

GHID PRIVIND APLICAREA LEGII NR. 363/2018

Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date **implementează**, în România, **Directiva (UE) nr. 680/2016** 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 al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

1. Care este domeniul de aplicare a Legii nr. 363/2018?

Legea nr. 363/2018 se aplică prelucrărilor de date cu caracter personal efectuate de către autoritățile competente în scopul realizării activităților de prevenire, descoperire, cercetare, urmărire penală și combatere a infracțiunilor, de executare a pedepselor, măsurilor educative și de siguranță, precum și de menținere și asigurare a ordinii și siguranței publice de către autoritățile competente, în limitele competențelor stabilite prin lege.

Prelucrarea datelor cu caracter personal pentru realizarea activităților de menținere și asigurare a ordinii și siguranței publice se realizează numai dacă acestea sunt prevăzute de lege și sunt necesare pentru prevenirea unui pericol cel puțin asupra vieții, integrității corporale sau sănătății unei persoane ori a proprietății acesteia, precum și pentru combaterea infracțiunilor.

Legea nr. 363/2018 se aplică prelucrării datelor cu caracter personal realizate integral sau parțial prin mijloace automatizate, precum și prelucrării, prin alte mijloace decât cele automatizate, a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să fie incluse într-un asemenea sistem.

(art. 1 alin. (1) și alin. (2) și art. 3 alin. (1) și alin. (2) din Legea nr. 363/2018)

2. Când nu se aplică Legea nr. 363/2018?

Legea nr. 363/2018 nu se aplică prelucrărilor de date cu caracter personal efectuate pentru realizarea activităților din domeniul apărării naționale și securității naționale, în limitele și cu restricțiile stabilite prin legislația în materie.

(art. 3 alin. (3) din Legea nr. 363/2018)

3. Ce înseamnă autoritate competentă?

Autoritate competentă înseamnă orice autoritate publică sau orice alt organism sau entitate învestită cu exercițiul autorității de stat, competentă în materie de prevenire, descoperire, cercetare, urmărire penală și combatere a infracțiunilor sau de executare a pedepselor, inclusiv în materia menținerii și asigurării ordinii și siguranței publice (de ex. organe de poliție, parchet).

(art. 4 lit. g) din Legea nr. 363/2018)

4. Ce înseamnă operator de date cu caracter personal și persoană împuternicită de operator?

Operator înseamnă autoritatea competentă care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele de prelucrare sunt stabilite printr-un act normativ, operatorul sau criteriile specifice pentru determinarea acestuia se stabilesc prin actul normativ de referință (a se vede pct. 3).

Persoana împuternicită de operator înseamnă persoana fizică sau juridică, instituția/autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

(art. 4 lit. h) și lit. i) din Legea nr. 363/2018)

5. Care este Autoritatea națională de supraveghere?

Supravegherea și controlul prelucrărilor de date cu caracter personal efectuate în temeiul Legii nr. 363/2018, în scopul protejării drepturilor și libertăților fundamentale ale persoanelor fizice, în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în cadrul Uniunii Europene, se realizează de către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, desemnată potrivit

Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

(art. 4 lit. o) și art. 51 alin. (1) din Legea nr. 363/2018)

6. Operatorii sau persoanele împuternicite de operatori trebuie să țină o evidență a prelucrărilor de date?

Operatorul este obligat să țină evidența tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Evidența categoriilor de activități de prelucrare cuprinde următoarele informații:

- a) denumirea și datele de contact ale operatorului și, după caz, ale operatorului asociat și ale responsabilului cu protecția datelor;
- b) scopul sau scopurile prelucrării;
- c) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- d) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal care sunt prelucrate;
- e) dacă este cazul, mențiuni cu privire la desfășurarea activității de creare de profiluri;
- f) dacă este cazul, categoriile de transferuri de date cu caracter personal către un stat terț sau o organizație internațională;
- g) indicarea temeiului juridic al operațiunii de prelucrare, inclusiv al transferurilor de date cu caracter personal efectuate;
- h) dacă este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date cu caracter personal;
- i) dacă este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 35 din Legea nr. 363/2018.

(art. 27 din Legea nr. 363/2018)

De asemenea, persoana împuternicită de către operator este obligată să țină evidența tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Această evidență cuprinde următoarele informații:

a) numele și datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acționează această persoană și, după caz, cele ale responsabilului cu protecția datelor cu caracter personal;

b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

c) după caz, transferurile de date cu caracter personal către un stat terț sau către o organizație internațională, inclusiv indicarea statului terț sau a organizației internaționale respective, atunci când au primit instrucțiuni explicite în acest sens de la operator;

d) dacă este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 35 din Lgea nr. 363/2018.

