

NOTĂ DE INFORMARE PRIVIND PRELUCRAREA ȘI FURNIZAREA DATELOR CU CARACTER PERSONAL DE CĂTRE SERVICIUL JUDEȚEAN DE EVIDENȚĂ A PERSOANELOR BRĂILA

Informare generală privind aplicarea Regulamentului (UE) 2016/679 (GDPR) în activitatea S.J.E.P. Brăila și furnizarea/verificarea datelor din Registrul Național de Evidență a Persoanelor (R.N.E.P.)

1. Ce sunt datele cu caracter personal?

În sensul art. 4 pct. 1 din Regulamentul (UE) 2016/679, datele cu caracter personal reprezintă orice informații privind o persoană fizică identificată sau identificabilă. O persoană poate fi identificată direct sau indirect, inclusiv prin nume, număr de identificare, date de localizare, identificator online ori prin elemente specifice identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

În activitatea de evidență a persoanelor și stare civilă, informațiile sunt prelucrate în sisteme informatice și/sau pe suport hârtie, potrivit competențelor stabilite de lege. Noțiunea de «prelucrare» include, între altele, colectarea, înregistrarea, organizarea, structurarea, stocarea, consultarea, utilizarea, modificarea, transmiterea, restricționarea și ștergerea datelor.

2. Ce categorii de date poate prelucra S.J.E.P. Brăila?

În funcție de atribuția legală concretă, S.J.E.P. Brăila poate prelucra date de identificare și de evidență a persoanelor, date din actele de identitate și de stare civilă, date de contact și alte informații necesare soluționării cererilor ori îndeplinirii atribuțiilor instituției.

- numele și prenumele, numele anterior, după caz, și prenumele părinților;
- codul numeric personal (CNP), data și locul nașterii, sexul;
- domiciliul, reședința și date referitoare la istoricul acestora, în condițiile legii;
- seria, numărul și celelalte elemente ale actelor de identitate;
- date și mențiuni din actele de stare civilă privind nașterea, căsătoria și decesul;
- imaginea facială și alte date tehnice/documentare asociate actelor de identitate, în măsura în care instituția are competență legală de prelucrare;
- date de contact furnizate de persoana vizată, precum adresă de corespondență, e-mail sau telefon, atunci când sunt necesare soluționării unei solicitări;
- date cuprinse în petiții, cereri, documente justificative, corespondență administrativă și dosare aferente activităților instituției;
- date privind personalul, colaboratorii, furnizorii ori reprezentanții acestora, în cadrul activităților administrative, contractuale și de resurse umane.

3. Categoriile speciale de date și date privind condamnările penale

Art. 9 GDPR acordă protecție sporită datelor care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase ori filosofice, apartenența sindicală, precum și datelor genetice, biometrice prelucrate în scopul identificării unice, datelor privind sănătatea sau viața sexuală/orientarea sexuală. Prelucrarea acestora este, ca regulă, interzisă, cu excepția situațiilor expres prevăzute de art. 9 alin. (2) și de dreptul aplicabil.

Datele referitoare la condamnări penale și infracțiuni sunt supuse regimului art. 10 GDPR. S.J.E.P. Brăila nu trebuie să colecteze asemenea date decât atunci când o dispoziție legală și atribuția concretă justifică prelucrarea.

4. Principiile pe care S.J.E.P. Brăila trebuie să le respecte

Art. 5 GDPR stabilește principiile fundamentale ale prelucrării. Acestea se aplică tuturor operațiunilor cu date personale efectuate de instituție.

- Legalitate, echitate și transparență – orice prelucrare trebuie să aibă un temei juridic și să fie realizată într-o manieră corectă și transparentă;
- Limitarea scopului – datele se colectează pentru scopuri determinate, explicite și legitime și nu se utilizează ulterior incompatibil cu acestea;
- Reducerea la minimum a datelor – se solicită și se utilizează numai datele adecvate, relevante și necesare;
- Exactitate – datele trebuie să fie corecte și, când este necesar, actualizate;
- Limitarea stocării – datele se păstrează numai pe perioada justificată de scop și de obligațiile legale/arhivistice;
- Integritate și confidențialitate – datele trebuie protejate împotriva accesului neautorizat, pierderii, distrugerii ori divulgării nepermise;
- Responsabilitate – operatorul trebuie să respecte principiile și să poată demonstra respectarea lor.

5. Care este temeiul juridic al prelucrării?

Pentru activitatea specifică unei autorități publice precum S.J.E.P. Brăila, temeiurile principale sunt art. 6 alin. (1) lit. c) GDPR – prelucrarea necesară îndeplinirii unei obligații legale – și art. 6 alin. (1) lit. e) – prelucrarea necesară îndeplinirii unei sarcini de interes public sau care rezultă din exercitarea autorității publice.

