AGENȚIA NAȚIONALĂ PENTRU REGLEMENTARE ÎN ENERGETICĂ
Republica Moldova

PLAN DE INSTRUIRE

Protecția Datelor cu Caracter Personal și Securitatea Informațională/Cibernetică

Curs integrat — 40 de ore — 10 module a câte 4 ore

📋 Acest document este exclusiv PLANUL de instruire — structura, agenda și obiectivele modulelor.

📋 Conținutul detaliat (suport de curs, exerciții, studii de caz) se elaborează separat, ulterior.

⏱ Durata totală: 40 de ore — 10 module x 4 ore, recomandat pe parcursul a 5 zile (8 ore/zi)

🔗 Plan rezultat din intercalarea a 2 surse: cursul ANRE de protecție a datelor (Legea 133/2011 și Legea 195/2024) și Cursul nr. 2 de securitate informațională/cibernetică (NIS2)

Clasificare: Uz intern
Ediția: 1.0 / 2026

Digitally signed by Monastîrli Nicolae
Date: 2026.06.30 13:54:12 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

1. Logica de integrare a celor două surse

Planul reorganizează și intercalează două documente sursă distincte într-un parcurs unic, coerent pedagogic, gândit specific pentru nevoile ANRE:

Sursă	Document de proveniență
PDCP / Legea 195	Curs ANRE — Protecția Datelor cu Caracter Personal (Legea 133/2011 și Legea 195/2024)
SI/SC / NIS2	Cursul nr. 2 — Protecția Informațiilor și Datelor cu Caracter Personal, Securitatea Informațională și Cibernetică
Integrat	Conținut nou, rezultat din intercalarea și convergența celor două surse pentru contextul specific ANRE

Ordinea modulelor urmează o progresie logică: pornim de la cadrul legal (de ce contează conformitatea), trecem prin fundamentele tehnice de securitate, apoi cuplăm fiecare obligație practică de protecție a datelor cu controlul tehnic corespunzător care o susține, și încheiem cu gestionarea incidentelor, auditul și un modul integrator final.

Principiu de proiectare: niciun modul tehnic de securitate nu este predat izolat de implicațiile sale pentru protecția datelor cu caracter personal — și nicio obligație legală de PDCP nu este predată fără controlul tehnic concret care o face aplicabilă în practică la ANRE.

2. Agenda generală — 10 module x 4 ore

Mod.	Plasare	Titlu modul	Durată	Format
M1	Ziua 1 — dim.	Cadrul legal integrat: protecția datelor (Legea 133/2011 → 195/2024) și securitatea informațională/cibernetică (NIS2, Legea 362/2018)	4 ore	Teoretic
M2	Ziua 1 — după-amiază	Fundamente de securitate informațională și cibernetică: triada CIA, Zero Trust, Security by Design — convergența cu PDCP	4 ore	Teoretic + Practic
M3	Ziua 2 — dim.	Confidențialitate, integritate, disponibilitate, autenticitate, nerepudiere — aplicare directă pe fluxurile de date ANRE	4 ore	Teoretic + Practic
M4	Ziua 2 — după-amiază	Obligațiile practice ANRE ca operator: registrul prelucrărilor, DPIA, persoane împuternicite + cultura organizațională de securitate	4 ore	Teoretic + Practic
M5	Ziua 3 — dim.	Amenințări, vulnerabilități și riscuri emergente — inclusiv riscuri specifice datelor cu caracter personal ale ANRE	4 ore	Teoretic + Practic
M6	Ziua 3 — după-amiază	Managementul vulnerabilităților și reducerea riscurilor — DPIA tehnică, scanare, testare, tratarea riscului	4 ore	Teoretic + Practic
M7	Ziua 4 — dim.	Controlul accesului și managementul identităților — aplicat la accesul la date cu caracter personal (RBAC, MFA, PAM)	4 ore	Teoretic + Practic
M8	Ziua 4 — după-amiază	Măsuri tehnice și organizatorice de securitate a prelucrării (art. 32) — criptare, pseudonimizare, backup, cloud, mobile	4 ore	Teoretic + Practic
M9	Ziua 5 — dim.	Gestionarea incidentelor de securitate și a breșelor de date — protocol unificat de notificare CNPDCP + NIS2	4 ore	Teoretic + Practic
M10	Ziua 5 — după-amiază	Audit, conformitate continuă, infrastructură critică (NIS2) și studii de caz integrate finale + evaluare	4 ore	Practic + Evaluare

