MINISTERUL FINANȚELOR
AL REPUBLICII MOLDOVA

2023

GHID AL AUDITULUI INTERN ORIZONTAL PRIVIND EVALUAREA PROTECȚIEI DATELOR CU CARACTER PERSONAL

Direcția politici în domeniul CFPI

Ministerul Finanțelor

Cuprins

Introducere

Protecția datelor în Europa a început în anii 1970. De-a lungul anilor, instrumentele de asigurare a confidențialității datelor au fost diversificate și îmbunătățite, iar protecția datelor a devenit o valoare distinctă. În cadrul juridic al Uniunii Europene, protecția datelor este recunoscut ca drept fundamental.

Protecția datelor cu caracter personal este privită ca un drept modern și activ, punând în aplicare un sistem de control pentru a proteja persoanele ori de câte ori datele lor personale sunt prelucrate. Prelucrarea trebuie să se conformeze cu cerințele esențiale privind protecției datelor cu caracter personal, și anume monitorizarea independentă și respectarea drepturilor subiectului de date cu caracter personal.

Protecția datelor cuprinde toate tipurile de date cu caracter personal și metodele de prelucrare a datelor, indiferent de impactul acestora cauzat de încălcarea dreptului la viață privată.

Viața de zi cu zi devine din ce în ce mai digitalizată. Ritmul evoluțiilor tehnologiilor informaționale și modul în care datele personale sunt prelucrate ne afectează pe fiecare dintre noi, în contextul acestor schimbări. Prin urmare, este esențial să se evalueze gradul de pregătire al sistemului de control intern managerial al autorităților publice de a răspunde (pentru a ține sub control), în timp util, adecvat, calitativ și eficient, riscurilor din perspectiva a tuturor celor 3 aspectele instituționale:

- oameni;
- procese;
- tehnologii.

Scopul prezentului Ghid este:

- ✓ promovarea unei înțelegeri comune de către subdiviziunile de audit intern ale administrației publice privind terminologia aplicată în domeniul protecției datelor cu caracter personal, procesul și elementele acestuia, repartizarea de roluri și responsabilități;
- ✓ stabilirea scopului general, domeniului de aplicare, criteriilor de evaluare și structurii raportului de prezentare a rezultatelor auditului intern privind evaluarea procesului de prelucrare a datelor cu caracter personal în cadrul autorităților publice.

Ghidul are caracter de recomandare pentru subdiviziunile de audit intern și este aplicabil ținând cont de specificul activității de bază a instituției auditate și de nivelul de maturitate al sistemului de control intern managerial în cadrul acesteia.

Prezentul Ghid a fost elaborat în cadrul Proiectului UE ,,Suport în implementarea Misiunii Înalților Consilieri ai UE pentru RM", cu participarea experților Direcției politici în domeniul controlului financiar public intern a Ministerului Finanțelor, Centrului Național pentru Protecția Datelor cu Caracter Personal, auditorilor interni și experților în probleme de protecție a datelor cu caracter personal din sectorul public al Republicii Moldova.

1. Cadrul de reglementare

Domeniul protecției datelor cu caracter personal este reglementat prin următoarele acte normative de nivel național:

- Legea privind protecția datelor cu caracter personal nr.133 din 08.07.2011, *(Monitorul Oficial al RM, 2011, nr.170-175, art.492)*;

- Legea cu privire la aprobarea Regulamentului Centrului Naţional pentru Protecţia Datelor cu Caracter Personal structurii, personalului-limită şi a modului de finanțare a Centrului Naţional pentru Protecţia Datelor nr.182 din 10.07.2008, *(Monitorul Oficial al RM, 2008, nr.140-142, art.578)*;
- Legea pentru aprobarea Strategiei naționale în domeniului protecției datelor cu caracter personal pentru anii 2013-2018 și a Planului de acțiuni privind implementarea acesteia nr.229 din 10.10.2013, *(Monitorul Oficial al RM, 2013, nr.284-289, art.776)*;
- Hotărârea Guvernului privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal nr.1123 din 14.12.2010, *(Monitorul Oficial al RM, 2010, nr.254-256, art.1282).*

Cadrul european de reglementare și ghiduri (disponibile în engleză și română)**:**

- 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 (Regulamentul general privind protecția datelor), *în continuare GDPR*
  Sursa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679 ;
- DIRECTIVA (UE) 2016/680 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului
  Sursa: https://www.dataprotection.ro/servlet/ViewDocument?id=1263 ;
- DIRECTIVA (UE) 2016/681 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, Sursa: https://www.dataprotection.ro/servlet/ViewDocument?id=1264 ;
- Ghid privind protecția datelor (https://ec.europa.eu/newsroom/article29/items/612048/en);
- Ghid 4/2019 privind articolul 25 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en);
- Ghid privind evaluarea impactului privind protecția datelor (DPIA) (https://ec.europa.eu/newsroom/article29/items/611236/en);
- Ghid 05/2020 privind consimțământul în temeiul Regulamentului 2016/679 (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en);
- Ghid privind transparența conform Regulamentului 2016/679 (https://ec.europa.eu/newsroom/article29/items/622227/en);
- Ghid privind notificarea încălcării datelor cu caracter personal conform Regulamentului 2016/679 (https://ec.europa.eu/newsroom/article29/items/612052/en);
- Manual de legislație europeană privind protecția datelor, ediția 2018 (https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1).

2. Terminologie

Pentru a înțelege mai bine termenii folosiți în domeniul protecției datelor cu caracter personal, definițiile și explicația principalilor noțiuni sunt prezentate în Tabelul nr.1:

Date cu caracter personal:	orice informație referitoare la o persoană fizică identificată sau identificabilă („subiect al datelor cu caracter personal"); o persoană fizică identificabilă este acea persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale cum ar fi nume, prenume, date de localizare, un identificator online, sau la unul sau mai mulți factori specifici fiziculuí; identitatea fiziologică, genetică, mentală, economică, culturală sau socială a acelei persoane fizice. *(Sursa: Legea nr.133/2011, GDPR)* *Definiția datelor cu caracter personal se referă la informațiile disponibile sub orice formă, cum ar fi litere, cifre, grafice, fotografii sau audio. Definiția se aplică informațiilor stocate pe hârtie și informațiilor stocate electronic în memoria computerului sub formă de cod binar sau, de exemplu, capturate într-o înregistrare video. O astfel de abordare rezultă în mod logic din includerea prelucrării automate a datelor în definiția prelucrării datelor cu caracter personal. Din acest punct de vedere, datele de sunet și imagine în special sunt considerate date personale, deoarece oferă informații despre o persoană.*
Categorii speciale de date cu caracter personal:	date care dezvăluie originea rasială sau etnică, convingerile politice, religioase sau filozofice, apartenența socială; date genetice, date biometrice în scopul identificării unice a unei persoane fizice; datele privind sănătatea sau datele privind viața sexuală sau orientarea sexuală a unei persoane fizice, precum și datele referitoare la condamnări penale, sancțiuni administrative sau măsuri procedurale coercitive. *(Sursa: Legea nr.133/2011, GDPR)*
Date genetice:	date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care oferă informații unice despre fiziologia sau sănătatea acelei persoane fizice și care rezultă, în special, dintr-o analiză a unei probe biologice de la persoana fizică în cauză. *(Sursa: GDPR)*
Date biometrice:	datele cu caracter personal rezultate din prelucrarea tehnică specifică referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acelei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice. *(Sursa: GDPR)*
Date privind sănătatea:	date cu caracter personal legate de sănătatea fizică sau mintală a unei persoane fizice, inclusiv furnizarea de servicii de îngrijire a sănătății, care dezvăluie informații despre starea de sănătate a acesteia. *(Sursa: GDPR)*
Prelucrarea datelor cu caracter personal:	orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau punerea la dispoziție în orice alt mod, alinierea sau combinare, blocarea ștergere sau distrugere. *(Sursa: Legea nr.133/2011, GDPR)*
Operator:	persoana fizică sau juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor

