau părți substanțiale ale acesteia), inclusiv țările în care sunt înregistrați subcontractanții, unde va fi prestat serviciul subcontractat, și locațiile (și anume regiunile sau țările) în care vor fi stocate datele;
- m) costul bugetar anual estimat al angajamentului de externalizare în cloud.

17. În cazul angajamentelor de externalizare în cloud referitoare la funcții necritice sau neimportante, o societate trebuie să definească informațiile care trebuie incluse în registru pe baza naturii, amplitudinii și complexității riscurilor inerente funcției externalizate.

Orientarea 2. Analiza de preexternalizare și procesul de diligență

18. Înainte de a încheia orice angajament de externalizare în cloud, o societate trebuie:

- a) să evalueze dacă angajamentul de externalizare în cloud privește o funcție critică sau importantă;

b) să identifice și să evalueze toate riscurile relevante ale angajamentului de externalizare în cloud;

c) să efectueze procesul de diligență corespunzător asupra FSC-ului potențial;

d) să identifice și să evalueze orice conflict de interese pe care îl poate genera externalizarea.

19. Analiza de preexternalizare și procesul de diligență asupra potențialului FSC trebuie să fie proporționale cu natura, amploarea și complexitatea funcției pe care societatea intenționează să o externalizeze și cu riscurile inerente acestei funcții. Aceasta trebuie să conțină cel puțin o evaluare a impactului potențial al angajamentului de externalizare în cloud asupra riscurilor operaționale, juridice, de conformitate și reputaționale ale societății.

20. În cazul în care angajamentul de externalizare în cloud privește funcții critice sau importante, o societate trebuie, de asemenea:

a) să evalueze toate riscurile relevante care pot apărea ca urmare a angajamentului de externalizare în cloud, inclusiv riscurile legate de tehnologia informației și comunicațiilor, de securitatea informațiilor, continuitatea activității, legalitate și conformitate, riscurile reputaționale, riscurile operaționale și posibile limitări în materie de supraveghere pentru societate, care rezultă din:

- (i) serviciul cloud selectat și modelele de implementare propuse;
- (ii) migrația și/sau procesul de implementare;
- (iii) sensibilitatea funcției și a datelor conexe care sunt avute în vedere pentru a fi externalizate și măsurile de securitate care trebuie luate;
- (iv) interoperabilitatea sistemelor și aplicațiilor societății și ale FSC, și anume capacitatea lor de a face schimb de informații și de a utiliza reciproc informațiile care au făcut obiectul unui schimb;
- (v) portabilitatea datelor societății, și anume capacitatea de a transfera cu ușurință datele societății de la un FSC la altul sau înapoi către societate;
- (vi) stabilitatea politică, situația de securitate și sistemul juridic (inclusiv dispozițiile în vigoare în materie de aplicare a legii, dispozițiile legale privind insolvența care s-ar aplica în caz de faliment al FSC, legislația în vigoare privind protecția datelor și îndeplinirea condițiilor pentru transferul datelor cu caracter personal într-o țară terță conform RGPD) în țările (din interiorul sau din afara UE) în care ar fi furnizate funcțiile externalizate și în care ar fi stocate datele externalizate; în cazul subcontractării, riscurile suplimentare care pot apărea dacă subcontractantul se află într-o țară terță sau într-o țară diferită de cea a FSC și, în cazul unui lanț de subcontractare, orice risc suplimentar care poate apărea, inclusiv în legătură cu absența unui contract direct între societate și subcontractantul care realizează funcția externalizată;
- (vii) concentrarea posibilă în cadrul societății (inclusiv, după caz, la nivelul grupului său), cauzată de angajamente multiple de externalizare în cloud cu același FSC, precum și concentrarea posibilă în cadrul sectorului financiar al UE, cauzată de situația în care mai multe societăți folosesc același FSC sau un grup mic de FSC-uri. La evaluarea riscului de concentrare, societatea trebuie să aibă în vedere toate angajamentele sale de externalizare în cloud (și, dacă este cazul, angajamentele de externalizare în cloud la nivelul grupului său) cu respectul FSC;

b) să țină seama de beneficiile și costurile preconizate ale angajamentului de externalizare în cloud, inclusiv cântărirea oricăror riscuri semnificative care pot fi reduse sau mai bine gestionate împotriva oricăror riscuri semnificative care pot apărea ca urmare a angajamentului de externalizare în cloud.

