PRELUCRAREA DATELOR PERSONALE DE CĂTRE
UNITATEA NAȚIONALĂ DE INFORMAȚII PRIVIND PASAGERII
DIN CADRUL INSPECTORATULUI GENERAL AL POLIȚIEI DE FRONTIERĂ

Unitatea Națională de Informații privind Pasagerii aplică prevederile legislației comunitare și naționale în materie, asigurîndu-se că drepturile persoanelor cu privire la protectia datelor personale sunt permanent respectate.

1. IDENTITATEA OPERATORULUI DE DATE

Unitatea Națională de Informații privind Pasagerii este structură de specialitate, fără personalitate juridică, în cadrul Inspectoratului General al Poliției de Frontieră, care prelucrează date cu caracter personal în scopul îndeplinirii atribuțiilor sale, prevăzute de Legea nr. 284 din 26 noiembrie 2018 privind utilizarea datelor din registrul cu numele pasagerilor din transportul aerian pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale.

Desemnarea operatorului

Conform art. 32 din Legea nr. 284/2018 în sensul Regulamentului UE 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și a legislației de punere în aplicare a acestuia se desemnează Inspectoratul General al Poliției de Frontieră în calitate de operator pentru prelucrările efectuate în cadrul Sistemului de evidență a datelor PNR.Cererile formulate în exercitarea drepturilor persoanelor vizate se adresează numai U.N.I.P.

- **DATELE DE CONTACT ALE U.N.I.P.**

Sediul: București, sector 6, Bulevardul Geniului, nr. 42C
Adresa e-mail: unip@igpf.ro
Telefon: 021.316.25.98; 021.318.25.92
Fax: 021.312.11.89
Telefon de informare: (+4)0219590

- **DATELE DE CONTACT ALE RESPONSABILULUI CU PROTECȚIA DATELOR U.N.I.P.**

La nivelul U.N.I.P. funcţionează Compartimentul Responsabil cu Protecția Datelor U.N.I.P.
Sediul: București, sector 6, Bulevardul Geniului, nr. 42C
Responsabili cu protecția datelor U.N.I.P.:
DUMITRU ALEXANDRU-GABRIEL
POPA CRISTIAN-EDUARD
Adresa e-mail: protectiadatelor.unip@igpf.ro
Telefon: 021.316.25.98/ interior 19.270, fax 021.316.35.11.

2. CADRUL LEGAL

- **Legislaţie europeană**:
  - Regulamentul UE 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
  - Directiva UE 2016/681 a Parlamentului European şi 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
  - Directiva UE 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date;
  - Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidenţialităţii în sectorul comunicaţiilor publice;

- Convenţia de Implementare a Acordului Schengen - art.102-118 - protecţia datelor personale în S.I.S. şi art. 126-130 - protecţia datelor cu caracter personal;
- Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, actualizată;

- **Legislaţie naţională**:
  - Legea nr. 284/2018 privind utilizarea datelor din registrul cu numele pasagerilor din transportul aerian pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale
  - Ordonanța nr. 34/2006 privind obligația transportatorilor aerieni de a comunica date despre pasageri
  - 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;
  - Legea nr. 682/2001 privind ratificarea de către România a Conventiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, actualizată;
  - Legea nr.129/2018 pentru modificarea şi completarea Legii nr.102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
  - Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (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);
  - Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

3. U.N.I.P. ÎNDEPLINEȘTE URMĂTOARELE ATRIBUȚII PRINCIPALE:

a) colectarea datelor PNR de la transportatorii aerieni, stocarea și prelucrarea acestor date și transferul datelor respective sau al rezultatului prelucrării acestora către autoritățile competente, în condițiile stabilite la art. 20-22 din Legea nr. 284/2018;
b) schimbul de date PNR și schimbul de rezultate ale prelucrării datelor PNR cu Unitățile de informații privind pasagerii din alte state membre ale Uniunii Europene și cu EUROPOL, în condițiile stabilite la art. 24, 26 și 27 din Legea nr. 284/2018;
c) schimbul de date PNR cu țări terțe, în condițiile stabilite la art. 28 și 29 din Legea nr. 284/2018.