3. Planul detaliat pe module

MODULUL 1 — Cadrul legal integrat: protecția datelor și securitatea informațională (4 ore)

Sursă / Provenență	*PDCP (Legea 133/2011 → 195/2024) intercalat cu SI/SC (NIS2, Legea 362/2018, GDPR art. 32-34)*
Teme integrate	– Legea nr. 133/2011 — cadrul actual aplicabil ANRE – Legea nr. 195/2024 — calendar de tranziție și noutăți (registrul prelucrărilor, DPIA, DPO) – Legea nr. 362/2018 și Directiva NIS2 — obligații de securitate a rețelelor și sistemelor – Regulamentul (UE) 2016/679 — art. 32 (securitate) corelat cu art. 33-34 (notificare breșe) – Standarde de referință: ISO/IEC 27001, 27701, 27005 – Autorități relevante: CNPDCP, STISC/ASC — rolurile lor față de ANRE
Format	Teoretic
Rezultat urmărit	Participanții văd cadrul legal ca un întreg coerent, nu ca două seturi separate de obligații — înțeleg unde se suprapun PDCP și securitatea informațională în activitatea ANRE.

MODULUL 2 — Fundamente de securitate informațională și cibernetică (4 ore)

Sursă / Provenență	*SI/SC, cu punte explicită către PDCP*
Teme integrate	– Securitate informațională vs. securitate cibernetică vs. protecția datelor — clarificarea conceptelor – Triada CIA (Confidențialitate, Integritate, Disponibilitate) + Autenticitate și Nerepudiere – Activul informațional și ciclul de viață al informației la ANRE – Apărarea în adâncime (Defense in Depth) și modelul Zero Trust – Security by Design / Security by Default — corespondentul tehnic al "privacy by design" din Legea 195/2024 – Convergența PDCP–SI: cum securitatea informațională susține, concret, protecția datelor
Format	Teoretic + exercițiu de clasificare a activelor informaționale ANRE
Rezultat urmărit	Participanții pot clasifica activele informaționale ale ANRE și pot lega fiecare principiu tehnic de o cerință legală corespunzătoare din Modulul 1.

MODULUL 3 — Confidențialitate, integritate, disponibilitate, autenticitate (4 ore)

Sursă / Provenență	*SI/SC — aplicat direct pe fluxurile de date ANRE identificate*
Teme integrate	– Confidențialitate: criptare, control acces, mascarea datelor — aplicat pe dosarele de petiții și date HR ANRE – Integritate: hashing, semnături digitale, jurnalizare — aplicat pe registrul activităților de prelucrare – Disponibilitate: BCP/DRP, redundanță, backup — corelat cu obligația de limitare a stocării din Legea 195/2024 – Autenticitate: certificate digitale, PKI, MFA — aplicat pe accesul la sistemele de reglementare ANRE – Nerepudiere: semnătura electronică, jurnale de audit — relevanță pentru deciziile de reglementare ANRE

Format	Teoretic + practic: demonstrație criptare și verificare integritate + studiu de caz (bază de date coruptă)
Rezultat urmărit	Participanții identifică, pentru fiecare flux de date ANRE cartografiat anterior, ce principiu CIA+ este prioritar și ce măsură tehnică îl susține.