(art. 28 din Legea nr. 363/2018)

7. Operatorul este obligat să desemneze un responsabil cu protecția datelor?

Da, operatorul este obligat să desemneze un responsabil cu protecția datelor cu caracter personal.

Instanțele sunt exceptate de la obligația desemnării unui responsabil cu protecția datelor cu caracter personal atunci când acționează în exercițiul funcției lor judiciare.

(art. 40 alin. (1) și alin. (2) din Legea nr. 363/2018)

8. Cine poate fi desemnat responsabil cu protecția datelor?

Poate fi desemnată responsabil cu protecția datelor persoana care îndeplinește următoarele condiții:

a) deține calități profesionale corespunzătoare;

b) deține cunoștințe de specialitate în domeniul legislației și practicilor privind protecția datelor cu caracter personal;

c) are capacitatea de a îndeplini următoarele sarcini, prevăzute la art. 42 din Legea nr. 363/2018, respectiv:

- informează și consiliază operatorul și angajații acestuia care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul Legii nr. 363/2018 și al altor dispoziții legale privind protecția datelor cu caracter personal;

- monitorizează respectarea dispozițiilor Legii nr. 363/2018, a altor dispoziții legale privind protecția datelor cu caracter personal;

- consiliază, la cerere, cu privire la evaluarea impactului asupra protecției datelor cu caracter personal și monitorizarea funcționării acesteia;
- cooperează cu autoritatea de supraveghere;
- este desemnat persoană de contact în relația cu autoritatea de supraveghere privind aspectele legate de prelucrare.

(art. 40 și art. 42 din Legea nr. 363/2018)

9. Cum se anunță responsabilul cu protecția datelor Autorității naționale de supraveghere?

Operatorul are obligația să publice datele de contact ale responsabilului cu protecția datelor și să le comunice Autorității naționale de supraveghere (ANSPDCP).

Comunicarea responsabilului cu protecția datelor către Autoritatea națională de supraveghere se realizează prin completarea on-line a formularului de declarare a responsabilului cu protecția datelor existent pe site-ul Autorității naționale de supraveghere www.dataprotection.ro, la Secțiunea „Responsabilul cu protecția datelor”, urmată de accesarea butonului „Trimite chestionarul”.

(art. 40 alin. (5) din Legea nr. 363/2018)

10. Cum se modifică datele responsabilului cu protecția datelor din formularul on-line transmis Autorității naționale de supraveghere?

În situația în care intervin modificări/completări în ceea ce privește informațiile cuprinse în formularul de declarare a responsabilului cu protecția datelor, este necesar să se completeze și să se transmită Autorității naționale de supraveghere un nou formular în același mod descris la punctul 9.

11. Care sunt drepturile persoanei vizate și cum se pot exercita aceste drepturi?

Potrivit Legii nr. 363/2018, persoana vizată beneficiază de anumite drepturi:

- **dreptul la informare** (art. 13 și art. 14);
- **dreptul de acces** (art. 16);
- **dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată** (art. 11);

- **dreptul la rectificare** (art. 18);
- **dreptul la ștergere** (art. 18);
- **dreptul la restricționare** (art. 18);
- **dreptul de a depune plângere la Autoritatea națională de supraveghere** (art. 57).

Pentru exercitarea drepturilor lor este necesar ca persoanele vizate să adreseze o cerere operatorului în acest sens. (art. 12)

12. În ce termen trebuie să răspundă operatorul la o cerere de exercitare a drepturilor persoanei vizate?

Operatorul are obligația de a informa persoana vizată, în scris, cu privire la modul de soluționare a cererilor formulate în temeiul prezentei legi în cel mult 60 de zile calendaristice.

În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

- a) să perceapă o taxă rezonabilă care să țină cont de costurile administrative pentru transmiterea sau comunicarea informațiilor sau pentru luarea măsurilor solicitate; sau
- b) să refuze să dea curs cererii.

Cuquantumul taxei va fi stabilit, respectiv actualizat prin act administrativ emis la nivelul operatorului.

