AUDIT ȘI CONFORMITATE

Protecția datelor personale | Sectorul public din România | Cazuistică ANSPDCP

Cadrul legislativ actualizat și ierarhia normelor

Conformitatea în sectorul public românesc este guvernată de un ansamblu normativ ierarhizat, care trebuie interpretat integrat pentru a evita conflictele juridice:

- Regulamentul (UE) 2016/679 (Regulamentul General privind Protecția Datelor/RGPD): norma de bază, direct aplicabilă, care stabilește principiile și drepturile fundamentale;
- Legea nr. 190/2018: actul normativ de punere în aplicare în România, care conține regimul derogatoriu și sancționator specific autorităților publice;
- OUG. nr. 57/2019 (Codul administrativ): reglementează atribuțiile instituțiilor și autorităților publice și obligativitatea respectării legalității în prelucrarea datelor în actele administrative;
- Legea nr. 102/2005 (republicată): privind înființarea și funcționarea ANSPDCP.

Paradigma protecției datelor în administrația publică modernă

Într-un peisaj digitalizat, instituția publică nu mai este doar un depozit de documente fizice, ci un nod central de procesare a fluxurilor masive de date personale ale cetățenilor. Protecția datelor cu caracter personal a încetat să fie o simplă bifă birocratică, devenind un pilon al statului de drept.

Prezentul raport detaliază modul în care legislația actualizată (inclusiv Legea nr. 363/2018 privind prelucrarea datelor personale de către autorități, Legea nr. 58/2023 privind securitatea și apărarea cibernetică și OUG nr.155/2024 de aplicare a Directivei NIS2, cu impact direct asupra integrității datelor prelucrate) impune o rigoare absolută în gestionarea informațiilor, fundamentând necesitatea unui pachet de conformitate robust și a consultanței de specialitate.

Respectarea principiilor generale

Instituțiile publice care prelucrează date cu caracter personal trebuie să asigure conformitatea cu principiile fundamentale ale RGPD, inclusiv:

• legalitate, echitate și transparență în prelucrare;

• limitarea scopului (datele să fie colectate doar în scopuri precise și legitime);

• minimizarea datelor (prelucrarea să fie adecvată, relevantă și limitată la ceea ce este necesar);

• acuratețe și actualizare a datelor;

• limitarea stocării (datele să nu fie păstrate mai mult decât este necesar pentru scopul declarat);

• integritate și confidențialitate (să fie protejate adecvat prin măsuri tehnice și organizatorice).

Aceste principii se regăsesc în articolele 5-6 RGPD și sunt obligatorii pentru orice prelucrare efectuată de autoritățile publice.

Obligațiile instituțiilor publice ca operatori de date

Instituțiile publice poartă responsabilitatea deplină pentru orice flux de date, de la colectare până la arhivare. Obligațiile sunt multidimensionale:

1. Desemnarea obligatorie a Responsabilului cu protecția datelor (DPO):

Orice autoritate sau organism public are obligația legală de a desemna un DPO, indiferent de volumul datelor prelucrate. Acesta trebuie să fie implicat în toate aspectele legate de protecția datelor.

2. Evidența activităților de prelucrare (ROPA):

Instituția trebuie să mențină un Registru al Operațiunilor de Prelucrare (art. 30 RGPD) care să includă:

- scopurile prelucrării;
- descrierea categoriilor de persoane vizate și a categoriilor de date;
- destinatarii cărora le-au fost sau le vor fi divulgate datele (inclusiv alte instituții);
- termenele-limită prevăzute pentru ștergerea diferitelor categorii de date (corelat cu nomenclatorul arhivistic).

Baza legală a prelucrărilor

Instituțiile publice trebuie să identifice temeiuri legale legitime pentru prelucrarea datelor, dintre care cele mai relevante sunt:

• prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau exercițiul autorității publice conferite operatorului;

• prelucrarea este necesară pentru îndeplinirea unei obligații legale;

• în alte situații, când este autorizată prin lege sau când sunt respectate garanțiile impuse de legislație.

Unele categorii de date – de exemplu date privind sănătatea, date biometrice sau codul numeric personal – sunt considerate date sensibile și, potrivit RGPD și normelor naționale, necesită condiții speciale de prelucrare și garanții sporite.