21. În cazul externalizării de funcții critice sau importante, procesul de diligență trebuie să includă o evaluare a adecvării FSC. La evaluarea adecvării FSC, o societate trebuie să se asigure că FSC are o bună reputație în afaceri, deține abilitățile, resursele (de exemplu, resurse umane, informatice și financiare), structura organizatorică și, dacă este cazul, autorizația (autorizațiile) sau înregistrarea (înregistrările) relevantă (relevante) necesare pentru a îndeplini în mod fiabil și profesional funcția critică sau importantă și a-și respecta obligațiile pe durata angajamentului de externalizare în cloud. Factorii suplimentari care trebuie avuți în vedere în cadrul procesului de diligență cu privire la FSC conțin, dar nu se limitează la:

a) gestionarea securității informațiilor și, în special, protecția datelor cu caracter personal, confidențiale sau sensibile în alt mod;

b) asistența pentru servicii, inclusiv planurile și contactele de asistență și procesele de gestionare a incidentelor;

c) planurile de asigurare a continuității activității și planurile de recuperare în caz de dezastru.

22. Acolo unde este cazul și pentru a sprijini procesul de diligență efectuat, o societate poate utiliza, de asemenea, certificări bazate pe standarde internaționale și rapoarte de audit externe sau interne.

23. Dacă o societate ia cunoștință de deficiențe semnificative și/sau de modificări semnificative ale serviciilor furnizate sau ale situației FSC, analiza de preexternalizare și procesul de diligență privind FSC trebuie revizuite imediat sau, dacă este necesar, reluate.

24. În cazul în care încheie un nou angajament de externalizare sau reînnoiește un angajament existent cu un FSC care a fost deja evaluat, societatea trebuie să stabilească, pe baza unei abordări bazate pe riscuri, dacă este necesar un nou proces de diligență.

Orientarea 3. Elemente contractuale esențiale

25. Drepturile și obligațiile care le revin unei societăți și furnizorului de servicii cloud trebuie să fie clar definite printr-un acord scris.

26. Acordul scris trebuie să acorde în mod expres societății posibilitatea de a-l rezilia, atunci când este necesar.

27. În cazul externalizării unor funcții critice sau importante, acordul scris trebuie să conțină cel puțin:

a) o descriere clară a funcției externalizate;

b) data de începere și data de încetare a acordului, după caz, și perioadele de preaviz pentru FSC și pentru întreprindere;

c) legea de reglementare a acordului și, dacă există, alegerea jurisdicției;

d) obligațiile financiare ale societății și ale FSC;

e) dacă este permisă subcontractarea și, dacă da, în ce condiții, având în vedere Orientarea 7;

f) locația (locațiile) (și anume regiunile sau țările) în care va fi asigurată funcția externalizată și în care vor fi păstrate și prelucrate datele, precum și condițiile care trebuie îndeplinite, inclusiv cerința de a notifica societatea dacă FSC propune schimbarea locației (locațiilor);

g) dispoziții privind securitatea informațiilor și protecția datelor cu caracter personal, având în vedere Orientarea 4;

h) dreptul societății de a monitoriza în mod regulat performanța FSC în cadrul angajamentului de externalizare în cloud, având în vedere Orientarea 6;

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

j) obligațiile de raportare ale FSC față de societate și, după caz, obligațiile de a prezenta rapoarte relevante pentru funcția

de securitate și funcțiile esențiale ale societății, precum rapoarte întocmite de funcția de audit intern a FSC;

k) dispoziții privind gestionarea incidentelor de către FSC, inclusiv obligația FSC de a raporta societății, fără întârzieri nejustificate, incidentele care au afectat funcționarea serviciului contractat al societății;

l) dacă FSC trebuie să încheie o asigurare obligatorie împotriva anumitor riscuri și, dacă este cazul, nivelul asigurării necesare;

m) cerințele pentru ca FSC să implementeze și să testeze continuitatea activității și planurile de recuperare în caz de dezastru;

n) cerința ca FSC să acorde societății, autorităților sale competente și oricărei alte persoane desemnate de societate sau autorităților competente dreptul de a accesa („drepturi de acces”) și de a inspecta („drepturi de audit”) informațiile, sediile, sistemele și dispozitivele relevante ale FSC în măsura necesară pentru a monitoriza performanța FSC în cadrul angajamentului de externalizare în cloud și conformitatea sa cu cerințele de reglementare și contractuale aplicabile, având în vedere Orientarea 6;

o) dispoziții prin care să se asigure că datele pe care FSC le prelucrează sau le stochează în numele societății pot fi accesate, recuperate și returnate societății, după caz, având în vedere Orientarea 5.