(art. 12 din Legea nr. 363/2018)

13. Ce informații trebuie să furnizeze operatorul persoanei vizate?

Operatorul este obligat să pună la dispoziția persoanelor interesate următoarele categorii de informații:

- a) identitatea și datele de contact ale operatorului;
- b) datele de contact ale responsabilului cu protecția datelor, după caz;
- c) scopurile în care sunt prelucrate datele cu caracter personal;
- d) dreptul de a depune o plângere la Autoritatea națională de supraveghere și datele de contact ale acesteia;
- e) dreptul de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ștergerea acestor date sau restricționarea prelucrării lor.

Atunci când legea nu prevede altfel, operatorul comunică persoanei vizate și următoarele informații suplimentare:

- a) temeiul juridic al prelucrării;
- b) perioada pentru care sunt stocate datele cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili perioada respectivă;
- c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv din state terțe sau organizații internaționale;
- d) orice alte informații suplimentare, în funcție de specificul activităților de prelucrare, în special atunci când datele cu caracter personal sunt colectate fără știrea persoanei vizate.

(art. 13 și art. 14 din Legea nr. 363/2018)

14. Când poate dispune operatorul amânarea, restricționarea sau omiterea furnizării de informații persoanei vizate?

Operatorul poate dispune, după caz, măsura amânării, restricționării sau omiterii furnizării de informații persoanei vizate în condițiile prevăzute la art. 14 din Legea nr. 363/2018 numai dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei vizate, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:

- a) evitarea obstrucționării bunei desfășurări a procesului penal;
- b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau a executării pedepselor;
- c) protejarea ordinii și siguranței publice;
- d) protejarea securității naționale;
- e) protejarea drepturilor și libertăților celorlalți.

Măsura amânării furnizării de informații se dispune pe o perioadă ce nu poate depăși un an, în situația în care incidența condițiilor care fac imposibilă comunicarea este limitată în timp. Măsura amânării poate fi prelungită în interiorul termenului de un an. La împlinirea termenului pentru care măsura amânării furnizării de informații a fost dispusă, operatorul transmite informațiile prevăzute de lege.

Persoana vizată este informată în scris, în cel mult 60 de zile calendaristice de la înregistrarea solicitării, cu privire la măsura amânării furnizării de informații și motivul dispunerii acesteia, cu privire la termenul pentru care a fost dispusă această măsură, precum și cu privire la faptul că se poate adresa autorității de supraveghere cu plângere împotriva deciziei operatorului sau poate ataca în instanță decizia operatorului.

Măsura restricționării furnizării de informații se dispune în situația în care incidența condițiilor care fac imposibilă comunicarea nu este limitată în timp. În situația restricționării

furnizării de informații, operatorul transmite persoanei vizate un răspuns. Forma și conținutul răspunsului sunt stabilite de fiecare operator în parte.

Măsura omisiunii furnizării de informații se dispune în situația în care chiar și simpla informare a persoanei vizate cu privire la una sau mai multe operațiuni de prelucrare este de natură să afecteze una dintre activitățile mai sus menționate la lit. a)-d).

Omisiunea furnizării de informații poate să fie parțială sau totală. În situația omisiunii parțiale, persoana vizată este informată, în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, cu privire la categoriile de prelucrări care nu sunt de natură a afecta activitățile mai sus menționate. În situația omisiunii totale, operatorul transmite persoanei vizate un răspuns. Forma și conținutul răspunsului sunt stabilite de fiecare operator în parte.

(art. 15 din Legea nr. 363/2018)

15. Poate avea acces persoana vizată la datele sale cu caracter personal?

Persoana vizată are dreptul de a obține de la operator, la cerere și în mod gratuit, confirmarea faptului că datele cu caracter personal care o privesc sunt sau nu sunt prelucrate de acesta. Operatorul este obligat, în situația în care prelucrează date cu caracter personal care privesc persoana vizată, să comunice acesteia, în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, pe lângă confirmare, inclusiv datele cu caracter personal care fac obiectul prelucrării, precum și următoarele informații:

- a) scopurile și temeiul juridic al prelucrării;
- b) categoriile de date cu caracter personal vizate;
- c) destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele cu caracter personal, în special destinatarii din state terțe sau organizații internaționale;
- d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, în cazul în care acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- e) dreptul de a solicita de la operator rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată;
- f) dreptul de a depune o plângere la autoritatea de supraveghere și datele de contact ale acesteia;
- g) comunicarea datelor cu caracter personal care sunt în curs de prelucrare și a oricărei informații disponibile cu privire la originea datelor cu caracter personal.