Notă critică privind temeiul legal:

Spre deosebire de sectorul privat, instituțiile publice nu pot invoca *„interesul legitim"* (art. 6 alin. 1 lit. f RGPD) pentru prelucrările efectuate în îndeplinirea sarcinilor lor.

Temeiurile corecte sunt:

- îndeplinirea unei sarcini care servește unui interes public (art. 6 alin. 1 lit. e);
- îndeplinirea unei obligații legale care îi revine operatorului (art. 6 alin. 1 lit. c).

3. Evaluarea impactului asupra protecției datelor (DPIA):

Este obligatorie atunci când un tip de prelucrare este susceptibil să genereze un risc ridicat pentru drepturile cetățenilor, în special în cazul:

- utilizării de noi tehnologii (ex. sisteme de recunoaștere facială în spații publice);
- monitorizării sistematice a zonelor accesibile publicului (supraveghere video pe scară largă);
- prelucrării pe scară largă a categoriilor speciale de date (dosare medicale în spitale publice).

4. Securitatea prelucrării:

Instituția trebuie să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător acestui risc, incluzând:

- capacitatea de a asigura confidențialitatea, integritatea și disponibilitatea sistemelor;
- proceduri pentru testarea și evaluarea periodică a eficienței măsurilor tehnice.

Rolul și independența DPO-ului în sectorul public

Responsabilul cu protecția datelor nu este doar un consultant intern, ci un garant al legalității. Statutul său în instituție trebuie să îndeplinească următoarele **condiții**:

- independență operațională: conducerea instituției nu poate da instrucțiuni DPO-ului cu privire la modul de îndeplinire a sarcinilor sale;
- raportare directă: DPO-ul trebuie să raporteze direct nivelului de conducere executivă (primar, președinte, director general);
- resurse adecvate: instituția are obligația de a asigura resursele financiare și timpul necesar pentru formarea continuă a DPO-ului.

Neconformitatea privind statutul DPO-ului (ex. desemnarea unei persoane în conflict de interese, cum ar fi șeful departamentului IT) constituie o încălcare gravă, sancționată de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal / ANSPDCP.

Responsabilul cu protecția datelor **trebuie să:**

- monitorizeze respectarea RGPD și a legislației naționale privind protecția datelor;
- colaboreze cu ANSPDCP drept punct de contact;

Registrele de evidență ale prelucrărilor

Fiecare instituție publică trebuie să întocmească și să actualizeze regulat registrele de activități de prelucrare, potrivit art. 30 RGPD. În aceste registre se vor menționa:

- scopurile prelucrării;
- categoriile de date
- prelucrate și categoriile de persoane vizate;
- destinatarii datelor;
- perioadele de păstrare;
- măsurile de securitate implementate.

Registrele sunt documente fundamentale pentru responsabilitatea demonstrabilă și pentru eventuale solicitări din partea ANSPDCP sau a persoanelor vizate.

Măsuri de securitate

Instituțiile publice trebuie să asigure confidențialitatea, integritatea și disponibilitatea datelor prelucrate prin: politici și proceduri, controlul accesului la date, criptare și audituri.

Evaluări de impact

Instituțiile publice trebuie să efectueze evaluări de impact asupra protecției datelor (DPIA) atunci când utilizează tehnologii noi sau se realizează o monitorizare sistematică pe scară largă, cu risc ridicat.

- ofere consultanță privind evaluările de impact DPIA;
- informeze și consiliază angajații instituției despre obligațiile privind protecția datelor;
- supravegheze instruirea personalului și implementarea politicilor interne.

Instituțiile publice trebuie să publice datele de contact ale DPO și să le transmită autorității de supraveghere.