Interesul legitim prevăzut la art. 6 alin. (1) lit. f) nu se aplică prelucrărilor efectuate de autoritățile publice în îndeplinirea atribuțiilor lor. Consimțământul nu trebuie prezentat ca temei general pentru activitățile legale obligatorii ale S.J.E.P.; el poate constitui temei numai în situațiile în care sunt îndeplinite efectiv condițiile GDPR.

6. Scopurile pentru care sunt prelucrate datele

În limitele atribuțiilor instituției, prelucrarea poate avea ca scop evidența persoanelor și activitățile conexe actelor de identitate; activitatea de stare civilă; verificarea și furnizarea datelor din R.N.E.P.; soluționarea cererilor și petițiilor; relațiile cu publicul; îndeplinirea obligațiilor juridice, financiar-contabile, de achiziții și resurse umane; exercitarea atribuțiilor de îndrumare, coordonare și control prevăzute de lege; apărarea drepturilor și intereselor instituției în proceduri administrative ori judiciare.

7. Furnizarea și verificarea datelor din R.N.E.P.

Potrivit art. 11 din O.U.G. nr. 97/2005, furnizarea sau verificarea unor date cu caracter personal din R.N.E.P. se face la cererea persoanelor fizice ori juridice, în condițiile stabilite de lege. Serviciile publice comunitare de evidență a persoanelor pot realiza asemenea operațiuni la solicitările scrise prevăzute de lege.

Solicitantul trebuie să indice scopul și temeiul juridic al solicitării și să furnizeze suficiente elemente pentru identificarea persoanei vizate. Nu se comunică automat toate informațiile existente în evidențe; se aplică principiul reducerii la minimum a datelor.

Consimțământul persoanei vizate nu este o condiție universală pentru furnizarea datelor. Atunci când există o obligație legală, o competență de autoritate publică sau un alt temei juridic prevăzut de lege, comunicarea se analizează în raport cu acel temei. În celelalte situații trebuie demonstrată existența unui temei valabil înaintea divulgării.

O.U.G. nr. 97/2005 reglementează și situațiile în care furnizarea/verificarea este supusă unei taxe, precum și categoriile exceptate de la plată. Cuantumul concret se verifică potrivit reglementărilor și tarifelor în vigoare la data solicitării.

8. Cui pot fi comunicate datele?

Datele pot fi comunicate autorităților și instituțiilor publice ori altor destinatari numai dacă există competență și temei juridic. Pot exista comunicări către instituții cu atribuții în domeniul ordinii publice, securității naționale, justiției, fiscalității, sănătății, protecției sociale sau către alte entități, în condițiile expres prevăzute de lege.

În cazul comunicării datelor, instituția trebuie să urmărească scopul, categoriile de date solicitate, identitatea și calitatea solicitantului și existența temeiului juridic, păstrând, după caz, evidențe care permit demonstrarea legalității operațiunii.

9. Informarea persoanei vizate

Art. 12-14 GDPR impun operatorului obligații de transparență. Informarea trebuie formulată într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu.

În funcție de situație, informarea trebuie să cuprindă identitatea și datele de contact ale operatorului, datele responsabilului cu protecția datelor, scopurile și temeiurile

prelucrării, destinatarii, perioada de stocare sau criteriile de stabilire a acesteia, drepturile persoanei vizate, dreptul de a depune plângere la autoritatea de supraveghere și, unde este cazul, informații privind transferurile sau procesele decizionale automatizate.

10. Drepturile cetățeanului / persoanei vizate

Capitolul III din GDPR recunoaște persoanei vizate mai multe drepturi. Aplicabilitatea lor trebuie analizată în raport cu temeiul și scopul prelucrării; unele drepturi nu sunt absolute.

- Dreptul la informare (art. 13-14) – dreptul de a cunoaște modul în care sunt prelucrate datele;
- Dreptul de acces (art. 15) – dreptul de a obține confirmarea prelucrării și acces la date și la informațiile prevăzute de regulament;
- Dreptul la rectificare (art. 16) – corectarea datelor inexacte și completarea celor incomplete, cu respectarea procedurilor legale aplicabile evidenței persoanelor și stării civile;
- Dreptul la ștergere (art. 17) – aplicabil numai în cazurile prevăzute de GDPR; nu permite ștergerea datelor pe care instituția este obligată prin lege să le păstreze sau să le prelucreze;
- Dreptul la restricționarea prelucrării (art. 18) – în situațiile expres prevăzute de regulament;
- Dreptul la portabilitate (art. 20) – se aplică numai dacă sunt îndeplinite condițiile articolului; nu se aplică prelucrării necesare unei sarcini de interes public sau exercitării autorității publice;
- Dreptul la opoziție (art. 21) – poate fi exercitat, în special, pentru prelucrări întemeiate pe art. 6 alin. (1) lit. e), în condițiile și limitele GDPR;
- Dreptul privind deciziile individuale automatizate (art. 22) – protecție împotriva anumitor decizii bazate exclusiv pe prelucrare automată, inclusiv profilare;
- Dreptul de a depune plângere (art. 77) la ANSPDCP și drepturile la căi de atac judiciare prevăzute de GDPR.

