Ministerul Agriculturii și Dezvoltării Rurale

Agenția pentru Finanțarea Investițiilor Rurale	Agenția Națională de Îmbunătățiri Funciare
Nr. P440/18.08.2026	Nr. 15.907/21.08.2026

ACT ADIȚIONAL NR. 1 la
ACORDUL DE DELEGARE AFIR nr. P188/04.10.2023 // ANIF nr. 20394/02.10.2023

privind unele verificări specifice necesare în implementarea tehnică și financiară a intervenției DR-25 Modernizarea infrastructurii de irigații și a intervenției DR-26 Înființarea sistemelor de irigații – din cadrul Planului Strategic 2023 - 2027

Părţile:

Agenţia pentru Finanțarea Investițiilor Rurale, denumită în continuare **AFIR**, cu sediul în strada Ştirbei Vodă, nr. 43, sector 1, Bucureşti, adresa de e-mail: cabinet@afir.info, telefon: 031.860.27.47, reprezentată legal prin **Adrian-Ionuț CHESNOIU**, în calitate de Director General

și

Agenția Națională de Îmbunătățiri Funciare, denumită în continuare **ANIF**, cu sediul în Șos. Olteniței, nr. 35-37, sector 4, Bucureşti, adresa de e-mail: centrala@anif.ro , telefon: 021.332.28.24, reprezentată legal prin Cornel POPA, în calitate de Director General,

În temeiul art. 8 din Acordul de Delegare AFIR nr. P188/04.10.2023 // ANIF nr. 20394/02.10.2023, părțile convin să încheie prezentul ACT ADIȚIONAL, după cum urmează:

Art. I Acordul de Delegare AFIR nr. P188/04.10.2023 // ANIF nr. 20394/02.10.2023 se completează după cum urmează:

1. La Art. 3.2. – DREPTURILE ȘI OBLIGAȚIILE ANIF, după alin. 3.2.21 se adaugă alin. 3.2.22 având următorul cuprins:

   "**3.2.22** Prevederile Anexei nr. 3 la prezentul Acord de delegare se duc la îndeplinire de către organismul delegat – în calitate de instituție *certificată SR EN ISO/IEC 27001:2023 – Tehnologia informației, securitatea cibernetică și protecția vieții private*."

2. După ANEXA nr. 2 se introduce ANEXA nr. 3 intitulată *Securitatea informației și a sistemelor informatice aferente activităților delegate,* ce devine parte integrantă a Acordul de delegare AFIR nr. P188/04.10.2023 // ANIF nr. 20394/02.10.2023, conform Anexei la prezentul act adițional.

Art. II - Prezentul act adițional este întocmit în două exemplare originale, în limba română, câte unul pentru fiecare parte și intră în vigoare la data semnării de către ambele părți.

Art. III - Celelalte prevederi ale Acordului de Delegare AFIR nr. P188/11.03.2024/04.10.2023 // ANIF nr. 20394/02.10.2023 rămân neschimbate.

AGENȚIA PENTRU FINANȚAREA INVESTIȚIILOR RURALE

DIRECTOR GENERAL
Adrian-Ionuţ CHESNOIU

AGENȚIA NAȚIONALĂ DE ÎMBUNĂTĂȚIRI FUNCIARE

DIRECTOR GENERAL
Cornel POPA

Director General Adjunct
Infrastructură, LEADER şi Investiţii Non-agricole
Florin-Dan SCARLAT

18.08.2026

Director
Direcţia Investiţii
Andreea-Valentina DUMITRU

Director
Direcţia Juridică şi Contencios
Alina FLOREA

17.08.2026

Director,
Direcţia Economică
Andrei BARABULEA

Director
Direcţia Infrastructură de Bază şi Acces
Cătălin GRIGORE

18.08.2026

Şef Serviciu
Serviciul Juridic şi Contencios Administrativ
Ovidiu-Florin DUMITRU

Director
Direcţia Coordonare Programe
Nicoleta-Mihaela MĂHĂLEAN

ANEXA
la Actul adițional nr. 1 la Acordul de delegare AFIR nr. P188/04.10.2023 // ANIF nr. 20394/02.10.2023.

SECURITATEA INFORMAȚIEI ȘI A SISTEMELOR INFORMATICE AFERENTE ACTIVITĂȚILOR DELEGATE

Art. 1 – Scop și domeniu de aplicare

(1) Prezenta anexă stabilește cerințele minime obligatorii privind securitatea informației și securitatea sistemelor informatice utilizate de Organismul Delegat pentru îndeplinirea atribuțiilor delegate de către Agenția pentru Finanțarea Investițiilor Rurale (denumită în continuare „AFIR" sau „Agenția de Plăți").