	cu caracter personal prevăzute în mod expres de legislația în vigoare *(Sursa: Legea nr.133/2011, GDPR)*
Operatori comuni:	doi sau mai mulți operatori care stabilesc în comun scopurile și modalitatea de prelucrare a datelor cu caracter personal. *(Sursa: GDPR)*
Persoană împuternicită de către operator:	persoană fizică sau persoană juridică de drept public sau de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele operatorului, conform instrucțiunilor primite de la operator. *(Sursa: Legea nr.133/2011, GDPR)* *De exemplu, furnizorul serviciilor contabile contractate de instituție este „persoană împuternicită de către operator" în cadrul îndeplinirii acestei funcții specifice.*
Terț:	persoană fizică sau persoană juridică, de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator și decât persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal. *(Sursa: Legea nr.133/2011, GDPR)*
Destinatar:	orice persoană fizică sau persoană juridică, de drept public sau de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț. Nu sunt considerate destinatari organele din domeniul apărării naționale, securității statului și ordinii publice, organele de urmărire penală și instanțele judecătorești cărora li se comunică date cu caracter personal în cadrul exercitării competențelor stabilite de lege. *(Sursa: Legea nr.133/2011, GDPR)*
Sistemul de arhivare a datelor cu caracter personal:	orice set structurat de date cu caracter personal care sunt accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau dispersate pe o bază funcțională sau geografică. (*(Sursa: Legea nr.133/2011, GDPR)*
Consimțământul subiectului de date cu caracter personal:	manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate. *(Sursa: Legea nr.133/2011, GDPR)*
Creare de profiluri:	orice formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prezice aspecte referitoare la performanța acelei persoane fizice la locul de muncă, situația economică, sănătatea, preferințele personale, interesele respective, fiabilitate, comportament, locație sau mișcarea persoanei respective. *(Sursa: Legea nr.133/2011, GDPR)*
Depersonalizarea datelor/ Pseudonimizare:	prelucrarea datelor cu caracter personal în așa fel încât datele cu caracter personal să nu mai poată fi atribuite unei anumite persoane vizate fără a se utiliza unor informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure că datele personale nu sunt atribuite unei persoane fizice identificate sau identificabile. *(Sursa: Legea nr.133/2011, GDPR)*

	Exemplu de depersonalizare este utilizarea unui cod criptat în loc de numele, prenumele și codul personal al unei persoane.
Anonimizare:	un proces de prelucrare a datelor cu caracter personal în care datele individuale identificabile sunt schimbate astfel încât să nu mai poată fi asociate cu persoana respectivă. *(Sursa: GDPR)* *Datele anonime sunt informații care nu se referă la o persoană fizică identificată sau identificabilă sau la date personale. Pseudonimizarea nu este același lucru cu anonimizarea. Criptarea nu este o tehnică de anonimizare, dar este un instrument de pseudonimizare.*
Încălcarea protecției datelor cu caracter personal:	o încălcare a securității care duce la distrugerea accidentală sau ilegală, pierderea, modificarea, dezvăluirea neautorizată sau accesarea datelor personale transmise, stocate sau prelucrate. *(Sursa: GDPR)*
Autoritatea de supraveghere:	o autoritate publică autonomă, independentă de alte autorități publice, responsabilă de monitorizarea aplicării legislației, în scopul protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. *(Sursa: Legea nr. 182/2008, Legea nr.133/2011, GDPR)* *În Republica Moldova autoritatea de supraveghere este Centrul Național pentru Protecția Datelor cu Caracter Personal, organ de control al prelucrării datelor cu caracter personal.*

Exemple de date cu caracter personal

➢ Nume, prenume, cod personal (IDNP)	*Date personale*
➢ Conversație audio	*În cazul în care, folosind serviciile unei instituții, vocea clientului atunci când face o solicitare verbală sau o cerere de informare este înregistrată pe bandă, înregistrarea audio a acestor informații trebuie să fie considerată ca fiind date cu caracter personal.*
➢ Supraveghere video	*Imaginile persoanelor surprinse de un sistem de supraveghere video pot fi date cu caracter personal în situația în care acele persoane sunt identificabile. Chiar dacă calitatea imaginii obținute este slabă, iar scopul obținerii acestora a fost identificarea persoanei, atunci imaginile de calitate slabă de asemenea sunt considerate date cu caracter personal.*
➢ Desenul copilului	*Într-un proces de judecată pentru custodia unui copil, desenul familiei sale reprezintă rezultatul testului ei neuropsihiatric. Desenul oferă informații despre starea de spirit a fetei și despre sentimentele ei față de diverși membri ai familiei. Un astfel de desen poate fi considerat drept „date cu caracter personal". Desenul va dezvălui informații despre fată însăși (starea ei psihologică de sănătate) sau, de exemplu, despre comportamentul tatălui sau al mamei sale. Părinții își pot exercita dreptul de acces la aceste informații în acest caz.*
➢ Adresa de e-mail	*O adresă de email care conține numele și prenumele deplin al persoane este considerată date cu caracter personal - nume.prenume@numedomeniu.md – deoarece această adresă de e-mail indică numele, prenumele și apartenența acestei persoane la instituție etc..* *Pe de altă parte, adresa de e-mail simplificată - nume_u@xxxxx.md - este considerată ca fiind una care nu conține date personale, deoarece nu poate fi folosită pentru a identifica direct persoana.* *Excepție este situația dacă numele persoanei este unic, de exemplu, există doar câteva persoane cu acest nume în Republica Moldova, atunci o anumită persoană poate fi identificată cu adresa de e-mail simplificată*
➢ Publicarea radiografiei și a numelui pacientului	*Un jurnal științific a publicat o imagine a radiografiei unei persoane împreună cu numele acesteia, care este foarte deosebit. Numele, prenumele împreună cu cunoașterea faptului că persoana are o anumită maladie, ajunge identificabil pentru un anumit cerc de persoane. Prin urmare, radiografia ar trebui să fie considerată date cu caracter personal.*
➢ Datele unei persoane decedate	*În principiu, informațiile referitoare la persoanele decedate nu sunt considerate date cu caracter personal, deoarece conform dreptului civil, decedații nu sunt persoane fizice. Cu toate acestea, în unele cazuri, datele persoanei decedate necesită a fi protejate, pentru a proteja indirect datele altor persoane vii. De exemplu, informațiile că persoana decedată **A** avea hemofilie indică faptul că și fiul ei **B** are aceeași boală, deoarece este legată de o genă situată pe cromozomul **X**. Astfel, în cazurile în care se*