Orientarea 4. Securitatea informațiilor

28. O societate trebuie să stabilească cerințe de securitate a informațiilor în politicile și procedurile sale interne și în cadrul acordului scris de externalizare în cloud și să monitorizeze în permanență respectarea acestor cerințe, inclusiv pentru a proteja datele confidențiale, cu caracter personal sau alte date sensibile. Aceste cerințe trebuie să fie proporționale cu natura, amploarea și complexitatea funcției pe care societatea o externalizează către FSC și cu riscurile inerente acestei funcții.

29. În acest scop, în cazul externalizării unor funcții critice sau importante și fără a aduce atingere cerințelor aplicabile conform RGPD, o societate care aplică o abordare bazată pe riscuri trebuie, cel puțin:

a) organizarea în domeniul securității informațiilor: să se asigure că există o alocare clară a rolurilor și responsabilităților în materie de securitate a informațiilor între societate și FSC, inclusiv în ceea ce privește detectarea amenințărilor, gestionarea incidentelor și gestionarea patch-urilor, și să se asigure că FSC este capabil efectiv să își îndeplinească rolurile și responsabilitățile;

b) gestionarea identității și accesului: să se asigure că există mecanisme robuste de autentificare (de exemplu, autentificare dublă) și controale ale accesului, pentru a preveni accesul neautorizat la datele și la resursele de cloud back-end ale societății;

c) criptarea și gestionarea cheilor de securitate: să se asigure că tehnologiile de criptare relevante sunt utilizate, acolo unde este necesar, pentru date în tranzit, date în memorie, date în repaus și copii de rezervă ale datelor, în combinație cu soluții adecvate de gestionare a cheilor de securitate pentru a limita riscul accesului neautorizat la cheile de criptare; în special, societatea trebuie să aibă în vedere tehnologia și procesele de ultimă generație atunci când își alege soluția de gestionare a cheilor de securitate;

d) securitatea operațiunilor și a rețelei: să ia în considerare nivelurile adecvate de disponibilitate a rețelei, segregarea rețelei [de exemplu, izolarea „chiriașilor” în mediul partajat al cloudului, separarea operațională în ceea ce privește webul, logica aplicației, sistemul de operare, rețeaua, sistemul de gestionare a bazei de date (DBMS) și straturile de stocare] și mediile de procesare (de exemplu, testarea acceptării de către utilizator, dezvoltare, producție);

e) interfețe de programare a aplicațiilor (API): să ia în considerare mecanismele de integrare a serviciilor cloud cu sistemele societății, pentru a asigura securitatea API-urilor (de exemplu, stabilirea și menținerea politicilor și procedurilor de securitate a informațiilor pentru API-uri pe mai multe interfețe de sistem, jurisdicții și funcții comerciale pentru a preveni divulgarea, modificarea sau distrugerea neautorizată a datelor);

f) continuitatea afacerii și recuperarea în caz de dezastru: să se asigure că există controale efective de continuitate a activității și de recuperare în caz de dezastru (de exemplu, prin stabilirea de cerințe minime de capacitate, selectarea opțiunilor de găzduire care sunt răspândite geografic, cu capacitatea de a comuta de la una la alta, sau solicitarea și revizuirea documentației care descrie ruta de transport al datelor societății între sistemele FSC, precum și luarea în considerare a posibilității de a reproduce imagini mecanice într-o locație de stocare independentă, care să fie suficient de bine izolată de rețea sau deconectată);

g) localizarea datelor: să adopte o abordare bazată pe riscuri în ceea ce privește locația (locațiile) de stocare și prelucrare a datelor (și anume regiuni sau țări);

h) conformitate și monitorizare: să verifice dacă FSC respectă standardele de securitate a informațiilor recunoscute la nivel internațional și dacă a implementat controale adecvate de securitate a informațiilor (de exemplu, obligația FSC de a furniza dovezi că efectuează revizuri relevante ale securității informațiilor și efectuarea de evaluări și teste periodice ale mecanismelor FSC de securitate a informațiilor).