Conform prevederilor legale în vigoare, Unitatea Națională de Informații Privind Pasagerii are obligaţia de a respecta caracterul privat şi securitatea prelucrării datelor cu caracter personal ale fiecărei persoane. De asemenea, are obligația de a administra, în condiţii de siguranţă, datele colectate pentru îndeplinirea atribuţiilor legale ce-i revin şi de a asigura persoanelor vizate, drepturile anume prevăzute în cuprinsul Legii nr. 363/2018, respectiv Regulamentului (UE) nr. 679/2016 (RGPD).

4. CE SE ÎNȚELEGE PRIN DATE CU CARACTER PERSONAL?

Date cu caracter personal: orice informaţii referitoare la o persoană fizică identificată sau identificabilă (”persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau la mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

5. PRELUCRAREA DATELOR PERSONALE

Unitatea Națională de Informații privind Pasagerii prelucrează date cu caracter personal, prin utilizarea datelor din registrul cu numele pasagerilor din transportul aerian pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale, fără consimțământul persoanei vizate, în scopul îndeplinirii atribuţiilor de serviciu, în condiţiile legii.

Registru cu numele pasagerilor sau PNR - registru al cerințelor de călătorie ale fiecărui pasager, care conține informațiile necesare pentru a permite prelucrarea și controlul rezervărilor de către transportatorii aerieni care efectuează rezervările și de către transportatorii aerieni participanți, pentru fiecare călătorie rezervată de către sau în numele oricărei persoane, indiferent că este conținut în sistemele de rezervare, în sistemele de control al plecărilor utilizate pentru verificarea pasagerilor la îmbarcarea în avion sau în sisteme echivalente care oferă aceleași funcționalități.

- **SCOPURILE ÎN CARE SUNT PRELUCRATE DATELE PNR**

Datele PNR cuprinse în Sistemul de evidență a datelor PNR se utilizează doar pentru următoarele scopuri:

a) prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism sau a infracțiunilor grave;

b) prevenirea și înlăturarea amenințărilor la adresa securității naționale prevăzute la art. 3 din Legea nr. 51/1991, republicată, cu completările ulterioare.

- **PRELUCRAREA DATELOR PNR DE CĂTRE U.N.I.P.**

U.N.I.P. prelucrează datele cuprinse în Sistemul de evidență a datelor PNR, exclusiv în următoarele scopuri:

a) efectuarea unei evaluări a pasagerilor înainte de sosirea sau de plecarea programată a acestora în/din România, în vederea identificării persoanelor cu privire la care este necesară o examinare suplimentară de către autoritățile competente și, după caz, de către EUROPOL, având în vedere faptul că respectivele persoane pot fi implicate în săvârșirea unei infracțiuni de terorism, a unei infracțiuni grave sau într-o activitate care constituie amenințare la adresa securității naționale;

b) oferirea de răspunsuri, de la caz la caz, unei cereri temeinic justificate bazate pe motive suficiente din partea autorităților competente vizând furnizarea și prelucrarea datelor PNR, în cazuri concrete, în scopurile prevăzute la art. 18 și comunicarea rezultatelor acestei prelucrări autorităților competente sau, după caz, EUROPOL;

c) analizarea datelor PNR în vederea actualizării sau a definirii de noi criterii ce urmează a fi utilizate pentru evaluările efectuate în temeiul alin. (2) lit. b) în scopul identificării oricăror persoane care pot fi implicate în săvârșirea unei infracțiuni de terorism, a unei infracțiuni grave sau într-o activitate care constituie amenințare la adresa securității naționale.