(art. 16 din Legea nr. 363/2018)

16. Poate dispune operatorul limitarea dreptului de acces?

Operatorul poate dispune măsura limitării dreptului de acces ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, dacă o astfel de măsură este necesară și proporțională într-o societate democratică, pentru:

- a) evitarea obstrucționării bunei desfășurări a procesului penal;
- b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau a executării pedepselor;
- c) protejarea ordinii și siguranței publice;
- d) protejarea securității naționale;
- e) protejarea drepturilor și libertăților celorlalți.

(art. 17 din Legea nr. 363/2018)

17. Poate obține persoana vizată rectificarea, ștergerea sau restricționarea datelor cu caracter personal?

Persoana vizată are dreptul de a obține de la operator, la cerere și în mod gratuit, rectificarea datelor cu caracter personal inexacte care o privesc.

Persoana vizată are dreptul de a solicita completarea datelor cu caracter personal care o privesc, inclusiv prin furnizarea unei declarații suplimentare.

Operatorul are obligația de a restricționa prelucrarea datelor cu caracter personal (și nu de a le șterge) în cazul în care este incidentă una dintre următoarele situații:

- a) exactitatea datelor cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu poate fi stabilită cu certitudine;
- b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.

În situația rectificării, ștergerii ori restricționării datelor cu caracter personal operatorul are obligația să verifice dacă acestea au fost transmise unui destinatar anterior rectificării.

În cazul în care datele cu caracter personal au fost transmise unui destinatar anterior rectificării, operatorul are obligația să transmită acestuia o notificare cu privire la rectificarea, ștergerea ori restricționarea prelucrării datelor cu caracter personal, după caz.

(art. 18 și art. 19 din Legea nr. 363/2018)

18. Cum se realizează transferul de date într-o țară terță sau către o organizație internațională?

Transferul de date cu caracter personal care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către un stat terț (din afara Uniunii Europene și Zonei Economice Europene) sau către o organizație internațională, inclusiv transferurile ulterioare către un alt stat terț sau o altă organizație internațională, poate avea loc doar cu respectarea dispozițiilor prezentei legi și numai dacă sunt îndeplinite următoarele condiții:

a) transferul este necesar pentru realizarea scopurilor prevăzute la art. 1 din Legea nr. 363/2018, respectiv: realizarea activităților de prevenire, descoperire, cercetare, urmărire penală și combatere a infracțiunilor, de executare a pedepselor, măsurilor educative și de siguranță, precum și de menținere și asigurare a ordinii și siguranței publice de către autoritățile competente;

b) datele cu caracter personal sunt transferate unui operator dintr-o țară terță, care este o autoritate competentă, în sensul art. 4 lit. g) din Legea nr. 363/2018, sau unei organizații internaționale, înființată în scopul prevăzut la art. 1 din Legea nr. 363/2018;

c) în cazul în care datele cu caracter personal au fost transmise sau au fost puse la dispoziție de către autoritățile competente ale altui stat membru, acel stat membru a autorizat în prealabil efectuarea transferului, în conformitate cu dreptul său intern;

d) Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție, în temeiul art. 36 din 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 al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, sau, în absența unei astfel de decizii, există sau se oferă garanții adecvate în temeiul art. 37 din Directivă sau, în absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu art. 36 sau a unor garanții adecvate în conformitate cu art. 37, se aplică derogări pentru situații speciale în conformitate cu art. 38 din aceasta;

e) în cazul unui transfer ulterior către un alt stat terț sau organizație internațională, autoritatea competentă care a realizat transferul inițial sau o altă autoritate competentă din același stat membru autorizează transferul ulterior, ținând seama în mod corespunzător de toți factorii relevanți.

Autoritățile competente române autorizează transferul datelor cu caracter personal către un stat terț sau către o organizație internațională, la cererea unei autorități competente

dintr-un stat membru, numai dacă sunt îndeplinite condițiile prevăzute de Legea nr. 363/2018.

(art. 43 din Legea nr. 363/2018)

19. Când este permis întotdeauna transferul de date cu caracter personal către o țară terță sau către o organizație internațională?

Transferul de date cu caracter personal către o țară terță sau o organizație internațională este întotdeauna posibil **atunci când Comisia Europeană a decis că statul terț**, un teritoriu ori una sau mai multe diviziuni administrativ-teritoriale determinate din acel stat terț sau organizația internațională în cauză **asigură un nivel de protecție adecvat**.