Orientarea 5. Strategiile de ieșire

30. În cazul externalizării unor funcții critice sau importante, o societate trebuie să se asigure că este capabilă să iasă din angajamentul de externalizare în cloud fără întreruperi nejustificate ale activităților și serviciilor sale către clienții săi și fără a aduce atingere respectării obligațiilor sale în temeiul dispozițiilor aplicabile și fără a afecta confidențialitatea, integritatea și disponibilitatea datelor sale. În acest scop, o societate trebuie:

a) să elaboreze planuri de ieșire cuprinzătoare, documentate și suficient de mult testate. Aceste planuri trebuie actualizate după necesități, inclusiv în cazul unor modificări aduse funcției externalizate;

b) să identifice soluții alternative și să elaboreze planuri de tranziție pentru a elimina funcția și datele externalizate de la FSC și, după caz, de la orice subcontractant și să le transfere către FSC-ul alternativ indicat de societate sau direct înapoi către societate. Aceste soluții trebuie definite în raport cu provocările care pot apărea din cauza locației datelor, luând măsurile necesare pentru a asigura continuitatea activității în faza de tranziție;

c) să se asigure că acordul scris de externalizare în cloud include o obligație pentru FSC de a sprijini transferul ordonat al funcției externalizate și prelucrarea conexă a datelor, de la FSC și orice subcontractant către un alt FSC, indicat de societate sau direct către societate, în cazul în care societatea activează strategia de ieșire. Obligația de a sprijini transferul ordonat al funcției externalizate și tratamentul aferent al datelor trebuie să includă, după caz, ștergerea în siguranță a datelor din sistemele FSC și ale oricărui subcontractant.

31. La elaborarea planurilor și soluțiilor de ieșire menționate la literele (a) și (b) („strategia de ieșire”), societatea trebuie să aibă în vedere următoarele:

a) să definească obiectivele strategiei de ieșire;

b) să definească evenimentele declanșatoare care ar putea activa strategia de ieșire. Aceste evenimente trebuie să includă cel puțin încetarea angajamentului de externalizare în cloud la inițiativa societății sau a FSC, precum și oprirea sau o altă întrerupere gravă a activității comerciale a FSC;

c) să efectueze o analiză a impactului economic, care să fie proporțională cu funcția externalizată, pentru a identifica ce resurse umane și de altă natură ar fi necesare pentru a implementa strategia de ieșire;

d) să atribuie roluri și responsabilități pentru gestionarea strategiei de ieșire;

e) să testeze caracterul oportun al strategiei de ieșire, folosind o abordare bazată pe riscuri (de exemplu, prin efectuarea unei analize a costurilor potențiale, a impactului, a resurselor și a implicațiilor temporale ale transferului unui serviciu externalizat către un furnizor alternativ);

f) să definească criteriile de succes ale tranziției.

32. O societate trebuie să includă indicatori ai evenimentelor declanșatoare ale strategiei de ieșire în monitorizarea și supravegherea sa continuă a serviciilor furnizate de FSC în temeiul angajamentului de externalizare în cloud.

Orientarea 6. Drepturi de acces și de audit

33. O societate trebuie să se asigure că acordul scris de externalizare în cloud nu limitează exercitarea efectivă a drepturilor de acces și de audit ale societății și ale autorităților competente și nici opțiunile de supraveghere asupra FSC.

34. O societate trebuie să se asigure că exercitarea drepturilor de acces și de audit (de exemplu, frecvența auditurilor și domeniile și serviciile de auditat) ia în considerare dacă externalizarea este legată de o funcție critică sau importantă, precum și natura și amploarea riscurilor și impactul care decurge din angajamentul de externalizare în cloud asupra societății.

35. În cazul în care exercitarea drepturilor de acces sau de audit sau utilizarea anumitor tehnici de audit creează un risc pentru mediul FSC și/sau pentru un alt client al FSC (de exemplu, prin impactul asupra nivelurilor serviciilor, confidențialității, integrității și disponibilității datelor), FSC trebuie să ofere societății o justificare clară a motivului pentru care acest lucru ar crea un risc, iar FSC trebuie să convină cu societatea asupra unor modalități alternative de a obține un rezultat similar [de exemplu, includerea unor mecanisme de control specifice care să fie testate într-un raport specific/certificare specifică elaborat(ă) de FSC].