MODULUL 4 — Obligațiile practice ANRE și cultura organizațională de securitate (4 ore)

Sursă / Provenență	*PDCP (obligații ANRE) intercalat cu SI/SC (cultura de securitate)*
Teme integrate	– Registrul activităților de prelucrare (art. 30, Legea 195/2024) — elaborare practică pentru ANRE – DPIA — când este obligatorie pentru prelucrările ANRE – Relația cu persoanele împuternicite (furnizori IT externi) — clauze contractuale obligatorii – Factorul uman ca vulnerabilitate și ca linie de apărare — politica de securitate informațională – Programul de conștientizare: campanii, simulări de phishing, teste – Responsabilitățile fiecărui angajat ANRE în protecția datelor și a informațiilor
Format	Teoretic + practic: elaborare registru prelucrări + plan de conștientizare în echipă
Rezultat urmărit	ANRE are un draft de registru al prelucrărilor și un plan de conștientizare adaptat instituției, nu doar concepte teoretice.

MODULUL 5 — Amenințări, vulnerabilități și riscuri emergente (4 ore)

Sursă / Provenență	*SI/SC, cu accent pe riscurile specifice datelor cu caracter personal*
Teme integrate	– Tipologia amenințărilor: malware, phishing/spear phishing, DDoS, MitM, injecții SQL/XSS, inginerie socială – Amenințări interne (insider threats) — relevanță directă pentru un operator cu date sensibile precum ANRE – Atacuri asupra lanțului de aprovizionare — relevanță pentru furnizorii IT externi ANRE – Riscuri emergente: AI/deepfakes, IoT, Ransomware-as-a-Service, riscuri cloud – Analiza amenințărilor specifice datelor cu caracter personal — conectare directă la Modulul 1 (art. 32-34)
Format	Teoretic + practic: utilizare baze CVE + studiu de caz atac ransomware real + hartă a amenințărilor ANRE
Rezultat urmărit	ANRE dispune de o hartă incipientă a amenințărilor proprii, prioritizată după impactul asupra datelor cu caracter personal.

MODULUL 6 — Managementul vulnerabilităților și reducerea riscurilor (4 ore)

Sursă / Provenență	*SI/SC, cu aplicare practică pe DPIA din Modulul 4*
Teme integrate	– Managementul vulnerabilităților: descoperire, evaluare, remediere, verificare – Scanarea vulnerabilităților și testarea de penetrare — tipuri și metodologii – Evaluarea riscurilor: ISO 27005, NIST SP 800-30 — metodologie aplicabilă DPIA-urilor ANRE – Probabilitate vs. impact; niveluri de risc acceptabil/tolerabil/inacceptabil – Tratarea riscului: evitare, reducere, transfer (asigurare cibernetică), acceptare – Managementul patch-urilor și hardening-ul sistemelor

Format	Teoretic + practic: demonstrație scanare vulnerabilități + evaluare de risc pentru un sistem ANRE cu date personale
Rezultat urmărit	Participanții elaborează o evaluare de risc completă pentru un sistem real ANRE, utilizabilă ca bază pentru o DPIA.

MODULUL 7 — Controlul accesului și managementul identităților (4 ore)

Sursă / Provenență	*SI/SC, aplicat direct la cerința legală de "need-to-know" din PDCP*
Teme integrate	– Principiul privilegiului minim și separarea atribuțiilor – Need-to-know / need-to-access — corespondentul tehnic al minimizării datelor (Legea 195/2024) – IAM: provisioning/de-provisioning, Single Sign-On, federarea identităților – Autentificare: factori, MFA/2FA, biometrie — considerente PDCP pentru datele biometrice – Autorizare: RBAC vs. ABAC – Accesul privilegiat (PAM) și accesul la datele cu caracter personal — cerințe specifice ANRE
Format	Teoretic + practic: proiectare matrice RBAC ANRE + studiu de caz (fost angajat cu acces activ) + demonstrație MFA
Rezultat urmărit	ANRE dispune de o matrice de acces RBAC-draft și o politică de control al accesului la datele cu caracter personal.