(2) Cerințele se aplică măsurilor organizatorice, procedurale, fizice și tehnice implementate pentru protejarea informațiilor aferente atribuțiilor delegate și a activelor asociate acestora, inclusiv a proceselor, sistemelor, aplicațiilor, infrastructurilor, canalelor de comunicație și a locațiilor prin intermediul cărora sunt create, transmise, primite, procesate, stocate, arhivate sau distruse datele, aferente atribuțiilor delegate și activităților desfășurate în baza prezentului protocol, indiferent de suportul acestora (electronic sau pe suport fizic).

(3) Aceste cerințe sunt complementare obligațiilor existente privind protecția datelor cu caracter personal și nu derogă de la prevederile Regulamentului (UE) 2016/679 (GDPR) și ale legislației naționale aplicabile.

Art. 2 – Cadru de referință

(1) Organismul Delegat se obligă să implementeze și să mențină măsuri de securitate a informației conforme cu:

a) Regulamentul (UE) 2022/127, Anexa I, pct. 1 – Mediul intern, lit. B (Securitatea sistemelor informatice) și lit. D (Delegarea), pct. 4 – Monitorizare;

b) standardul ISO/IEC 27001 (în varianta în vigoare), pentru toate sistemele și procesele care susțin activitățile delegate;

c) reglementările naționale aplicabile în domeniul securității cibernetice și al protecției infrastructurilor critice.

(2) Organismul Delegat va putea demonstra conformitatea cu cadrul de referință prin documentație, evidențe operaționale, rapoarte de audit intern și/sau rapoarte de audit independent.

Art. 3 – Sistemul de Management al Securității Informației (SMSI)

(1) Organismul Delegat menține un Sistem de Management al Securității Informației aplicabil activităților delegate, care include cel puțin:

a) o politică de securitate a informației aprobată de conducere și revizuită cel puțin anual;

b) o analiză de risc documentată, actualizată periodic și după orice schimbare semnificativă;

c) un Plan de tratare a riscurilor și o Declarație de Aplicabilitate (Statement of Applicability) sau echivalent;

d) roluri și responsabilități clar definite, inclusiv desemnarea unui responsabil cu securitatea informației (CISO / ofițer de securitate) ca punct de contact pentru AFIR.

Art. 4 – Controlul accesului

(1) Accesul la informațiile și sistemele utilizate pentru atribuțiile delegate se acordă pe baza principiilor „need-to-know" și „least privilege".

(2) Organismul Delegat implementează:

a) procese formalizate de acordare, modificare, revizuire periodică (cel puțin semestrial) și revocare a drepturilor de acces;

b) autentificare individuală, fără utilizarea conturilor partajate pentru utilizatori cu acces la date sensibile;

c) autentificare multifactor (MFA) pentru accesul administrativ, accesul de la distanță și accesul la aplicații care procesează date aferente activităților delegate;

d) o politică de parole conformă cu bunele practici recunoscute (complexitate, rotație controlată, protecție împotriva atacurilor de tip brute-force).

Art. 5 – Securitatea comunicațiilor

(1) Orice transmitere de informații între Organismul Delegat și AFIR, sau între Organismul Delegat și terți, în legătură cu atribuțiile delegate, se realizează exclusiv prin canale securizate, cu asigurarea confidențialității și integrității datelor pe întreaga durată a transferului.

(2) Cerințe minime pe canale de comunicare:

a) **Poșta electronică (e-mail):** transmiterea informațiilor sensibile se efectuează cu utilizarea criptării în tranzit (TLS aplicat pe conexiunile SMTP/IMAP/POP), iar pentru documente cu nivel sporit de sensibilitate se utilizează criptare la nivel de mesaj sau de atașament (de ex. S/MIME, PGP sau atașamente protejate cu parolă transmisă printr-un canal separat); cheile și parolele nu se transmit pe același canal cu informația protejată;

b) **VPN și acces la distanță:** conexiunile VPN utilizează protocoale moderne (IPsec, TLS-VPN), algoritmi criptografici considerați siguri la momentul implementării, autentificare multifactor și jurnalizare a sesiunilor; accesul de la distanță la sistemele care procesează date aferente activităților delegate se efectuează exclusiv prin VPN sau prin echivalent funcțional securizat;

c) **Transfer de fișiere:** se utilizează soluții de tip SFTP, FTPS, HTTPS sau platforme dedicate de schimb securizat de date; nu se permite utilizarea protocoalelor necriptate (FTP, HTTP, Telnet) pentru date aferente activităților delegate;

d) **Servicii cloud și platforme colaborative:** utilizarea acestora pentru date aferente activităților delegate este permisă numai dacă furnizorul îndeplinește cerințele de securitate echivalente prezentului capitol și dacă utilizarea a fost notificată în prealabil AFIR.