	poate considera că informațiile despre persoanele decedate se aplică în același timp și persoanelor în viață, acestea sunt considerate date cu caracter personal, care sunt reglementate de legislația privind protecția datelor cu caracter personal.
➢ Valoarea imobilului	*Valoarea unui imobil este informație despre obiect. Reglementările privind protecția datelor cu caracter personal nu se vor aplica acestor tipuri de informații dacă sunt folosite doar pentru a descrie nivelul prețurilor imobiliare într-o anumită zonă. Cu toate acestea, în anumite cazuri, astfel de informații ar trebui considerate date cu caracter personal, de exemplu, dacă imobilul este deținută de o persoană și valoarea acesteia va fi utilizată pentru a determina obligația acelei persoane de a plăti anumite impozite. Din acest punct de vedere, informațiile trebuie considerate date personale.*
➢ Adresa IP (internet protocol)	*Adresele IP ar trebui să fie considerate date referitoare la o persoană identificabilă. Furnizorii de servicii de comunicații electronice (furnizorii de internet), folosind mijloace rezonabile, identifică utilizatorii de internet cărora le-au atribuit adrese IP, „înregistrând" în mod regulat într-un fișier separat data, ora și termenul de atribuire a adresei dinamice de IP atribuite utilizatorului de internet și cât timp a fost utilizat. Furnizorii de servicii de comunicații electronice, care mențin un jurnal de registru pe un server de Internet, fac același lucru. Nu există nicio îndoială că în aceste cazuri datele personale trebuie să fie protejate. În special în cazurile în care prelucrarea adresei IP este efectuată cu intenția de a identifica utilizatorii de computer (de exemplu, deținătorii de drepturi de autor al căror scop este urmărirea penală a utilizatorilor de computer pentru încălcarea drepturilor de proprietate intelectuală), operatorul demonstrează în prealabil că „înseamnă că poate fi folosit în mod rezonabil", pentru a identifica persoana fizică va fi disponibilă, de exemplu, instanței la care va fi depusă cererea, iar astfel aceste informații sunt considerate date cu caracter personal.*

3. Principii de bază

Operatorul este responsabil pentru planificarea, implementarea, menținerea, monitorizarea și îmbunătățirea sistemului de protecție a datelor cu caracter personal din cadrul instituției, precum și este responsabil și ar trebui să poată demonstra conformitatea cu principiile de bază referitoare la prelucrarea datelor cu caracter personal care se referă la:

Legalitate, corectitudine și transparență:

- Principiile legalității, echității și transparenței se aplică tuturor operațiunilor de prelucrare a datelor cu caracter personal
- Legalitatea cere să fie:
  - consimțământul persoanei vizate;
  - necesitatea încheierii unui contract;
  - obligație legală;
  - necesitatea de a proteja interesele vitale ale persoanei vizate sau ale altei persoane;
  - necesitatea îndeplinirii unei sarcini de interes public;
  - necesitate pentru interesele legitime ale operatorului sau ale unui terț, dacă acestea nu sunt depășite de interesele și drepturile persoanei vizate.
- Prelucrarea datelor cu caracter personal ar trebui să se facă într-un mod echitabil.
  - Persoana vizată trebuie informată cu privire la riscuri pentru a se asigura că prelucrarea nu are efecte negative imprevizibile.
- Prelucrarea datelor cu caracter personal ar trebui să se facă într-o manieră transparentă.
  - Operatorii trebuie să informeze persoanele vizate înainte de a le prelucra datele despre scopul prelucrării și despre identitatea și adresa operatorului;
  - Informațiile privind operațiunile de prelucrare trebuie furnizate într-un limbaj clar și simplu, pentru a permite persoanelor vizate să înțeleagă cu ușurință regulile, riscurile, garanțiile și drepturile implicate;
  - Persoanele vizate au dreptul de a-și accesa datele oriunde sunt prelucrate.

Limitarea scopului:

- Scopul prelucrării datelor trebuie definit înainte de începerea procesării.
- Nu poate exista o prelucrare ulterioară a datelor într-un mod care să fie incompatibil cu scopul inițial, deși există excepții de la această regulă în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică, precum și în scopuri statistice.
- În esență, principiul limitării scopului înseamnă că orice prelucrare a datelor cu caracter personal trebuie să se facă într-un scop specific bine definit și numai pentru scopuri suplimentare, specificate, care sunt compatibile cu cel inițial.

Minimizarea datelor:

- Prelucrarea datelor cu caracter personal trebuie să se limiteze la ceea ce este necesar pentru a îndeplini un scop legitim.
- Prelucrarea datelor cu caracter personal ar trebui să aibă loc numai atunci când scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace.
- Prelucrarea datelor cu caracter personal nu poate interfera în mod disproporționat cu interesele, drepturile și libertățile.

Precizia datelor:

- Principiul acurateței datelor trebuie implementat de către operator în toate operațiunile de prelucrare.
- Datele inexacte trebuie șterse sau rectificate fără întârziere.
- Este posibil ca datele să fie verificate în mod regulat și menținute la zi pentru a asigura acuratețea.

Limitarea stocării:

- Principiul limitării stocării înseamnă că datele cu caracter personal trebuie șterse sau anonimizate de îndată ce nu mai sunt necesare în scopurile pentru care au fost colectate.

Integritate și confidențialitate:

- Securitatea și confidențialitatea datelor cu caracter personal sunt esențiale pentru prevenirea efectelor adverse pentru persoana vizată.
- Măsurile de securitate pot fi de natură tehnică și/sau organizatorică.
- Depersonalizarea este un proces care poate proteja datele personale.
- Nivelul adecvat al măsurilor de securitate trebuie să fie determinat de la caz la caz și revizuită în mod regulat.

Responsabilitate:

- Responsabilitatea cere operatorilor și persoanelor împuternicite de către operatori să implementeze în mod activ și continuu măsuri pentru a proteja protecția datelor cu caracter personal în procesul de prelucrare a acestora.
- Operatorii și persoanele împuternicite de către operatori sunt responsabili pentru conformitatea proceselor de prelucrare cu Legea privind protecția datelor cu caracter personal, corespunzător obligațiilor ce le revin.
- Operatorii trebuie să fie în măsură să demonstreze, în orice moment, persoanelor vizate, publicului larg și autorităților de supraveghere, conformitatea cu prevederile cadrului normativ privind protecția datelor cu caracter personal (cum ar fi păstrarea unei evidențe a operațiunilor de prelucrare, numirea unui responsabil cu protecția datelor, etc.).

4. Misiunea de audit intern orizontal

1.	**Titlul misiunii de audit Universului de audit**	Evaluarea procesului de prelucrare a datelor cu caracter personal în cadrul autorităților publice *Având în vedere că, în general, datele cu caracter personal sunt prelucrate în toate procesele administrației publice și se suprapun cu întregul univers de audit intern (sisteme operaționale, de management și de suport), subdiviziunea de audit intern va planifica acest audit ca misiune de audit separată în planul anual de activitate, în care sistemul de control intern managerial este evaluat pe orizontal.*
2.	**Tip de audit intern**	Auditul de conformitate
3.	**Posibile riscuri, puncte slabe ale procesului auditat**	✓ Reglementările/procedurile interne cu privire la prelucrarea datelor cu caracter personal lipsesc sau sunt generale, inconsecvente în conținut, contradictorii sau nu sunt actualizate; ✓ Nedesemnarea responsabilului de protecția datelor cu caracter personal sau atribuirea acestei funcții unei persoane care nu corespunde cerințelor; ✓ Responsabilul de protecția datelor cu caracter personal are cunoștințe profesionale specifice insuficiente, îndeplinirea formală a atribuțiilor delegate; ✓ Măsuri tehnice și organizatorice inadecvate, neclare, de calitate scăzută pentru a asigura protecția datelor cu caracter personal; ✓ Responsabilitatea pentru asigurarea conformității prelucrării datelor cu caracter personal este impusă fiecărui angajat, fără asigurarea de resurse și competențe (cunoștințe) suficiente. Instruirea angajaților cu privire la protecția datelor cu caracter personal neregulată și generală; ✓ Prelucrarea datelor cu caracter personal fără consimțământul persoanelor vizate (subiecților) sau în baza consimțământului formulat incorect; ✓ Colectarea și stocarea datelor cu caracter personal fără un scop anume, justificat printr-un temei juridic, sau în cantități excesive, nejustificate. Păstrarea datelor cu caracter personal pe un termen mai lung decât cel stabilit întru atingerea scopului pentru care au fost colectate; ✓ Utilizarea datelor cu caracter personal în scopuri neautorizate; ✓ Oferirea accesului neautorizat la date cu caracter personal, transferul neautorizat a datelor către terți; ✓ Neasigurarea evidenței accesării datelor cu caracter personal; ✓ Încălcări ale drepturilor subiecților datelor cu caracter personal, refuzul de a le furniza informații privind accesarea datelor personale; ✓ Managementul inadecvat al incidentelor de scurgere a datelor cu caracter personal.