MODULUL 8 — Măsuri tehnice și organizatorice de securitate a prelucrării (4 ore)

Sursă / Provenență	*SI/SC (măsuri tehnice) ancorat direct în art. 32 GDPR / Legea 195/2024*
Teme integrate	– Art. 32 — măsuri tehnice și organizatorice adecvate (legătură directă cu Modulul 1) – Criptarea: simetrică/asimetrică, date în repaus/tranzit/uz, managementul cheilor – Pseudonimizarea și anonimizarea — tehnici aplicabile direct registrului ANRE – Firewall, IDS/IPS, SIEM; segmentarea rețelei – Securitatea endpoint-urilor, a aplicațiilor (OWASP Top 10), a cloud-ului, a dispozitivelor mobile (MDM/BYOD) – Backup și recuperare — strategii și testare, corelat cu disponibilitatea din Modulul 3
Format	Teoretic + practic: demonstrație criptare disc/comunicații + exercițiu pseudonimizare pe date tip ANRE
Rezultat urmărit	Participanții aplică pseudonimizarea pe un set de date simulat de tip ANRE și înțeleg exact ce înseamnă "măsuri adecvate" din art. 32.

MODULUL 9 — Gestionarea incidentelor de securitate și a breșelor de date (4 ore)

Sursă / Provenență	*Modul integrat — protocol unificat PDCP (notificare CNPDCP) + SI/SC (răspuns la incident)*
Teme integrate	– Definirea și diferențierea: incident de securitate vs. breșă de date cu caracter personal – Planul de răspuns la incidente: pregătire, identificare, izolare, eradicare, recuperare, lecții învățate – Echipa de răspuns la incidente — roluri clare (IT, DPO, conducere ANRE) – Notificarea breșelor: către CNPDCP în 72 de ore, către persoanele vizate când este obligatoriu

	– Investigația digitală și conservarea probelor; comunicarea în criză – Cooperarea cu autoritățile competente (CNPDCP, organele de drept)
Format	Teoretic + practic: simulare completă de incident (atac ransomware) + redactare notificare CNPDCP pe scenariu ANRE
Rezultat urmărit	ANRE dispune de un protocol unic de răspuns la incident care acoperă atât cerințele tehnice, cât și cele legale de notificare — nu două proceduri separate.

MODULUL 10 — Audit, conformitate continuă și studii de caz integrate (4 ore)

Sursă / Provenență	*Modul integrator final — sinteza tuturor surselor, cu accent pe infrastructura critică (NIS2) și conformitatea continuă*
Teme integrate	– Auditul intern și extern al securității informaționale; certificări ISO 27001/27701 – Monitorizarea continuă (SOC, SIEM) și jurnalizarea — cerințe și bune practici – Conceptul de infrastructură critică și servicii esențiale — relevanța NIS2 pentru sectorul energetic reglementat de ANRE – Evaluarea conformității cu legislația PDCP și de securitate; raportare către conducerea ANRE – Studiu de caz integrat final: scenariu complex care combină o breșă de date cu o obligație NIS2, rezolvat în echipe – Evaluare finală: test practic integrat (scenariu de răspuns + verificare cunoștințe)
Format	Exclusiv practic — lucru în echipă, prezentare, dezbatere, evaluare finală
Rezultat urmărit	Cursul se încheie cu un exercițiu unic care obligă participanții să mobilizeze cunoștințe din toate cele 9 module anterioare, plus o evaluare formală a competențelor dobândite.

4. Programare sugerată pe 5 zile

Ziua	Module	Ore	Accent principal
Ziua 1	Modulul 1 + Modulul 2	8 ore	Cadru legal + fundamente tehnice
Ziua 2	Modulul 3 + Modulul 4	8 ore	Principii CIA+ + obligații practice ANRE
Ziua 3	Modulul 5 + Modulul 6	8 ore	Amenințări + managementul riscului
Ziua 4	Modulul 7 + Modulul 8	8 ore	Control acces + măsuri tehnice (art. 32)
Ziua 5	Modulul 9 + Modulul 10	8 ore	Incidente + audit + evaluare finală

5. Notă privind pașii următori

Acest document conține exclusiv planul/structura cursului integrat. Conținutul detaliat al fiecărui modul (suport teoretic complet, exerciții pas-cu-pas, studii de caz redactate, fișe de evaluare, checkliste) urmează a fi elaborat ulterior, pe baza informațiilor specifice ANRE care vor fi identificate separat, conform precizării din cerința de elaborare a acestui plan.