(3) Indiferent de canalul de comunicare utilizat, Organismul Delegat asigură păstrarea evidențelor (jurnale, registre de corespondență) pe o perioadă care permite trasabilitatea fluxurilor de informații pentru cel puțin durata aplicabilă obligațiilor contractuale și a celor impuse de cadrul de reglementare UE.

Art. 6 – Protecția datelor în repaus și pe ciclul de viață

(1) Datele aferente activităților delegate sunt protejate prin măsuri tehnice și organizatorice adecvate pe întreg ciclul de viață: colectare, prelucrare, transmitere, stocare, arhivare și distrugere.

(2) Cerințe minime:

a) criptarea datelor în repaus pentru bazele de date, sistemele de fișiere, dispozitivele mobile și mediile de stocare amovibile care conțin informații aferente activităților delegate;

b) clasificarea informațiilor și a echipamentelor care procesează date clasificate, cu aplicarea măsurilor de protecție corespunzătoare nivelului de clasificare;

c) proceduri documentate de păstrare, arhivare și ștergere sigură / distrugere certificată a datelor și suporturilor, la finalizarea perioadei de retenție.

Art. 7 – Securitatea operațională, jurnalizare și monitorizare

(1) Organismul Delegat implementează măsuri de securitate operațională care includ cel puțin:

a) protecție antimalware actualizată permanent pe toate stațiile de lucru și serverele;

b) management al vulnerabilităților, cu scanări periodice și aplicarea patch-urilor de securitate în termene rezonabile, corelate cu nivelul de criticitate;

c) jurnalizarea evenimentelor de securitate relevante (autentificări, modificări de privilegii, acces la date sensibile, acțiuni administrative) și păstrarea jurnalelor pentru o perioadă de minimum 12 luni sau conform cerințelor legale aplicabile, oricare este mai lungă;

d) protecția jurnalelor împotriva modificării sau ștergerii neautorizate;

e) sincronizarea ceasurilor sistemelor (NTP) pentru asigurarea corelării evenimentelor.

Art. 8 – Managementul incidentelor de securitate

(1) Organismul Delegat menține o procedură formalizată de management al incidentelor de securitate a informației, care include detectare, raportare, escaladare, tratare, comunicare și lecții învățate.

(2) Orice incident de securitate care afectează sau poate afecta confidențialitatea, integritatea sau disponibilitatea datelor ori sistemelor aferente activităților delegate se notifică AFIR fără întârziere nejustificată, dar nu mai târziu de 24 de ore de la momentul identificării, prin canalul de comunicare desemnat în acord.

(3) Notificarea include cel puțin: natura incidentului, momentul producerii și al detectării, sistemele și datele afectate, măsurile imediate de limitare a impactului și măsurile corective planificate.

(4) Un raport final privind incidentul este transmis AFIR în termen de 30 de zile de la închiderea incidentului, sau într-un termen agreat în funcție de complexitate.

Art. 9 – Continuitatea activității și recuperarea în caz de dezastru

(1) Organismul Delegat menține un Plan de Continuitate a Activității (BCP) și un Plan de Recuperare în caz de Dezastru (DRP) pentru sistemele și procesele care susțin activitățile delegate.

(2) Planurile sunt testate cel puțin anual, iar rezultatele testelor sunt documentate și puse la dispoziția AFIR la cerere.

(3) Organismul Delegat asigură efectuarea de copii de siguranță (backup) periodice, stocate într-o locație separată fizic și/sau logic, și testează periodic capacitatea de restaurare a acestora.

Art. 10 – Securitatea personalului

(1) Personalul Organismului Delegat implicat în activitățile delegate este supus unor obligații formale de confidențialitate, prin clauze contractuale sau acorduri NDA distincte.

(2) Organismul Delegat asigură instruirea inițială și periodică a personalului în domeniul securității informației, cu evidențierea participării (liste de prezență, certificate, înregistrări LMS).