Drepturile persoanelor vizate și gestionarea acestora

Cetățenii au drepturi consolidate și garantate de RGPD în raport cu autoritățile, iar instituția trebuie să dețină proceduri clare pentru soluționarea acestora în termen de cel mult o lună:

- dreptul de acces: cetățeanul poate solicita o copie a tuturor datelor pe care instituția le deține despre el;
- dreptul la rectificare: corectarea datelor inexacte din evidențele fiscale sau de stare civilă;
- dreptul la ștergerea datelor: aplicabil doar dacă datele nu mai sunt necesare pentru scopul public sau dacă perioada de arhivare legală a expirat;
- dreptul de a se opune prelucrării datelor într-un anumit context;
- drepturile privind deciziile automate și profilarea;
- dreptul de a depune o plângere la ANSPDCP sau în fața instanțelor judecătorești;
- dreptul la restricționarea prelucrării: în cazul în care persoana contestă exactitatea datelor.

Particularitate: în sectorul public, dreptul la portabilitatea datelor nu se aplică, de regulă, prelucrărilor efectuate în temeiul unei obligații legale sau sarcini publice.

Analiza cazuisticii ANSPDCP: încălcări reale și sancțiuni

Rapoartele anuale ale ANSPDCP (2022, 2023 și 2024, cel mai recent publicat) evidențiază o serie de vulnerabilități cronice în instituțiile publice. Analiza acestor cazuri reale fundamentează necesitatea unei revizuiri a politicilor interne:

Încălcări recurente în sectorul public

Analiza rapoartelor relevă următoarele tipuri principale de abateri:

- **divulgarea neautorizată și accesul ilegal la date**: publicarea pe site-urile instituțiilor a unor fișiere parolate necorespunzător (cu parola aflată chiar în interiorul arhivei) conținând CNP-uri și date medicale (în cazul cazul Caselor de Asigurări de Sănătate sau spitalelor). Au fost identificate scurgeri de date în sistemele de gestionare a petițiilor online și în comunicările prin e-mail, unde adresele petenților au fost lăsate vizibile (la secțiunea "To" în loc de "BCC").
- **monitorizarea nelegală a angajaților**: o practică frecvent sancționată a fost utilizarea sistemelor de supraveghere video pentru monitorizarea prezenței și realizarea pontajului, scop considerat incompatibil cu cel declarat (paza bunurilor și persoanelor).
- **utilizarea noilor tehnologii fără evaluarea impactului:** Implementarea sistemelor de tip "body-worn camera" (de către poliția locală) sau a sistemelor de recunoaștere facială, în unități de învățământ,

1. publicarea nelegală a datelor personale pe site-urile instituțiilor:

- în numeroase cazuri, primăriile au publicat liste cu debitori (persoane fizice) care conțineau CNP-ul și adresa completă a acestora;
- ANSPDCP a reținut că, deși există o obligație de transparență, aceasta nu trebuie să încalce principiul reducerii la minimum a datelor. Publicarea numelui și a sumei datorate este suficientă, CNP-ul fiind considerat excesiv.

2. utilizarea sistemelor de supraveghere video (CCTV):

- instalarea camerelor video în birourile angajaților sau în sălile de clasă fără o justificare legală solidă și fără o informare prealabilă corectă;
- încălcarea art. 5 din RGPD (principiile prelucrării) prin monitorizarea audio-video constantă a funcționarilor, considerată o intruziune nejustificată în viața privată.

3. securitatea datelor medicale în spitale:

- accesarea neautorizată a dosarelor pacienților de către personal care nu era implicat în actul medical respectiv;
- lipsa jurnalizării (log-urilor) care să permită identificarea persoanei care a accesat datele sensibile.

4. regimul sancționator (Legea 190/2018):

Pentru instituțiile publice, procesul sancționator este secvențial:

- pasul 1: aplicarea avertismentului (sancțiune principală);
- pasul 2: aplicarea unui plan de remediere cu termene stricte (maximum 90 zile);
- pasul 3: dacă planul de remediere nu este îndeplinit sau instituția se abate de la măsurile prevăzute în plan, se aplică amenda contravențională (de la 10.000 lei până la 200.000 lei) pentru nerespectarea obligațiilor de protecție a datelor de către autoritățile publice.

Acest regim sancționator este distinct de cel pentru entități private, ceea ce reflectă flexibilitatea conferită statelor membre pentru instituțiile publice.