4.	**Obiectivul general al auditului**	De a evalua conformitatea protecției datelor cu caracter personal cu reglementările aplicabile în domeniu și a oferi asigurare că prelucrarea datelor cu caracter personal în entitate este efectuată legal, responsabil, corect și transparent în raport cu subiecții acestor date.
5.	**Obiective specifice ale auditului**	Pentru a atinge obiectivul general al auditului intern, echipa de audit intern va asigura: 1) Evaluarea cadrului intern de guvernare (reglementare și delegare de atribuții) cu referire la protecția datelor cu caracter personal, prin prisma calității și actualității acestuia; 2) Evaluarea conformității operațiunilor de colectare, prelucrare și stocare a datelor cu caracter personal; 3) Analiza faptului dacă măsurile tehnice și organizatorice introduse pentru asigurarea confidențialității și protecția datelor cu caracter personal, la toate etapele de prelucrare a acestora, sunt suficiente și funcționale; 4) Obținerea asigurării rezonabile cu privire la respectarea de către entitate a drepturilor subiecților datelor cu caracter personal; 5) Evaluarea modului de gestionare a incidentelor de încălcări admise de către entitate cu privire la protecția datelor cu caracter personal.
6.	**Aria de aplicabilitate a auditului**	În cadrul misiunii, echipa de audit intern va supune evaluării operațiunile de colectare, prelucrare și stocare a datelor cu caracter personal în cadrul sistemelor operaționale, de management și de suport ale entității, prin prisma conformității cu normele și procedurile aferente, precum și stabilirii activităților de control pentru asigurarea confidențialității și protecției datelor cu caracter personal și respectării drepturilor subiecților acestora.
7.	**Perioada de audit**	Cu anumite rezerve și excepții eventual stabilite de echipa de audit la etapa lucrului în teren, ținând cont de specificul riscurilor identificate și, respectiv, a testelor planificate, perioada supusă evaluării este anul 2023 (până la începerea misiunii de audit).
8.	**Limitele auditului intern**	Ca parte a misiunii de audit intern orizontal nu vor fi evaluate următoarele: ✓ conformitatea și eficacitatea funcționării Centrului Național pentru Protecția Datelor cu Caracter Personal; ✓ implementarea Strategiei naționale în domeniul protecției datelor cu caracter personal pentru anii 2013-2018 (Legea nr. 229/2013); ✓ conformitatea proiectării și funcționarii sistemelor informaționale utilizate în procesul de prelucrare a datelor cu caracter personal; ✓ prelucrarea datelor cu caracter personal atribuite la secret de stat, precum și altor date care nu formează domeniul de

		aplicare a Legii nr. 133/2011 privind protecția datelor cu caracter personal.
9.	**Metodologia de audit:**	Misiunea de audit se va desfășura în conformitate cu standardele naționale de audit intern (SNAI), Normele metodologice de audit intern în sectorul public și alte acte normative care reglementează activitatea respectivă, după caz, cu aplicarea procedurilor interne de desfășurare a activității de audit intern. Auditorii interni au angajamentul de a asigura respectarea principiilor fundamentale de integritate, independență și obiectivitate, competență și confidențialitate. În vederea neadmiterii unor eventuale conflicte de interese, la etapa de inițiere a misiunii, fiecare auditor implicat în misiunea de audit semnează Declarația de interese. Datele cu caracter personal utilizate pentru documentarea probelor de audit vor fi depersonalizate. Activitățile desfășurate pe parcursul misiunii de audit vor fi supervizate și evaluate în conformitate cu prevederile Programului de asigurare și îmbunătățire a calității activității de audit intern. Misiunea de audit cuprinde următoarele etape: ***(i)*** *planificarea misiunii;* ***(ii)*** *lucrul în teren;* ***(iii)*** *raportare;* ***(iv)*** *monitorizarea implementării recomandărilor de audit:* ➢ **Etapa de planificare** include o examinare a informațiilor de fond, după caz interviuri cu managerii și personalul cheie din cadrul unităților auditate. Această etapă urmărește evaluarea preliminară a riscurilor, înțelegerea domeniului auditat și a documentării sistemelor (proceselor) existente, stabilirea obiectivelor specifice de audit, ariei de aplicabilitate și criteriilor de evaluare, determinarea calendarului activităților, etc., care vor fi prezentate și puse în discuție în cadrul ședinței de deschidere a misiunii de audit. Totodată, se elaborează Programul de lucru în teren, cu specificarea termenelor limită de realizare și a responsabililor pentru fiecare activitate / test. ➢ **Etapa lucrului în teren** include colectarea și analiza probelor de audit, prin realizarea testelor conform Programului de lucru aprobat, analiza rezultatelor acestora și formularea variantei preliminare a constatărilor și recomandărilor. Pentru realizarea obiectivelor misiunii de audit, activitatea în teren a echipei de audit va fi efectuată în două etape după cum urmează: 1. Persoanele responsabile din cadrul entității care gestionează date cu caracter personal sunt rugate să completeze un Chestionar de autoevaluare a controlului intern instituit în domeniul protecției datelor cu caracter personal (Anexa nr. 1 la Ghid). 2. În baza examinării rezultatelor autoevaluării efectuate și analizei preliminare a procesului auditat (inclusiv evaluarea riscurilor, evaluarea proiectării activităților de control, rezultatele auditurilor interne și externe anterioare, alte informații relevante), echipa de audit:

		2.1. decide să se bazeze pe rezultatele autoevaluării și să nu efectueze verificări detaliate suplimentare pe anumite aspecte sau sisteme de gestionare a datelor cu caracter personal. Dacă este necesar, auditorul poate adresa întrebări suplimentare cu privire la informațiile incluse în chestionarul de autoevaluare, dacă răspunsurile nu sunt corecte sau nu oferă dovezi suficiente cu privire la funcționarea sistemului de control intern managerial pentru protecția datelor cu caracter personal; 2.2. decide să efectueze verificări detaliate. În funcție de volumul de lucru în raport cu resursele alocate, echipa de audit va utiliza eșantionarea în baza raționamentului profesional pentru obținerea probelor suficiente prin analiza unui număr mai mic de elemente. Echipa de audit prezintă o justificare scrisă în documentele de lucru cu privire la deciziile luate. Versiunea preliminară a constatărilor și recomandările de audit urmează a fi discutate cu reprezentanții unităților auditate până la finalizarea lucrului în teren, fie în cadrul unei ședințe de finalizare a lucrului în teren. ➢ **Etapa de raportare** include elaborarea și prezentarea proiectului raportului de audit unităților auditate, care în termen de 5 zile va prezenta comentarii (reacția de răspuns) și/sau după caz un proiect a planului de implementare a recomandărilor de audit. În rezultatul analizei reacției de răspuns, echipa de audit va ajusta raportul de audit și/sau va include în raport comentariile recepționate. Rezultatele auditului vor fi prezentate în cadrul ședinței de închidere a misiunii. Rezultatele auditului vor fi prezentate Ministerului Finanțelor, în formatul prestabilit, până la data de 29.12.2023. ➢ **Urmărire implementării recomandărilor** va fi efectuată ulterior, în baza măsurilor stabilite în planul de acțiuni aprobat în acest scop.
7.	**Criterii de evaluare**	Criteriile de evaluare derivă din cerințele cadrului normativ național în domeniul prelucrării și protecției datelor cu caracter personal, precum și din aspecte de bune practici preluate din legislația Uniunii Europene, în special Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului - Regulamentul general privind protecția datelor. Un set de criterii de evaluare sunt prezentate în anexa nr. 1 la Ghid.
8.	**Metode și tehnici de audit utilizate**	În cadrul lucrului în teren, echipele de audit vor utiliza următoarele tehnici și instrumente de colectare a probelor / datelor: ✓ chestionarul de Control intern, pentru organizarea autoevaluării procesului de prelucrare și protecție a datelor cu caracter personal în cadrul entității; ✓ interviuri cu conducerea superioară a entității, responsabilul de protecția datelor cu caracter personal, personal