Autoritățile competente române au obligația monitorizării listei statelor terțe, a teritoriilor și diviziunilor administrativ-teritoriale determinate din statele terțe și a organizațiilor internaționale în cazul cărora Comisia Europeană a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat, prin consultarea Jurnalului Oficial al Uniunii Europene și a siteului web al Comisiei Europene.

(art. 44 din Legea nr. 363/2018)

20. În ce alte situații se mai poate efectua transferul de date cu caracter personal către o țară terță sau către o organizație internațională?

În absența unei decizii adoptate de Comisia Europeană, transferul de date cu caracter personal către o țară terță sau către o organizație internațională poate avea loc atunci când:

a) au fost stabilite garanții adecvate în ceea ce privește protecția datelor cu caracter personal printr-un act cu caracter juridic obligatoriu; sau

b) operatorul a evaluat toate circumstanțele aferente transferului de date cu caracter personal și a concluzionat că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal.

În cazul în care nu pot fi îndeplinite condițiile de mai sus, un transfer sau o categorie de transferuri de date cu caracter personal către o țară terță sau către o organizație internațională poate avea loc numai în condițiile în care transferul este necesar pentru atingerea unuia dintre următoarele scopuri:

a) protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane, cum ar fi prevenirea unui pericol iminent cel puțin asupra vieții, integrității corporale sau sănătății acestora;

b) protejarea intereselor legitime ale persoanei vizate, în cazul în care există o dispoziție legală expresă în acest sens;

c) prevenirea unei amenințări imediate și grave la adresa ordinii și siguranței publice a unui stat membru sau a unei țări terțe; d) în cazuri individuale în scopurile stabilite la art. 1 din Legea nr. 363/2018;

e) într-un caz individual pentru descoperirea, exercitarea sau apărarea unui drept în instanță privind scopurile stabilite la art. 1 din Legea nr. 363/2018.

(art. 45 și art. 46 din Legea nr. 363/2018)

21. Ce înseamnă interoperabilizare?

Interoperabilizare înseamnă operațiunea de a pune în legătură datele cu caracter personal cuprinse într-un fișier, într-o bază de date sau într-un sistem de evidență automat cu cele cuprinse într-unul sau mai multe fișiere, baze de date sau sisteme de evidență automate care sunt gestionate de operatori diferiți sau de către același operator, dar având scopuri diferite, similare sau corelate, după caz.

(art. 4 lit. q) din Legea nr. 363/2018)

22. Pot fi interoperabilizate sistemele de evidență a datelor cu caracter personal?

Sistemele de evidență a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care operatorii le dețin, pentru scopuri diferite, pot fi interoperabilizate pentru realizarea activităților de cercetare și combatere a infracțiunilor.

Interoperabilizarea sistemelor de evidență a datelor cu caracter personal sau a mijloacelor automate de prelucrare a datelor cu caracter personal se poate realiza și cu sistemele de evidență ori cu mijloacele automate de prelucrare a datelor cu caracter personal deținute de alți operatori, autorități și instituții publice naționale în scopul realizării activităților de cercetare și combatere a infracțiunilor.

În cazul activităților de prevenire a infracțiunilor, de menținere și de asigurare a ordinii și siguranței publice, sistemele de evidență a datelor cu caracter personal sau mijloacele automate de prelucrare a datelor cu caracter personal pot fi interoperabilizate cu:

- a) Registrul național de evidență a persoanelor;
- b) Registrul național de evidență a pașapoartelor simple;
- c) Registrul național de evidență a permiselor de conducere și a vehiculelor înmatriculate.

(art. 49 și art. 50 din Legea nr. 363/2018)

23. Ce măsuri trebuie să ia operatorii și persoanele împuternicite de operatori pentru asigurarea securității prelucrării datelor cu caracter personal?

Operatorul, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de gradul de ingerință în drepturile și libertățile persoanelor fizice, este obligat să aplice măsurile tehnice și organizatorice adecvate pentru a asigura și a fi în măsură să demonstreze efectuarea prelucrării în conformitate cu prezenta lege.

Măsurile adoptate trebuie să fie proporționale cu operațiunile de prelucrare realizate de către operator și includ politici corespunzătoare de protecție a datelor cu caracter personal.