Particularități pe categorii de instituții

Fiecare segment al administrației prezintă riscuri specifice care necesită abordări personalizate în cadrul pachetului de conformitate:

- (pentru controlul accesului elevilor), fără o bază legală expresă și fără efectuarea unei evaluări a impactului asupra protecției datelor (DPIA);
- **deficiențe privind DPO:** omisiunea desemnării unui responsabil cu protecția datelor sau generarea unor conflicte de interese prin cumularea funcției de DPO cu funcții de conducere (ex: director executiv) care stabilesc scopurile prelucrării; cazuri de refuz al acordării sprijinului necesar DPO-ului în monitorizarea conformității;
- **nerespectarea principiului reducerii la minimum a datelor:** colectarea sau publicarea excesivă de date (ex: publicarea nominală a rezultatelor la concursuri sau examene când scopul putea fi atins prin anonimizare sau codificare).

Sancțiuni și măsuri corective

Regimul sancționator aplicat autorităților și organismelor publice include:

- **avertismentul însoțit de planul de remediere:** reprezintă sancțiunea principală conform Legii nr. 190/2018. Operatorul are un termen strict (de regulă între 10 și 20 de zile lucrătoare) pentru a implementa măsurile dispuse de Autoritate.
- **amenzi contravenționale pentru neîndeplinirea planului:** dacă instituția nu aplică măsurile de remediere,

1. Primării și Consilii Județene:

- gestionarea documentelor de urbanism și cadastru care conțin date de identificare și proprietate;
- prelucrarea datelor în contextul asistenței sociale (date sensibile privind starea de sănătate sau situația materială);
- arhivarea fizică masivă: riscul de acces neautorizat în depozitele de arhivă.

2. instituții de învățământ (școli, universități):

- protecția datelor minorilor: necesitatea acordurilor pentru utilizarea imaginii în scopuri de promovare;
- utilizarea platformelor de tip catalog electronic: securitatea transmiterii notelor și absențelor.

3. unități sanitare (spitale publice):

- regimul strict al datelor privind sănătatea (art. 9 RGPD);
- obligația de a asigura confidențialitatea datelor în relația cu aparținătorii.

Corelarea cu securitatea cibernetică și digitalizarea

Protecția datelor este indisolubil legată de reziliența sistemelor IT. Instituțiile publice trebuie să:

- implementeze standarde de securitate conform Legii 58/2023 (securitatea cibernetică);
- utilizeze semnătura electronică calificată pentru a asigura integritatea și non-repudierea documentelor;
- efectueze audituri tehnice de tip „penetration testing” pentru portalurile cetățenești;
- automatizeze fluxurile documentelor pentru a reduce manipularea manuală și riscul de pierdere/alterare a datelor.

Protecția datelor și securitatea cibernetică sunt discipline complementare:

- măsurile de securitate cibernetică – controlul accesului, criptare, monitorizare a rețelelor – contribuie direct la îndeplinirea obligațiilor de securitate prevăzute de RGPD (art. 32);
- instituțiile trebuie să implementeze politici de securitate a informațiilor care să includă gestionarea incidentelor de securitate (inclusiv breșe de date) și notificarea persoanelor vizate atunci când există un risc ridicat pentru drepturile și libertățile acestora;

- ANSPDCP aplică amenzi contravenționale (ex: 10.000 - 13.000 lei);
- **amenzi cominatorii:** în caz de refuz explicit sau tacit de a furniza informații în timpul investigațiilor, se pot aplica amenzi de până la 3.000 lei pentru fiecare zi de întârziere. Într-un caz din 2024, o primărie a cumulat astfel o sancțiune de 159.000 lei;
- **măsuri corective specifice:** încheierea operațiunilor de prelucrare nelegală, ștergerea sistemelor de evidență constituite prin body-cam, revizuirea procedurilor interne de lucru și de securitate IT și instruirea periodică a personalului.

Practica ANSPDCP privind instituțiile publice

Din cazuistica ultimilor ani, se desprind următoarele orientări practice ale Autorității

- **subsidiaritatea comunicării prin publicitate:** publicarea datelor debitorilor sau petenților este considerată o modalitate ultimă și subsidiară. Instituțiile trebuie să demonstreze că au epuizat celelalte căi de comunicare (poștă, personal) înainte de a publica datele debitorilor/ petenților pe site-uri;
- **securitatea datelor** (art. 32 RGPD): ANSPDCP sancționează sever utilizarea dispozitivelor personale (telefoane mobile) pentru fotografierea actelor de identitate ale cetățenilor de către agenții publici sau utilizarea aplicației WhatsApp
- conform standardelor naționale și europene (ex. NIS2), instituțiile publice trebuie să asigure un nivel înalt de securitate cibernetică, care este un element esențial în protejarea datelor personale.