- **CATEGORII DE DESTINATARI AI DATELOR PERSONALE**

Datele PNR sau rezultatul prelucrării datelor PNR pot fi comunicate doar autorităților competente să solicite sau să primească aceste date, prevăzute la art. 11 din Legea nr. 284 din 26 noiembrie 2018 privind utilizarea datelor din registrul cu numele pasagerilor din transportul aerian pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale.

Categorii de destinatari ai datelor personale:

- persoana vizată/reprezentanții legali ai persoanei vizate;
- autorități competente prevăzute la art. 11 din Legea nr. 284/2018
- Unitățile de informații privind pasagerii din alte state membre ale Uniunii Europene și cu EUROPOL
- autorități publice de aplicare a legii (instanțe de judecată, parchete etc).

- **Transferul datelor PNR către țări terțe**

U.N.I.P. poate transfera date PNR sau rezultatul prelucrării datelor PNR către autoritățile unei țări terțe doar de la caz la caz și dacă sunt îndeplinite în mod cumulativ condițiile prevăzute la art. 28 din Legea nr. 284/2018, după ce destinatarii notifică în scris faptul că intenționează să utilizeze datele PNR în conformitate cu condițiile și garanțiile prevăzute de lege.

- **PERIOADA DE PĂSTRARE A DATELOR PNR ȘI DEPERSONALIZAREA**

Datele PNR furnizate de transportatorii aerieni se păstrează în cadrul Sistemului de evidență a datelor PNR pentru o perioadă de 5 ani de la momentul finalizării transmisiunii active a respectivelor date PNR din sistemele transportatorilor aerieni în Sistemul de evidență a datelor PNR, denumit în continuare momentul furnizării.

La împlinea unui termen de 6 luni de la momentul furnizării datelor PNR de către transportatorii aerieni, acestea sunt depersonalizate prin mascarea următoarelor elemente de date:

a) numele, inclusiv numele altor pasageri, precum și numărul pasagerilor care călătoresc împreună;
b) adresa și informațiile de contact asociate rezervării;
c) toate informațiile privind forma de plată, inclusiv adresa de facturare;
d) informațiile din profilul „client fidel“;
e) mențiunile cu caracter general prevăzute la art. 14 alin. (1) lit. l);
f) orice date API care au fost colectate.

La împlinirea termenului de 5 ani, datele PNR din sistemul de evidență a datelor PNR se șterg în mod automat, printr-o procedură ireversibilă.

- **CATEGORIILE DE DATE CU CARACTER PERSONAL PRELUCRATE**

Transportatorii aerieni transmit către U.N.I.P., în condițiile prevăzute la art. 15 și 16 din Legea nr. 284/2018, următoarele date din registrul cu numele pasagerilor:

a) codul de rezervare;
b) data rezervării sau a emiterii biletului;
c) data/datele programată/programate a/ale călătoriei;
d) numele și prenumele asociate rezervării;
e) adresa și informațiile de contact - număr de telefon, adresă de e-mail - asociate rezervării;
f) toate informațiile privind forma de plată, inclusiv adresa de facturare;
g) itinerarul complet de călătorie;
h) informațiile din profilul „client fidel“;
i) agenția sau agentul de turism prin care a fost făcută rezervarea sau a fost cumpărat biletul;
j) situația de călătorie a pasagerului, inclusiv confirmările, situația înregistrării pentru zbor, informații privind neprezentarea pasagerului la îmbarcare sau privind prezentarea acestuia în ultimul moment la îmbarcare fără rezervare prealabilă;
k) informațiile scindate sau divizate din registrul cu numele pasagerilor;
l) mențiunile cu caracter general, inclusiv toate informațiile disponibile despre minorii neînsoțiți cu vârsta sub 18 ani, precum numele și sexul minorului, vârsta, limba/limbile vorbită/vorbite, numele și datele de contact ale persoanei care îl însoțește la plecare și relația sa cu minorul, numele și datele de contact ale persoanei care îl așteaptă la sosire și relația sa cu minorul, agentul prezent la plecare și la sosire;
m) informațiile despre bilet, inclusiv numărul biletului, data emiterii biletului și bilete dus simplu și câmpurile aferente furnizării automate a prețului unui bilet de călătorie;
n) numărul locului și alte informații privind locul;
o) informațiile cu privire la codurile partajate;
p) toate informațiile cu privire la bagaje;
q) numărul pasagerilor înregistrați în PNR și alte nume ale acestora;
r) orice date API colectate, inclusiv tipul, numărul, țara de emitere și data expirării oricărui document de identitate, cetățenia, numele de familie, prenumele, sexul, data nașterii, compania aeriană, numărul zborului, data plecării, data sosirii, aeroportul de plecare, aeroportul de sosire, ora plecării și ora sosirii;
s) un istoric al tuturor modificărilor datelor PNR prevăzute la lit. a)-r).