În scopul punerii în aplicare în mod eficient a principiilor de protecție a datelor cu caracter personal, precum și pentru reducerea la minimum a prelucrărilor de date cu caracter personal, dar și în scopul integrării garanțiilor necesare în cadrul prelucrării, pentru a îndeplini cerințele Legii nr. 363/2018 și pentru a proteja drepturile persoanelor vizate, operatorul este obligat ca, la momentul stabilirii mijloacelor de prelucrare, precum și la cel al prelucrării efective, să pună în aplicare măsuri tehnice și organizatorice adecvate, având în vedere:

- a) stadiul actual al tehnologiei;
- b) costurile de punere în aplicare;
- c) natura, domeniul de aplicare, contextul și scopurile prelucrării;
- d) riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice pe care le prezintă prelucrarea.

Operatorul are obligația de a pune în aplicare măsuri tehnice și organizatorice adecvate prin care să se asigure că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării.

(art. 22 și art. 23 din Legea nr. 363/2018)

24. Care sunt atribuțiile Autorității naționale de supraveghere (ANSPDCP)?

Autoritatea națională de supraveghere îndeplinește competențele de supraveghere și control prevăzute la art. 57 alin. (1) lit. b), c) și t) din Regulamentul (UE) 2016/679, precum și următoarele:

a) promovează acțiuni de conștientizare în rândurile operatorilor și ale persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul Legii nr. 363/2018;

b) furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul Legii nr. 363/2018 și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;

c) primește plângerile depuse de o persoană vizată sau de un organism, o organizație sau o asociație, în conformitate cu art. 55 sau 57 din Legea nr. 363/2018, investighează într-o măsură adecvată obiectul plângerii și informează persoana care a depus plângerea cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;

d) verifică legalitatea prelucrării în conformitate cu art. 20 din Legea nr. 363/2018 și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul art. 20 alin. (3) din aceeași lege sau cu privire la motivele pentru care nu a avut loc verificarea;

e) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă reciproc asistență pentru a asigura consecvența aplicării și respectării Legii nr. 363/2018;

f) desfășoară investigații privind aplicarea Legii nr. 363/2018, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau autoritate publică;

g) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informațiilor și comunicațiilor;

h) oferă consiliere cu privire la operațiunile de prelucrare menționate la art. 33 și 34 din Legea nr. 363/2018.

De asemenea, Autoritatea națională de supraveghere are următoarele competențe:

a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la probabilitatea ca operațiunile de prelucrare vizate să încalce prevederile Legii nr. 363/2018;

b) de a dispune operatorului sau persoanei împuternicite de către operator să asigure conformitatea operațiunilor de prelucrare cu prevederile Legii nr. 363/2018, specificând, după caz, modalitatea și termenul-limită pentru aceasta, în special dispunând rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării acestora, în conformitate cu art. 18 din Legea nr. 363/2018;

c) de a dispune limitarea temporară sau definitivă ori interdicția prelucrărilor.

În exercitarea competențelor de investigare, Autoritatea națională de supraveghere are acces la toate datele cu caracter personal prelucrate de operator și persoana împuternicită de operator, precum și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.

Autoritatea națională de supraveghere nu este competentă să supravegheze operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare.

(art. 52 și art. 53 din Legea nr. 363/2018)

25. Ce sancțiuni poate aplica Autoritatea națională de supraveghere în cazul în care constată încălcarea prevederilor Legii nr. 363/2018?

În cazul constatării încălcării prevederilor Legii nr. 363/2018 de către operator sau, după caz, de către persoana împuternicită de operator, Autoritatea națională de supraveghere încheie un proces-verbal de constatare și sancționare a contravenției prin care se aplică sancțiunea **avertismentului**, conform art. 58 alin. (2) lit. b) din Regulamentul general privind protecția datelor, și **la care anexează un plan de remediere**.

Termenul de remediere se stabilește în funcție de riscurile asociate prelucrării, precum și demersurile necesar a fi îndeplinite pentru asigurarea conformității prelucrării.

În termen de 10 zile de la data expirării termenului de remediere, **Autoritatea națională de supraveghere poate să reia controlul.**

Dacă, la reluarea controlului, Autoritatea națională de supraveghere constată faptul că **operatorul nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere**, aceasta, în funcție de circumstanțele fiecărui caz în parte, **poate aplica sancțiunea contravențională a amenzii.**

Autoritatea națională de supraveghere poate aplica amenzi de la 10.000 lei până la 100.000 lei, respectiv de la 20.000 până la 200.000 lei, în funcție de contravențiile constatate prevăzute la art. 61 din Legea nr. 363/2018.

(art. 61, art. 62 și art. 63 din Legea nr. 363/2018)