36. Fără a aduce atingere responsabilității lor finale cu privire la angajamentele de externalizare în cloud, pentru a utiliza mai eficient resursele de audit și pentru a reduce povara organizatorică asupra FSC și clienților săi, societățile pot utiliza:

a) certificări de la terți și rapoarte de audit intern sau extern efectuate de terți, puse la dispoziție de FSC;

b) audituri centralizate efectuate împreună cu alți clienți ai aceluiași FSC sau audituri centralizate efectuate de un terț auditor desemnat de mai mulți clienți ai aceluiași FSC.

37. În cazul externalizării unor funcții critice sau importante, societățile trebuie să evalueze dacă certificările de la terți și rapoartele de audit intern sau extern menționate la pct. 37 lit. a) sunt adecvate și suficiente pentru a se conforma obligațiilor sale în temeiul legislației aplicabile și, în timp, trebuie să urmărească să nu se bazeze doar pe aceste certificări și rapoarte.

38. În cazul externalizării unor funcții critice sau importante, o societate trebuie să utilizeze certificările de la terți și rapoartele de audit intern sau extern menționate la pct. 37 lit. a) numai dacă:

a) este mulțumită de faptul că obiectul certificărilor sau al rapoartelor de audit acoperă sistemele-cheie ale FSC (de exemplu, procesele, aplicațiile, infrastructura, centrele de date etc.), mecanismele de control identificate de societate și conformitatea cu legislația aplicabilă relevantă;

b) evaluează temeinic și periodic conținutul certificărilor sau rapoartelor de audit și verifică să nu fie caduce rapoartele sau certificările;

c) se asigură că sistemele-cheie și mecanismele de control importante ale FSC sunt incluse în viitoarele versiuni ale certificărilor sau ale rapoartelor de audit;

d) este mulțumită de partea care realizează certificarea sau auditul (de exemplu, cu privire la calificările și expertiza acesteia, la reefectuarea/verificarea dovezilor din dosarul de audit subiacent, precum și în ceea ce privește rotația entității de certificare sau de audit);

e) este mulțumită că certificările sunt emise și auditurile sunt efectuate conform unor standarde corespunzătoare și că includ un test de eficacitate a mecanismelor de control importante implementate;

f) are dreptul contractual de a solicita extinderea domeniului de aplicare al certificărilor sau al rapoartelor de audit la alte sisteme și mecanisme de control relevante ale FSC; numărul și frecvența acestor cereri de modificare a domeniului de aplicare trebuie să fie rezonabile și legitime din perspectiva administrării riscurilor;

g) își păstrează dreptul contractual de a efectua audituri individuale la fața locului, la aprecierea proprie, în ceea ce privește funcția externalizată.

39. O societate trebuie să se asigure că, înainte de o vizită la fața locului, inclusiv a unui terț desemnat de societate (de exemplu, un auditor), FSC transmite un preaviz într-un termen rezonabil, cu excepția cazului în care o notificare prealabilă timpurie nu este posibilă din cauza unei situații de urgență sau de criză sau din cauză că ar crea o situație în care auditul nu ar mai fi eficient. Un astfel de preaviz trebuie să includă locația și scopul vizitei, precum și personalul care va participa la vizită.

40. Având în vedere că serviciile cloud prezintă un nivel ridicat de complexitate tehnică și implică anumite provocări de natură jurisdicțională, personalul care efectuează auditul — care poate consta din auditorii săi interni sau din grupul de auditori care acționează în numele său — trebuie să aibă aptitudinile și cunoștințele adecvate pentru a evalua în mod corespunzător serviciile de cloud relevante și a efectua un audit eficient și relevant. Acest lucru trebuie să se aplice și personalului societății, care revizuește certificările sau rapoartele de audit furnizate de FSC.

Orientarea 7. Subcontractarea externalizării

41. Dacă este permisă externalizarea în lanț a funcțiilor critice sau importante (sau a unor părți semnificative din acestea), acordul scris de externalizare în cloud dintre societate și FSC trebuie:

a) să precizeze orice parte sau aspect al funcției externalizate care sunt excluse de la potențiala subcontractare;

b) să indice condițiile care trebuie îndeplinite în cazul subcontractării;

c) să precizeze că FSC poartă răspunderea și obligația de a supraveghea serviciile pe care le-a subcontractat, pentru a se asigura că toate obligațiile contractuale dintre FSC și societate sunt îndeplinite în permanență;