		responsabil de colectarea, prelucrarea și stocarea datelor cu caracter personal; ✓ verificarea documentelor (regulamente interne, proceduri, registre, contracte, fișe de post, rapoarte etc.); ✓ după caz, observări fizice directe, simularea situației, etc..

5. Procedura de transmitere a rezultatelor auditului intern către Ministerul Finanțelor

Subdiviziunile de audit intern din cadrul ministerelor și altor autorități publice centrale de specialitate vor transmite Ministerului Finanțelor Raportul privind rezultatele auditului intern orizontal privind evaluarea procesului de prelucrare a datelor cu caracter personal până la data de **29 decembrie 2023**. Modelul de raport este prezentat în Anexa 2 la Ghid.

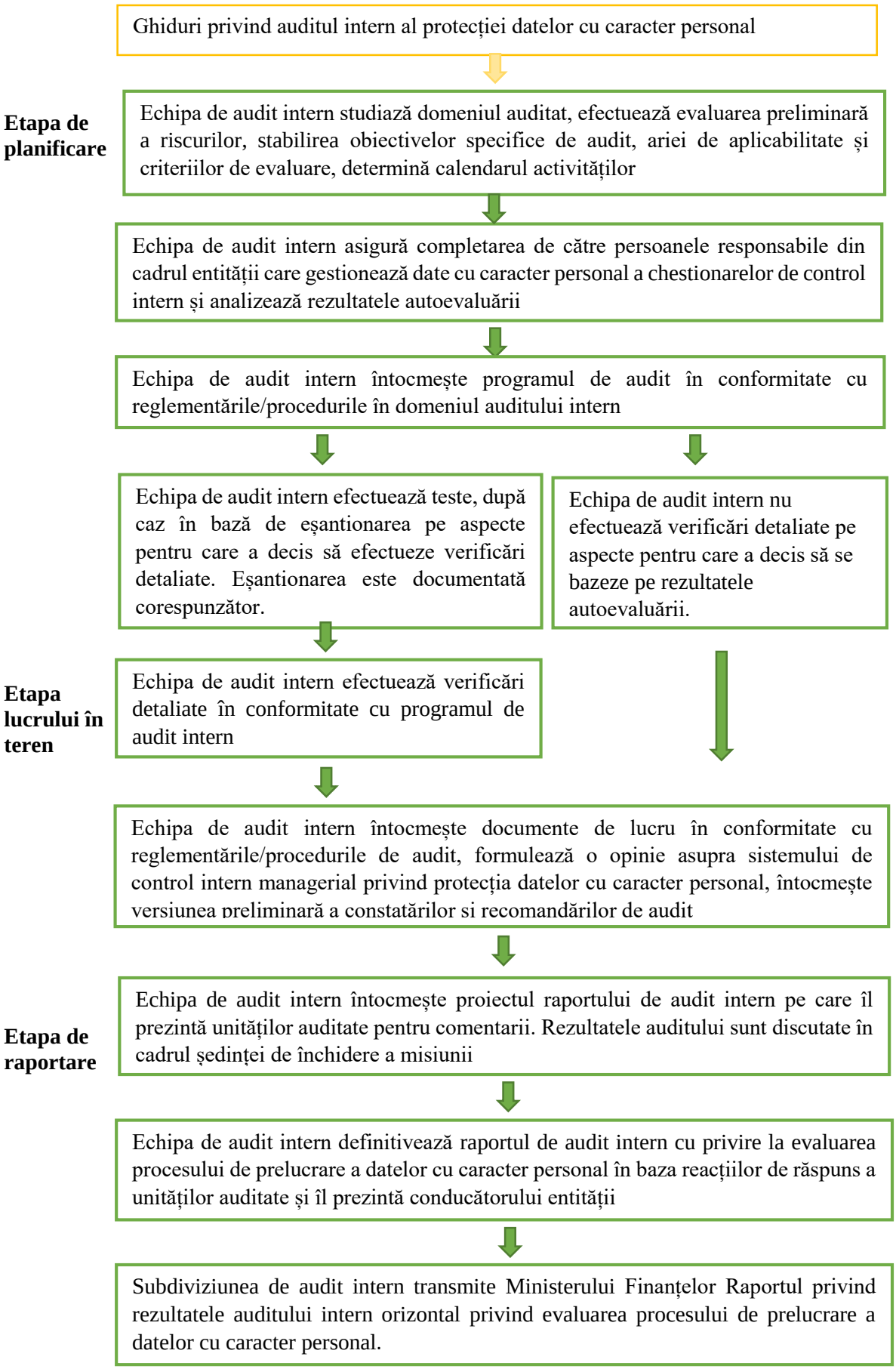
Ministerul Finanțelor va generaliza rezultatele auditului intern orizontal. Pentru a se asigura că informațiile privind sistemul de protecție a datelor cu caracter personal din entitățile incluse în raportul de sinteză sunt relevante, complete, exacte și inteligibile, Ministerul Finanțelor va evalua necesitatea organizării de întâlniri/discuții individuale cu fiecare echipă de audit intern.

Rezumatul principalelor constatări și recomandări de audit vor fi prezentate Guvernului în Raportul anual consolidat privind controlul financiar public intern pentru anul 2024.

Având în vedere sfera de aplicare a misiunii de audit intern orizontale definită în prezentul Ghid, pașii care trebuie întreprinși de subdiviziunea de audit intern sunt reflectați în Figura 1.

Figura 1

Etape de realizare a auditului intern orizontal



6. Anexe

1. Anexa nr. 1. Chestionar de autoevaluare / Criterii de evaluare privind funcționarea sistemului de protecție a datelor cu caracter personal, pe 6 pagini.
2. Anexa nr. 2. Model al Raportului privind rezultatele auditului intern orizontal privind evaluarea procesului de prelucrare a datelor cu caracter personal, pe 6 pagini.