6. DREPTURILE PERSOANELOR VIZATE

Ca o garanție a realizării scopului declarat al Legii nr. 363/2018 și Regulamentului (UE) nr. 679/2016, drepturile ce revin persoanei vizate sunt:

- dreptul la informare (art. 12, 13, 14 din Legea nr. 363/2018 și art. 13, 14, 34 din RGPD);
- dreptul de acces al persoanei vizate (art. 16 din Legea nr. 363/2018 și art. 15 din RGPD);
- dreptul la ștergerea datelor - ”dreptul de a fi uitat” (art. 18 din Legea nr. 363/2018 și art. 17 din RGPD);
- dreptul de a depune o plângere la o autoritate de supraveghere (art. 57 din Legea nr. 363/2018 și art. 77 din RGPD);

- dreptul de a se adresa justiţiei (art. 58 din Legea nr. 363/2018 și art. 79 din RGPD).

Drepturile cuprinse în Legea nr. 363/2018 sunt redate mai jos:

Dreptul la informare (art. 12, 13, 14 din Legea nr. 363/2018)
ART. 12
(1) Operatorii sunt obligați să instituie măsurile organizatorice, tehnice şi de procedură pentru a furniza persoanei vizate informaţiile necesare potrivit prevederilor art. 13 şi art. 16-21 şi pentru a asigura transmiterea unui răspuns în legătură cu prelucrările desfăşurate în condiţiile prevăzute la art. 11 sau în legătură cu notificarea persoanelor vizate în cazul apariției unui incident de securitate, în condiţiile prevederilor art. 39.
(2) Răspunsul trebuie formulat într-o formă concisă, inteligibilă şi ușor accesibilă, utilizând un limbaj clar şi simplu.
(3) Comunicarea informaţiilor în condiţiile prevăzute la alin. (2) se realizează în același format în care cererea a fost formulată, cu următoarele excepții:
a) identitatea solicitantului nu poate fi stabilită cu exactitate, în condiţiile prevăzute la alin. (10);
b) formatul ales pentru transmiterea cererii presupune riscuri de prelucrare neautorizată sau ilegală ori de pierdere, distrugere sau deteriorare accidentală, prin raportare la cantitatea de date cu caracter personal, gradul de sensibilitate al informaţiei, în special în situaţia categoriilor de date prevăzute la art. 10 ori a datelor referitoare la minori.
(4) Operatorul este obligat să instituie măsuri organizatorice şi de procedură în scopul facilitării exercitării drepturilor persoanei vizate în temeiul prevederilor art. 11 şi art. 16-21.
(5) Operatorul are obligaţia de a informa persoana vizată, în scris, cu privire la modul de soluţionare a cererilor formulate în temeiul prezentei legi. Răspunsul se transmite în mod gratuit, în cel mult 60 de zile calendaristice.
(6) 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 informaţiilor sau pentru luarea măsurilor solicitate; sau
b) să refuze să dea curs cererii.
(7) Cuantumul taxei prevăzute la alin. (6) lit. a) va fi stabilit, respectiv actualizat prin act administrativ emis la nivelul operatorului.
(8) Caracterul nefondat sau excesiv al cererii se stabileşte de la caz la caz, în funcţie de următoarele criterii:
a) obiectul cererii;
b) caracterul repetitiv al cererii;
c) existenţa unor prelucrări suplimentare de date cu caracter personal, prin raportare la cele desfăşurate la momentul formulării cererii precedente.
(9) Caracterul nefondat sau excesiv al cererii, în condiţiile prevăzute la alin. (6), trebuie demonstrat de operator.
(10) În cazul în care identitatea persoanei care formulează o cerere în temeiul prevederilor art. 16 sau 18 nu a putut fi stabilită cu exactitate, operatorul îi solicită acesteia informaţii suplimentare necesare pentru confirmarea identităţii.
(11) Informaţiile suplimentare colectate potrivit prevederilor alin. (10) nu pot fi prelucrate în niciun alt scop decât pentru confirmarea identităţii şi se distrug în termen de 3 ani de la colectare. Operatorul poate stabili termene de păstrare mai mici.
ART. 13
Operatorii sunt obligaţi să instituie măsuri organizatorice, tehnice şi de procedură în scopul punerii la dispoziţia persoanelor interesate a următoarelor categorii de informaţii:
a) identitatea şi datele de contact ale operatorului;
b) datele de contact ale responsabilului cu protecţia datelor, după caz;
c) scopurile în care sunt prelucrate datele cu caracter personal;
d) dreptul de a depune o plângere la autoritatea de supraveghere şi datele de contact ale acesteia;
e) dreptul de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ştergerea acestor date sau restricţionarea prelucrării lor.
ART. 14
La cerere, atunci când legea nu prevede altfel, operatorul comunică persoanei vizate informaţiile prevăzute la art. 13, precum şi următoarele informaţii 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 terţe sau organizaţii internaţionale;
d) orice alte informaţii suplimentare, în funcţie de specificul activităţilor de prelucrare, în special atunci când datele cu caracter personal sunt colectate fără ştirea persoanei vizate.