(3) La încetarea raporturilor de muncă sau a misiunii, drepturile de acces sunt revocate fără întârziere, iar bunurile informaționale (echipamente, credențiale, documente) sunt recuperate pe baza unei proceduri documentate.

Art. 11 – Managementul furnizorilor și subcontractanților

(1) Atunci când activitățile delegate sau părți ale acestora implică furnizori sau subcontractanți cu acces la informații sau sisteme aferente, Organismul Delegat:

a) notifică AFIR cu privire la utilizarea acestora;

b) impune contractual furnizorilor cerințe de securitate cel puțin echivalente celor din prezenta anexă(flow-down);

c) monitorizează conformitatea furnizorilor prin mecanisme adecvate (chestionare, certificări, audituri).

Art. 12 – Audit și monitorizare de către AFIR

(1) AFIR are dreptul, în calitate de Agenție de Plăți responsabilă, de a evalua periodic modul în care Organismul Delegat asigură securitatea informațiilor și a sistemelor informatice aferente activităților delegate, prin:

a) misiuni de audit intern efectuate prin Serviciul Audit Intern al AFIR;

b) misiuni efectuate prin terți independenți mandatați de AFIR;

c) solicitarea de rapoarte de audit independente (de ex. ISO/IEC 27001, SOC 2 sau echivalent), dacă acestea există.

(2) Organismul Delegat asigură accesul rezonabil al echipei de audit la documentele, sistemele, locațiile și personalul relevant, cu respectarea cerințelor de confidențialitate și a programului operațional.

(3) Constatările auditurilor sunt comunicate Organismului Delegat, care prezintă, în termen de 30 de zile, un plan de acțiuni corective cu termene și responsabili, monitorizat de AFIR până la închidere.

(4) Monitorizare continuă prin activități de control intern din Anexa I a Reg.127/ 2022 care să asigure o supraveghere preventivă și continuă pentru a identifica riscurile în timp real se realizează prin DIT; Aceasta consta în asigurarea de către DIT că organismul delegat deține un certificat ISO27001 valid și menține această certificare pe toată durata valabilității acordului de delegare. Astfel, organismul delegat se obligă să transmită către AFIR certificatul ISO27001 valid, precum și rapoartele de audit desfășurate cu ocazia acordării certificării precum și cele aferente vizitelor de supraveghere.

(5) Activitatea de audit a AFIR se desfășoară conform standardelor recunoscute la nivel internațional, iar planificarea acoperă toate domeniile semnificative pe o perioadă de maximum 5 ani.

Art. 13 – Raportare periodică

(1) Organismul Delegat transmite AFIR, cel puțin anual, un raport sintetic privind starea securității informației aferente activităților delegate, care include:

a) sinteza riscurilor identificate și a măsurilor de tratare;

b) incidentele de securitate înregistrate în perioada de raportare;

c) rezultatele auditurilor interne sau externe efectuate;

d) modificările semnificative ale infrastructurii sau proceselor;

e) stadiul planurilor de acțiuni corective deschise.

(2) Adrese de contact: relatiiInstitutionale@afir.info, centrala@anif.ro, smsi@afir.info, audit.intern@afir.info.

Art. 14 – Managementul schimbării

(1) Organismul Delegat notifică AFIR, în timp util, cu privire la orice schimbare semnificativă care poate afecta securitatea informațiilor sau a sistemelor aferente activităților delegate, inclusiv:

a) migrări de sisteme sau aplicații;

b) externalizarea unor componente operaționale;

c) modificări ale arhitecturii de rețea sau ale canalelor de comunicare cu AFIR;

d) schimbarea furnizorilor de servicii cloud sau de telecomunicații.

Art. 15 – Neconformitate și remediere

(1) În cazul în care AFIR constată neconformități față de cerințele prezentei anexe, Organismul Delegat este obligat să implementeze măsurile corective solicitate, conform unui plan agreat.

(2) Neconformitățile repetate sau majore, care afectează capacitatea AFIR de a-și menține criteriile de acreditare în calitate de Agenție de Plăți, pot constitui motiv de revizuire sau reziliere a acordului de delegare, în condițiile stabilite în corpul principal al acordului.

Art. 16 – Revizuire periodică

(1) Prezenta anexă se revizuiește cel puțin o dată la 2 ani sau ori de câte ori intervin modificări semnificative în cadrul de reglementare european sau național aplicabil ori în arhitectura proceselor delegate.