Anexa nr. 1
la Ghidul de audit intern privind
protecția datelor cu caracter personal

Chestionar de autoevaluare a controlului intern instituit asupra procesului de prelucrare și protecției datelor cu caracter personal[1]

	Criteriu de evaluare	Comentariu, referire la documente justificative
I. Cadrul de guvernare	În cadrul entității este aprobată o politică* privind prelucrarea și protecția datelor cu caracter personal, inclusiv securitatea sistemului informațional? Aceasta este adusă la cunoștință angajaților care prelucrează/au acces la date cu caracter personal, în limitele competenţelor funcţionale? ** proceduri, regulile interne care reglementează principiile prelucrării și protecției datelor cu caracter personal, obligațiile și responsabilitățile angajaților în prelucrarea datelor cu caracter personal, nivelului de acces acordat, etc.*	*Vă rugăm să descrieți modul în care entitatea organizează prelucrarea și protecția datelor cu caracter personal cu referire la reglementările interne.*
	Politica privind prelucrarea și protecția datelor cu caracter personal este revizuită sistematic (cel puţin o dată pe an)? Când au fost actualizate ultima dată reglementările interne?	
	Entitatea oferă angajaților (inclusiv a celor care prelucrează zilnic date cu caracter personal) instruire în domeniul prelucrării și protecției datelor cu caracter personal? Cum obține entitatea asigurare cu privire la nivelul de cunoștințe al angajaților în acest domeniu?	*Descrieți:* *- Dacă instruirea este obligatorie? Unde are loc?* *- Cât de regulat este organizată?* *- Când a fost desfășurată ultima dată?* *- Câți angajați sunt instruiți?* *După caz, vă rugăm să anexați un plan de formare profesională.*
	Fiecare subdiviziune cunoaște procesele pentru care este necesară colectarea, prelucrarea și stocarea datelor cu caracter personal?	
	În cadrul entității (sau persoanei împuternicite) este desemnată subdiviziunea / persoana responsabilă cu protecția datelor cu caracter personal? Se asigură continuitatea atribuțiilor delegate în timpul absenței temporare, suspendării sau încetării raporturilor de serviciu a responsabilului cu protecția datelor?	*Descrieți:* *- Ce măsuri au fost întreprinse pentru a asigura continuitatea îndeplinirii atribuțiilor/sarcinilor delegate persoanei responsabile cu protecția datelor cu caracter personal, precum și disponibilitatea documentelor și dosarelor de lucru în timpul absenței acestuia? Vă rugăm să anexați actul administrativ de delegare.*

[1] Chestionarul de autoevaluare se completează de către unitatea auditată. Dacă este necesar, echipa de audit poate include întrebări suplimentare de clarificare.

I. Cadrul de guvernare	În baza cărei proceduri și criterii a fost selectată subdiviziunea/persoana pentru îndeplinirea atribuțiilor de responsabilă cu protecția datelor cu caracter personal?	*Vă rugăm să descrieți dacă persoana responsabilă cu protecția datelor cu caracter personal are o calificare profesională în domeniul dreptului și practicii privind protecția datelor? Vă rugăm să anexați fișa(-ele) postului.*
	Ce proceduri interne stabilesc: • obligația responsabilului cu protecția datelor cu caracter personal de a raporta conducerii superioare cu privire la aspectele legate de protecția datelor; • resursele necesare responsabilului cu protecție datelor cu caracter personal; • independența și competențele persoanei responsabile cu protecția datelor cu caracter personal; • prevenirea conflictului de interese al persoanei responsabile cu protecția datelor cu caracter personal, în procesul exercitării atribuțiilor și responsabilităților delegate.	*Descrieți:* *- În cazul în care atribuțiile persoanei responsabile cu protecția datelor cu caracter personal sunt combinate cu alte sarcini/funcții, ce aspecte au fost evaluate pentru a asigura independența acestuia, pentru a evita conflictele de interese și pentru a asigura resurse suficiente corespunzător volumului de muncă aferent protecției datelor cu caracter personal?* *Referire la reglementări/proceduri interne*
	Cum se asigură faptul că persoana responsabilă cu protecția datelor este implicată în mod corespunzător și în timp util în toate problemele legate de protecția datelor cu caracter personal în cadrul entității?	*Vă rugăm să indicați în ce procese/probleme este implicată persoana responsabilă cu protecția datelor cu caracter personal.* *Referire la reglementări/proceduri interne.*
	Cum se asigură că persoana responsabilă cu protecția datelor cu caracter personal își menține și își îmbunătățește calificările *(participă la cursuri de dezvoltare profesională în domeniul protecției datelor cu caracter personal, își actualizează cunoștințele și abilitățile în domeniul legislației și practicii privind protecția datelor)*?	*Plan de instruire.* *Cursuri de formare și perfecționare a calificărilor urmate în ultimii ani.*
	Au fost publicate/actualizate datele de contact ale subdiviziunii/persoanei responsabile cu protecția datele cu caracter personal? Acestea au fost comunicate angajaților entității?	*Ce informații au fost publicate? Referință/link către pagina web a entității unde au fost publicate informațiile.*
	A fost informat Centrul Național pentru Protecția Datelor cu Caracter Personal cu privire la desemnarea subdiviziunii/persoanei responsabile cu protecția datelor?	*Trimitere la scrisoarea de notificare/informații.*

II. Colectarea, prelucrarea și stocarea datelor cu caracter personal	În cadrul entității se ține un registru de sisteme/procese de prelucrare a datelor cu caracter personal *(care include informații privind categoriile de date colectate, scopul colectării și prelucrării datelor, categorii de subiecți a căror date sunt prelucrate, termene de păstrare, subdiviziunile implicate în prelucrarea datelor, sistemele de arhivare a datelor, etc.)*? Este acest registru actualizat sistematic?	*Specificați persoanele responsabile de ținerea registrului.*
	Datele cu caracter personal sunt colectate de entitate în scopuri determinate, explicite și legitime, adecvate, pertinente și neexcesive în ceea ce servește scopul pentru care sunt colectate? Specificați dacă se efectuează o analiză a justificării legale* a prelucrării datelor cu caracter personal. ** prelucrarea datelor se face în temeiul cadrului normativ, cerințelor contractuale, drepturilor legitime ale operatorului, etc.*	*Specificați:* *- Care sunt rezultatele evaluării?* *- Unde și cum sunt documentate aceste rezultate?* *- A participat persoana responsabilă cu protecția datelor la pregătirea documentului de evaluare?* *Referință la documentul de evaluare.*
	Datele cu caracter personal sunt colectate pe baza consimțământului subiectului datelor (persoanei vizate)? Subiecții datelor cu caracter personal sunt informați cu privire la scopul prelucrării datelor colectate?	
	Sunt prescrise și implementate măsuri tehnice și organizatorice adecvate pentru prelucrarea datelor cu caracter personal?	*Vă rugăm să descrieți măsurile aplicate.* *Referire la reglementări interne.*
	Datele cu caracter personal se stochează și se păstrează numai în scopurile pentru care au fost colectate? Datele se păstrează doar pentru perioada strict necesară atingerii scopurilor pentru care au fost colectate, fiind păstrate întru-un mediu sigur?	
	Ce cadru de reglementare (politica internă) stabilește termenele limită de stocare a datelor cu caracter personal, procedura de depersonalizare și de distrugere a datelor (pe suport hârtie și în format electronic)?	*Când au fost revizuite ultima dată termenele și procedurile?* *Persoana responsabilă cu protecția datelor cu caracter personal a participat la evaluarea acestora?* *Referiri la reglementări/proceduri interne.*