d) să includă obligația FSC de a notifica societatea cu privire la orice intenție de subcontractare sau orice modificare semnificative la aceasta, mai ales atunci când acest lucru ar putea afecta capacitatea FSC de a-și îndeplini obligațiile în temeiul angajamentului de externalizare în cloud cu societatea. Perioada de notificare stabilită în acordul scris trebuie să permită societății suficient timp, cel puțin pentru a efectua o evaluare a riscului subcontractării propuse sau a modificărilor semnificative ale acesteia și pentru a o contesta sau aproba în mod explicit, după cum se indică la lit. e);

e) să se asigure că societatea are dreptul de a contesta subcontractarea planificată sau modificările semnificative aduse acesteia sau că este necesară o aprobare explicită înainte de intrarea în vigoare a subcontractării sau a modificărilor semnificative propuse;

f) să se asigure că societatea are dreptul contractual de a rezilia angajamentul de externalizare în cloud cu FSC în cazul în care contestă subcontractarea propusă sau modificări semnificative aduse acesteia și în cazul unei subcontractări nejustificate (de exemplu, dacă FSC continuă cu subcontractarea

fără notificarea societății sau încalcă grav condițiile de subcontractare stipulate în contractul de externalizare).

42. Societatea trebuie să se asigure că FSC supraveghează în mod adecvat subcontractantul.

Orientarea 8. Notificarea scrisă adresată autorităților competente

43. Societatea trebuie să comunice în scris și în timp util autorității sale competente angajamentul planificat de externalizare în cloud care vizează o funcție critică sau importantă. De asemenea, societatea trebuie să notifice în timp util și în scris autoritatea competentă cu privire la angajamentele de externalizare în cloud care privesc o funcție care anterior a fost clasificată ca fiind necritică sau neimportantă, dar apoi a devenit critică sau importantă.

44. Notificarea scrisă a societății trebuie să includă, ținând cont de principiul proporționalității, cel puțin următoarele informații:

a) data de începere a acordului de externalizare în cloud și, după caz, următoarea dată de reînnoire a contractului, data de încetare și/sau perioadele de preaviz pentru FSC și pentru societate;

b) o descriere succintă a funcției externalizate;

c) un scurt rezumat al motivelor pentru care funcția externalizată este considerată critică sau importantă;

d) numele și numele de marcă (dacă este cazul) ale FSC, țara sa de înregistrare, numărul de înregistrare, identificatorul entității juridice (dacă este disponibil), adresa sa înregistrată, datele sale de contact relevante, precum și denumirea societății-mamă (dacă este cazul);

e) legea de reglementare a angajamentului de externalizare în cloud și, dacă există, alegerea jurisdicției;

f) modele de implementare în cloud și natura specifică a datelor care trebuie păstrate de FSC și locațiile (și anume regiunile sau țările) în care vor fi stocate aceste date;

g) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate;

h) data celei mai recente evaluări a riscului sau a celui mai recent audit al FSC, împreună cu un scurt rezumat al principalelor rezultate, și data următoarei evaluări planificate sau a următorului audit planificat;

i) persoana fizică sau organul de decizie din cadrul societății care a aprobat angajamentul de externalizare în cloud;

j) după caz, numele tuturor subcontractanților cărora le sunt subcontractate părți semnificative ale unei funcții critice sau importante, inclusiv țara sau regiunea în care sunt înregistrați subcontractanții, în care va fi furnizat serviciul subcontractat și în care vor fi stocate datele.

Orientarea 9. Supravegherea angajamentelor de externalizare în cloud

45. Autoritățile competente trebuie să evalueze riscurile care decurg din angajamentele de externalizare în cloud ale societăților în cadrul procesului lor de supraveghere. În special, această evaluare trebuie să se concentreze asupra angajamentelor legate de externalizarea funcțiilor critice sau importante.

46. Autoritățile competente trebuie să fie convinse că pot asigura o supraveghere eficientă, în special atunci când societățile externalizează funcții critice sau importante care sunt efectuate în afara UE.

47. Autoritățile competente trebuie să evalueze, în cadrul unei abordări bazate pe riscuri, dacă societățile:

a) dețin resursele necesare și au instituit procesele operaționale și de guvernare relevante pentru a încheia, implementa și supraveghea în mod adecvat și eficient angajamente de externalizare în cloud;

b) identifică și gestionează toate riscurile relevante asociate externalizării în cloud.