Un program comprehensiv de conformitate trebuie să includă atât politici de protecție a datelor, cât și proceduri de securitate cibernetică integrate.

Pachetul de conformitate RGPD: componente esențiale

O instituție publică conformă trebuie să dețină un set de documente cadru, proceduri și anexe operaționale. Acesta este nucleul serviciilor oferite de firma noastră de consultanță:

1. politici și norme interne:

- politica generală de protecție a datelor (Manualul RGPD al instituției);
- politica de securitate a informațiilor, a sistemelor informatice și de comunicații (corelată cu cerințele RGPD și standardele de securitate cibernetică);
- politica de utilizare a dispozitivelor mobile și a muncii la distanță (telemuncă);

- pentru transmiterea datelor profesionale, din cauza lipsei măsurilor tehnice adecvate de control;
- **transparența:** simpla trimitere la „politica de confidențialitate" pe un site nu este suficientă; informarea trebuie să fie punctuală, adaptată contextului specific al persoanei vizate.

Obligațiile instituțiilor publice ca operatori

În sinteză, obligațiile extrase din practica ANSPDCP sunt:

1. asigurarea independenței DPO: acesta trebuie să raporteze direct managementului superior și să nu fie în conflict de interese;
2. implementarea principiului "privacy by design": configurarea sistemelor informatice (ex: platforme de petiții sau portaluri de facturare) astfel încât să prevină scurgerile de date din faza de proiectare;
3. gestionarea incidentelor de securitate: notificarea ANSPDCP în termen de cel mult 72 de ore de la luarea la cunoștință a oricărei breșe de securitate;
4. minimizarea accesului: angajații trebuie să aibă acces doar la datele necesare îndeplinirii atribuțiilor specifice (necesitatea de a cunoaște);
5. respectarea termenelor de stocare: datele (inclusiv înregistrările video) nu pot fi păstrate pe perioadă nedeterminată, ci doar atât timp cât este necesar scopului.

- politica privind gestionarea accesului la date.

2. registre și documente de evidență:

- registrul activităților de prelucrare (ROPA) - detaliat pe fiecare compartiment;
- registrul incidentelor de securitate (breșe de date);
- registrul cererilor persoanelor vizate.

3. proceduri operaționale:

- procedura privind gestionarea breșelor de securitate și notificarea ANSPDCP;
- procedura pentru exercitarea drepturilor persoanelor vizate;
- procedura de reținere și distrugere a datelor;
- procedura privind supravegherea video (CCTV).

4. documente de informare și consimțământ (unde e cazul):

- note de informare specifice (pentru angajați, cetățeni, vizitatori, site);
- formulare de consimțământ pentru situații deosebite (ex. activități culturale/promovare);
- acorduri de prelucrare a datelor cu furnizorii externi.

5. instrumente de evaluare:

- metodologie și șabloane pentru Evaluarea Impactului (DPIA);
- chestionare de audit intern pentru verificarea conformității departamentelor.

Concluzii și recomandări pentru management

Lipsa unei strategii de protecție a datelor atrage nu doar sancțiuni de la ANSPDCP, ci și riscuri juridice majore (litigii cu cetățenii) și deteriorarea imaginii instituției. Recomandăm implementarea următoarelor măsuri urgente:

- realizarea unui audit de conformitate pentru a identifica punctele slabe;
- actualizarea nomenclatorului arhivistic în concordanță cu perioadele de retenție RGPD;
- instruirea specializată a personalului din departamentele cheie (Resurse Umane, IT, Urbanism, Asistență Socială).

Firma noastră de consultanță oferă expertiza necesară pentru a transforma obligațiile RGPD într-un sistem de management eficient, asigurând liniștea juridică a instituției și protecția reală a cetățeanului.