III. Asigurarea confidențialității și protecția datelor cu caracter personal	În cadrul entității este restricționat accesul la datele cu caracter personal? Doar acei angajați care prelucrează datele cu caracter personal au acces la acestea?	
	Obligațiunile de asigurare a confidențialității datelor cu caracter personal sunt reglementate printr-un act juridic (contract/declarație/etc.)?	
	Ce măsuri tehnice și organizatorice au fost stabilite și implementate în entitate pentru a asigura în mod eficient protecția și confidențialitatea datelor cu caracter personal?	*Vă rugăm să descrieți măsurile aplicate. Referire la reglementări/proceduri interne.*
	Sunt implementate condițiile/criteriile de evaluare și verificare a eficacității măsurilor tehnice și organizatorice de protecție a datelor cu caracter personal?	*Unde sunt definite aceste condiții și criterii? Când a fost efectuată ultima dată evaluarea conform acestor condiții și criterii? Cât de regulată este efectuată evaluarea? Cum și unde sunt documentate rezultatele acestei evaluări?*
	Entitatea implementează mecanisme de înregistrare și evidenţă a persoanelor care au accesat și/sau au realizat operațiuni de prelucrare a datelor cu caracter personal. Aceste înregistrări permit identificarea cazurilor de accesare neautorizată sau de prelucrare ilegală a datelor cu caracter personal?	
	Accesul în sediile/oficiile/birourile unde sunt amplasate sistemele informaționale (alte tipuri de sisteme de arhivare) de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară și doar în timpul orelor de program? Liste de acces sunt actualizate sistematic (nu mai rar decât o dată în lună)?	
	Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori?	
	În cadrul entității se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor de autentificare la sistemele informaționale de date cu caracter personal?	*Acestea reguli includ:* ✓ *păstrarea confidenţialităţii parolelor;* ✓ *interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;* ✓ *modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri ale sistemului sau parolei;* ✓ *alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice*

		consecutive şi nu sunt compuse integral din grupuri de cifre sau litere; ✓ *modificarea parolelor peste intervale de maximum 3 luni;* ✓ *dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).*
	Au fost încheiate contracte de externalizare pentru întreținerea / exploatarea/ elaborarea /dezvoltarea etc. a sistemelor informaționale destinate prelucrării datelor cu caracter personal? Cum se obțin asigurări că procesatorii angajați asigură o prelucrare adecvată a datelor cu caracter personal și protecția drepturilor subiecților acestor date?	*Vă rugăm să specificați contractul de externalizare.*
	Folosește entitatea metode de transfer de date cu caracter personal prin canale de comunicare internă și externă (de exemplu: prin e-mail, transmitere a fișierelor, documentelor pe suport de hârtie, etc.)? Sunt stabilite proceduri de transmitere securizată a datelor? Entitatea folosește metode securizate de transfer de date?	*Vă rugăm să indicați ce documente reglementează comunicarea internă și externă sigură a datelor cu caracter personal în entitate?* *Când a efectuat persoana responsabilă cu protecția datelor cu caracter personal o evaluare a securității transferului de date? Care sunt rezultatele acestei evaluări?*
	Dacă datele cu caracter personal sunt trimise către țări terțe, ce măsuri de securitate organizatorică și tehnică sunt prevăzute pentru transferul de date? Ce mecanisme legale de transfer de date se aplică?	*Dacă astfel de date există, vă rugăm să indicați tipurile de prelucrare a datelor cu caracter personal, să indicați justificarea legală.* *Descrieți ce măsuri de securitate sunt prevăzute pentru astfel de date sau identificați cadrul de reglementare în care sunt stipulate.*
III (a) Evaluarea impactului privind protecția datelor cu caracter personal	Entitatea a identificat operațiunile de prelucrare a datelor cu caracter personal, care implică un risc sporit pentru drepturile și libertățile persoanelor? A fost efectuată o evaluare a impactului pentru prelucrarea datelor cu risc ridicat?	*Vă rugăm să enumerați metodele de procesare a datelor cu risc sporit în entitate.* *Furnizați dovezi (registru, document etc.) pe baza cărora este posibil să obțineți asigurarea că evaluarea impactului prelucrării datelor cu risc sporit este efectuată în practică și este adecvată.*
	Specificați pentru ce tip de prelucrare a datelor cu caracter personal se efectuează o evaluare de impact? Care este justificarea pentru a face evaluarea impactului?	*Vă rugăm să oferiți o justificare pentru efectuarea evaluării de impact.*
	Cine este responsabil pentru realizarea evaluării impactului privind protecția datelor cu caracter personal? Persoana responsabilă cu protecția datelor cu caracter personal este implicată în realizarea evaluării impactului?	
	Este stabilită o procedură de detectare a modificărilor riscurilor? Sunt evaluările de impact privind protecția datelor cu caracter personal revizuite în urma modificării riscurilor?	*Vă rugăm să descrieți măsurile aplicate.*

	Sunt stabilite măsuri preventive pentru a reduce riscurile legate de protecția datelor cu caracter personal?	*Vă rugăm să furnizați/indicați documente care stabilesc măsuri pentru atenuarea riscurilor identificate.*
IV. Respectarea drepturilor subiecților datelor cu caracter personal	Are entitatea stabilite proceduri pentru gestionarea solicitărilor de rectificare, actualizare, blocare sau ștergere a datelor cu caracter personal a căror prelucrare contravine prevederilor legale?	*Faceți referire la reglementări/proceduri interne în care sunt definite cerințele/procedurile de examinare a solicitărilor parvenite din partea subiecților datelor cu caracter personal.*
	Cum sunt informați subiecții despre politica de confidențialitate și protecție a datelor cu caracter personal?	*Vă rugăm să indicați modalitățile în care subiecții sunt informați.*
	Entitatea oferă subiecților informații corespunzătoare cu privire la modul în care sunt prelucrate datele, la cererea acestora? Au existat solicitări din partea subiecților datelor cu caracter personal? Unde sunt înregistrate solicitările respective? Persoana responsabilă cu protecția datelor cu caracter personal a participat la evaluarea acestor solicitări și la îndeplinirea cerințelor?	
V. Managementul incidentelor de încălcări admise	Reglementările/Procedurile interne și persoanele responsabile pentru evaluarea și comunicarea încălcărilor privind protecția datelor cu caracter personal au fost stabilite?	*Vă rugăm să descrieți procedura sau să specificați unde este determinată (regulament, proceduri etc.).*
	În cadrul entității se ține un registru de evidență a încălcărilor admise privind protecția datelor cu caracter personal (care să includă fapte legate de încălcare, efectele și acțiunile corective întreprinse?	*Cine este responsabil pentru ținerea registrului de încălcări?* *Câte încălcări au fost înregistrate în Registru?*
	Entitatea raportează anual Centrului Național pentru Protecția Datelor cu Caracter Personal privind incidentele de încălcare a protecției datelor cu caracter personal admise?	*Referire la reguli/proceduri interne.*

Anexa nr. 2
la Ghidul de audit intern privind
protecția datelor cu caracter personal

APROBAT,
Șeful subdiviziunii de audit intern,

_____
(numele, prenumele)

_____
(semnătura)

„___” _____ 20__

2023

REZUMAT AL RAPORTULUI DE AUDIT INTERN

Nr. __

Titlul misiunii de audit:

Evaluarea procesului de prelucrare a datelor cu caracter personal în cadrul _____?”

(denumirea entității în cadrul căreia a fost realizat auditul)

Supervizor:

_____
(numele, prenumele, funcția)

Şeful echipei:

_____
(numele, prenumele, funcția)

Membrii echipei:

_____
(numele, prenumele, funcția)

_____
(numele, prenumele, funcția)

I. DATE GENERALE

(În acest capitol vor fi incluse informații generale privind misiunea de audit intern orizontal, prezentate pentru fiecare din cele 7 sub-capitole. Conținutul subcapitolelor urmează a fi ajustat în corespundere cu datele despre misiunea de audit realizată în entitatea Dvs., excepție fiind sub-capitolele 1.1. Obiectivul general al auditului și 1.5 Obiectivele specifice ale misiunii de audit, care urmează a fi expuse cel puțin în redacția propusă)

1.1 Obiectivul general al auditului

Evaluarea conformității protecției datelor cu caracter personal cu reglementările aplicabile în domeniu și oferirea asigurării că prelucrarea datelor cu caracter personal în entitate este efectuată legal, responsabil, corect și transparent în raport cu subiecții acestor date.