48. Atunci când sunt identificate riscuri de concentrare, autoritățile competente trebuie să monitorizeze evoluția acestor riscuri și să evalueze atât impactul lor potențial asupra altor societăți pe care le supraveghează, cât și stabilitatea pieței financiare.

ACTE ALE AUTORITĂȚII ELECTORALE PERMANENTE

AUTORITATEA ELECTORALĂ PERMANENTĂ

R A P O R T

privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul Câmpina Curată

— extras —

În conformitate cu prevederile art. 42 alin. (1) și ale art. 44 alin. (1), (4) și (6) din Legea nr. 334/2006 privind finanțarea activității partidelor politice și a campaniilor electorale, republicată, cu modificările și completările ulterioare, cu Planul de control pe anul 2025 aprobat de președintele Autorității Electorale Permanente, precum și cu notificarea misiunii de control, în perioada 15.09.2025-7.10.2025 s-a desfășurat misiunea de control referitoare la respectarea prevederilor legale privind veniturile și cheltuielile înregistrate de Partidul Câmpina Curată în anii 2023-2024, perioada verificată fiind 1.01.2023-31.12.2024.

I. Constatări

Ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control, s-a constatat că în anul 2023 veniturile Partidului Câmpina Curată au totalizat 800.125,61 lei și au fost obținute din donații în sumă de 800.000,00 lei și venituri din dobânzi bancare în sumă de 125,61 lei. Cheltuielile în anul 2023 au fost în sumă de 696.684,75 lei.

Totodată, ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control s-a constatat că în anul 2024 veniturile Partidului Câmpina Curată au totalizat 1.039.106,66 lei și au fost obținute din donații în sumă de 1.039.030,00 lei și venituri din dobânzi bancare în cuantum de 76,66 lei. Cheltuielile în anul 2024 au fost în sumă de 1.104.035,20 lei.

II. Sancțiuni aplicate

Partidul Câmpina Curată nu a fost sancționat.

București, 30 octombrie 2025.

Nr. 18.197.

AUTORITATEA ELECTORALĂ PERMANENTĂ

R A P O R T

privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă la Partidul Republican Conservator în anul 2025

— extras —

În conformitate cu prevederile art. 42 alin. (1) și ale art. 44 alin. (1), (4) și (6) din Legea nr. 334/2006 privind finanțarea activității partidelor politice și a campaniilor electorale, republicată, cu modificările și completările ulterioare, cu Planul de control pe anul 2025, aprobat de președintele Autorității Electorale Permanente, precum și cu notificarea misiunii de control, în perioada 3.10.2025-24.10.2025 s-a desfășurat misiunea de control referitoare la verificarea respectării dispozițiilor legale privind veniturile și cheltuielile înregistrate de Partidul Republican Conservator în perioada 1.01.2023-31.12.2024.

I. Constatări

Ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control s-a constatat că:

În anul 2023 veniturile Partidului Republican Conservator au totalizat 5.880,00 lei și au fost obținute din cotizații. Cheltuielile au fost în sumă de 8.737,83 lei.

În anul 2024 veniturile Partidului Republican Conservator au totalizat 600,00 lei și au fost obținute din cotizații. Cheltuielile au fost în sumă de 3.142,34 lei.

II. Sancțiuni

Nu au fost aplicate sancțiuni.

București, 6 noiembrie 2025.

Nr. 18.550.

AUTORITATEA ELECTORALĂ PERMANENTĂ

R A P O R T**privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă
la Partidul Arădenilor în anul 2025**

— extras —

În conformitate cu prevederile art. 42 alin. (1) și ale art. 44 alin. (1), (4) și (6) din Legea nr. 334/2006 privind finanțarea activității partidelor politice și a campaniilor electorale, republicată, cu modificările și completările ulterioare, cu Planul de control pe anul 2025 aprobat de președintele Autorității Electorale Permanente, precum și cu notificarea misiunii de control, în perioada 15.09.2025-5.11.2025 s-a desfășurat misiunea de control referitoare la respectarea prevederilor legale privind veniturile și cheltuielile înregistrate de Partidul Arădenilor în anii 2023-2024, perioada verificată fiind 1.01.2023-31.12.2024.

I. Constatări

Cu ocazia desfășurării misiunii de control, echipa de control a constatat că Partidul Arădenilor a respectat în totalitate prevederile legale privind veniturile și cheltuielile în anii 2023-2024.