11. Cum se exercită drepturile?

Persoana vizată poate adresa operatorului o cerere privind exercitarea drepturilor. Conform art. 12 GDPR, operatorul furnizează informații privind acțiunile întreprinse fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea cererii. Termenul poate fi prelungit cu încă două luni atunci când este necesar, ținând seama de complexitatea și numărul cererilor; persoana trebuie informată despre prelungire și motive în termenul inițial.

Înainte de a comunica date, operatorul poate solicita informații suplimentare necesare confirmării identității solicitantului atunci când există îndoieli rezonabile.

Exercitarea drepturilor este, ca regulă, gratuită, fără a exclude situațiile prevăzute de art. 12 alin. (5) pentru cereri vădit nefondate sau excesive.

12. Securitatea datelor

Art. 32 GDPR impune operatorului și persoanelor împuternicite să adopte măsuri tehnice și organizatorice adecvate riscului. Într-o instituție care prelucrează date de identitate, acestea pot include controlul accesului pe baza atribuțiilor, autentificare, gestionarea drepturilor utilizatorilor, jurnalizarea operațiunilor, copii de siguranță, actualizarea sistemelor, protecție împotriva programelor malițioase, instruirea personalului și reguli privind documentele pe suport hârtie.

Personalul care are acces la date trebuie să le prelucreze numai potrivit atribuțiilor și instrucțiunilor legale și să respecte confidențialitatea.

13. Încălcarea securității datelor

O încălcare a securității datelor poate consta în distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la date. Potrivit art. 33 GDPR, atunci când sunt îndeplinite condițiile legale, operatorul notifică autoritatea de supraveghere fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore de la momentul la care a luat cunoștință de încălcare. Art. 34 reglementează situațiile în care trebuie informată și persoana vizată.

14. Responsabilul cu protecția datelor (DPO)

Autoritățile și organismele publice desemnează un responsabil cu protecția datelor, în condițiile art. 37 GDPR. Acesta informează și consiliază operatorul și personalul, monitorizează respectarea GDPR, oferă consiliere privind evaluările de impact și cooperează cu autoritatea de supraveghere. Datele de contact ale responsabilului trebuie făcute publice și comunicate autorității de supraveghere.

15. Protecția datelor începând cu momentul conceperii și în mod implicit

Art. 25 GDPR impune integrarea protecției datelor în proiectarea proceselor și sistemelor. În mod implicit trebuie prelucrate numai datele necesare fiecărui scop, inclusiv în ceea ce privește volumul, întinderea prelucrării, perioada de stocare și accesibilitatea.

16. Evidența activităților, evaluarea impactului și responsabilitatea

Operatorul trebuie să poată demonstra conformitatea. În condițiile art. 30 GDPR se ține evidența activităților de prelucrare. Atunci când un tip de prelucrare este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor, art. 35 prevede efectuarea unei evaluări de impact asupra protecției datelor (DPIA). Măsurile trebuie revizuite și actualizate atunci când este necesar.

17. Păstrarea și arhivarea datelor

GDPR nu stabilește un termen unic de păstrare pentru toate datele. Perioada rezultă din scopul prelucrării și din legislația specială, inclusiv obligațiile de evidență și arhivare. Datele nu trebuie păstrate într-o formă care permite identificarea persoanei mai mult decât este necesar, cu excepțiile prevăzute de regulament pentru arhivarea în interes public și celelalte situații legale.

18. Temeiul normativ relevant pentru S.J.E.P. Brăila

Prezenta informare are în vedere, în principal, Regulamentul (UE) 2016/679; Legea nr. 190/2018; O.U.G. nr. 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, republicată, cu modificările și completările ulterioare; H.G. nr. 295/2021; O.G. nr. 84/2001; Legea nr. 119/1996 cu privire la actele de stare civilă, republicată, cu modificările și completările ulterioare; H.G. nr. 255/2024 și celelalte acte normative aplicabile atribuțiilor instituției.