1.2 Perioada desfășurării auditului

Misiunea de audit s-a desfășurat în perioada _____ 2023, în baza ordinului Ministrului/Directorului _____nr.__ din _____ 2023.

1.3 Tipul auditului

Audit de conformitate, axat pe verificarea respectării cadrului normativ, a politicilor şi procedurilor aplicate în cadrul entității cu privire la prelucrarea și protecția datelor cu caracter personal şi, după caz, determinarea necesității de îmbunătăţire a activităților de control și procedurilor de delegare a responsabilităților.

1.4. Aria de aplicabilitate a misiunii de audit

În cadrul misiunii de audit a fost evaluat modul de organizare și derulare a operațiunilor prin care sunt colectate, prelucrate și stocate datele cu caracter personal în cadrul sistemelor operaționale, de management și de suport în _____ *(entitatea),* prin prisma conformității cu normele și procedurile aferente, precum și stabilirii activităților de control pentru asigurarea confidențialității și protecției datelor cu caracter personal și respectării drepturilor subiecților acestora.

Perioada supusă auditului, pentru care au fost examinate procesele și colectate probele de audit, este _____.

Aria de aplicabilitate a misiunii de audit realizată a fost stabilită în conformitate cu SNAI, fiind suficientă pentru realizarea obiectivului general al misiunii de audit.

1.5 Obiectivele specifice misiunii de audit

1. De a evalua cadrul intern de guvernare (reglementare și delegare de atribuții) cu referire la protecția datelor cu caracter personal, prin prisma calității și actualității acestuia;
2. De a evalua conformitatea operațiunilor de colectare, prelucrare și stocare a datelor cu caracter personal;
3. De a analiza dacă măsurile tehnice și organizatorice introduse pentru asigurarea confidențialității și protecția datelor cu caracter personal, la toate etapele de prelucrare a acestora, sunt suficiente și funcționale;
4. De a obține o asigurare rezonabilă cu privire la respectarea de către entitate a drepturilor subiecților datelor cu caracter personal;

5. De a evalua modul de gestionare a incidentelor de încălcări admise de către entitate cu privire la protecția datelor cu caracter personal.

1.6 Metode și tehnici de audit

(În acest subcapitol vor fi expuse principalele metode și tehnici utilizate de echipa de audit pentru analiză datelor și colectarea probelor)

1.7 Resurse utilizate

Pentru realizarea misiunii de audit au fost utilizate ____ om/zile.

(În acest subcapitol vor fi prezentate resursele (nr. de om/zile) efectiv utilizate pentru desfășurarea etapei de planificare a misiunii, lucrului în teren și raportare a rezultatelor)

II. CONTEXT ADMINISTRATIV

(Capitolul va include o descriere succintă a domeniului auditat, particularitățile organizării acestuia în cadrul entității Dvs., fiind luate în considerare aspecte importante care subliniază circumstanțele cu impact direct asupra obiectivului misiunii de audit – maxim 1 pag.)

III. REZUMATUL CONSTATĂRILOR ȘI RECOMANDĂRILOR

Nr.	Obiectivul specific	**Rezumat concis al constatărilor*** *(Fapte, observații, inclusiv abateri/ neajunsuri/ probleme. Dacă există - bună practică)*	**Cauzele** *abaterilor/neajunsurilor /problemelor constatate*	**Impactul (efect)** *abaterilor/neajunsurilor /problemelor constatate*	**Opinie generală asupra controlului intern managerial**** *(Deplin conform / General conform / Parțial Conform / Neconform)*	**Recomandări pentru entitate**
1.	**Evaluarea cadrului intern de guvernare (reglementare și delegare de atribuții) cu referire la protecția datelor cu caracter personal, prin prisma calității și actualității acestuia.**					
2.	**Evaluarea conformității operațiunilor de colectare, prelucrare și stocare a datelor cu caracter personal**					
3.	**Analiza faptului dacă măsurile tehnice și organizatorice introduse pentru asigurarea confidențialității și protecția datelor cu caracter personal, la toate etapele de prelucrare a acestora, sunt suficiente și funcționale**					
4.	**Obținerea asigurării rezonabile cu privire la respectarea de către**					

Nr.	Obiectivul specific	**Rezumat concis al constatărilor*** *(Fapte, observații, inclusiv abateri/ neajunsuri/ probleme. Dacă există - bună practică)*	**Cauzele** *abaterilor/neajunsurilor /problemelor constatate*	**Impactul (efect)** *abaterilor/neajunsurilor /problemelor constatate*	**Opinie generală asupra controlului intern managerial**** *(Deplin conform / General conform / Parțial Conform / Neconform)*	**Recomandări pentru entitate**
	entitate a drepturilor subiecților datelor cu caracter personal					
5.	**Evaluarea modului de gestionare a incidentelor de încălcări admise de către entitate cu privire la protecția datelor cu caracter personal**					

Note:

** Evaluarea funcționării sistemului de control intern managerial în cadrul procesului auditat trebui să se bazeze pe probe sigure, relevante și suficiente, obținute în cadrul testelor de către echipei de audit.*

*** Opinia privind conformitatea și eficacitatea funcționării controlului intern managerial va fi apreciată în baza următoarei matrice:*

Deplin Conform	Procesul auditat este organizat și funcționează în deplină conformitate cu cadrul normativ și procedurile interne aprobate. Activitățile de control în cadrul procesului sunt evaluate ca fiind necesare, suficiente, adecvate și eficiente, și oferă o asigurare rezonabilă că riscurile sunt atenuate / ținute sub control.
General Conform	Procesul auditat este organizat în conformitate cu cadrul normativ și procedurile interne aprobate, dar au fost identificate unele deficiențe și sunt necesare unele îmbunătățiri cu privire la funcționarea acestuia. Activitățile de control sunt stabilite, necesare, adecvate, cu toate acestea, funcționează neregulat. Au fost identificate și alte deficiențe individuale, dar care nu afectează semnificativ funcționarea procesului auditat. În general, activitățile de control evaluate oferă o asigurare rezonabilă că riscurile sunt atenuate / ținute sub control.
Parțial Conform	În timpul auditului intern au fost identificate unele abateri de la prevederile cadrului normativ și procedurile interne aprobate, și sunt necesare îmbunătățiri cu privire la organizarea și funcționarea procesului auditat. Activitățile de control sunt stabilite și funcționează neregulat.
Neconform	Procesul auditat este organizat și funcționează necorespunzător. Activitățile de control nu sunt suficiente, adecvate și/sau eficiente. Au fost identificate un număr semnificativ de abateri de la prevederile cadrului normativ și procedurile interne aprobate, care se repetă frecvent și/sau în mod regulat. Auditul intern nu a putut obține asigurarea că riscurile sunt atenuate/ ținute sub control.

IV. RECOMANDĂRI PENTRU DEZVOLTAREA ȘI ÎMBUNĂTĂȚIREA POLITICII / PROCEDURILOR DE PRELUCRARE ȘI PROTECȚIE A DATELOR CU CARACTER PERSONAL

Nu.	Recomandări/ sugestii/ propuneri
1.	
2.	
3.	
4.	
5.	
…	

V. CONCLUZIE / OPINIE GENERALĂ

(În acest Capitolul va fi inclusă opinia generală a auditului intern cu privire la aplicarea în cadrul entității a cadrului normativ cu privire la protecția datelor cu caracter personal.)