II. Sancțiuni aplicate

În urma verificărilor efectuate asupra documentelor puse la dispoziție de către reprezentanții Partidului Arădenilor, echipa de control nu a constatat săvârșirea unor fapte contravenționale.

București, 28 noiembrie 2025.

Nr. 20.000.

AUTORITATEA ELECTORALĂ PERMANENTĂ

R A P O R T**privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă
la Partidul România în Acțiune**

— extras —

În conformitate cu prevederile art. 42 alin. (1) și ale art. 44 alin. (1), (4) și (6) din Legea nr. 334/2006 privind finanțarea activității partidelor politice și a campaniilor electorale, republicată, cu modificările și completările ulterioare, cu Planul de control pe anul 2025 aprobat de președintele Autorității Electorale Permanente, precum și cu notificarea misiunii de control, în perioada 15.09.2025-11.11.2025 s-a desfășurat misiunea de control referitoare la respectarea prevederilor legale privind veniturile și cheltuielile înregistrate de Partidul România în Acțiune în anii 2023-2024, perioada verificată fiind 1.01.2023-31.12.2024.

I. Constatări

Ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control, s-a constatat că în anul 2023 veniturile Partidului România în Acțiune au totalizat 31.235,00 lei și au fost obținute din cotizații ale membrilor de partid în sumă de 25.235,00 lei și venituri din donații în sumă de 6.000,00 lei. Cheltuielile în anul 2023 au fost în sumă de 34.681,83 lei.

Totodată, ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control s-a constatat că în anul 2024 veniturile Partidului România în Acțiune au totalizat 3.136.955,45 lei și au fost obținute din cotizații ale membrilor de partid în sumă de 115.453,00 lei, venituri din donații în sumă de 90.834,00 lei, venituri din dobânzi bancare în cuantum de 2.039,45 lei și venituri din contribuțiile membrilor reprezentând contribuții pentru finanțarea campaniei electorale aferente alegerilor locale și parlamentare din anul 2024 în cuantum de 2.928.629,00 lei. Cheltuielile în anul 2024 au fost în sumă de 3.135.351,11 lei.

II. Sancțiuni aplicate

Partidul România în Acțiune nu a fost sancționat.

București, 28 noiembrie 2025.

Nr. 20.042.

AUTORITATEA ELECTORALĂ PERMANENTĂ

R A P O R T**privind rezultatul controlului efectuat de Autoritatea Electorală Permanentă
la Partidul SOS România în anii 2023 și 2024**

— extras —

În conformitate cu prevederile art. 42 alin. (1) și ale art. 44 alin. (1), (4) și (6) din Legea nr. 334/2006 privind finanțarea activității partidelor politice și a campaniilor electorale, republicată, cu modificările și completările ulterioare, cu Planul de control pe anii 2023-2024 aprobat de președintele Autorității Electorale Permanente, precum și cu notificarea misiunii de control, în perioada 15.09.2025-8.12.2025 s-a desfășurat misiunea de control referitoare la respectarea prevederilor legale privind veniturile și cheltuielile înregistrate de Partidul SOS România în anii 2023-2024, perioada verificată fiind 1.01.2023-31.12.2024.

Constatări

Ca urmare a verificărilor efectuate asupra documentelor contabile puse la dispoziția echipei de control s-a constatat că:

— pentru anul 2023 veniturile Partidului SOS România au fost totalizate în sumă de 339.206,53 lei și au fost obținute din venituri din cotizații în sumă de 252.564,07 lei, venituri din donații în sumă de 82.047,19 lei și venituri din exploatare în valoare de 4.595,27 lei. Cheltuielile au fost în sumă de 117.772,13 lei;

— pentru anul 2024 veniturile Partidului SOS România au fost totalizate în sumă de 7.103.823,31 lei și au fost obținute din venituri din cotizații în sumă de 607.397,10 lei, venituri din donații în sumă de 6.496.420,90 lei, venituri din dobânzi în valoare de 25,95 lei. Cheltuielile au fost în sumă de 7.161.495,28 lei.

București, 9 decembrie 2025.

Nr. 20.791.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Relații cu publicul: șos. Panduri nr. 1, bloc P33, sectorul 5, București; 050651.

Tel. 021.401.00.73, 021.401.00.78/79/83.

Pentru publicări, încărcări actele pe site, la: <https://www.monitoruloficial.ro>, secțiunea Publicări.