Dreptul de acces al persoanei vizate (art. 16 din Legea nr. 363/2018)
ART. 16
(1) Persoana vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit, confirmarea faptului că datele cu caracter personal care o privesc sunt sau nu sunt prelucrate de acesta.
(2) Operatorul este obligat, în situaţia 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, în condiţiile prevăzute la art. 12 alin. (2) şi (3), pe lângă confirmare, inclusiv datele cu caracter personal care fac obiectul prelucrării, precum şi următoarele informaţii:
a) scopurile şi 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 terţe sau organizaţii internaţionale;
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 ştergerea datelor cu caracter personal sau restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată;
f) dreptul de a depune o plângere la autoritatea de supraveghere şi datele de contact ale acesteia;
g) comunicarea datelor cu caracter personal care sunt în curs de prelucrare şi a oricărei informaţii disponibile cu privire la originea datelor cu caracter personal.

Dreptul la ștergerea datelor – „dreptul de a fi uitat” (art. 18 din Legea nr. 363/2018)
ART. 18
(3) Operatorul are obligaţia de a şterge, prin proceduri ireversibile, din oficiu sau la cererea persoanei vizate, datele cu caracter personal a căror prelucrare nu este conformă dispoziţiilor art. 1 alin. (2), art. 5 sau 10 ori care trebuie şterse în virtutea îndeplinirii unei obligaţii prevăzute expres de lege.
(4) Operatorul are obligaţia de a restricţiona prelucrarea datelor cu caracter personal, şi nu de a le şterge, în cazul în care este incidentă una dintre următoarele situaţii:
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.
(5) Operatorul este obligat să comunice persoanei vizate, în condiţiile art. 12 alin. (2)-(4), în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, confirmarea sau, după caz, infirmarea soluţionării cererilor formulate potrivit prevederilor alin. (1), (2) sau (3), motivele pe care se întemeiază măsura infirmării, precum şi faptul că se poate adresa cu plângere la autoritatea de supraveghere sau poate ataca în instanţă decizia operatorului.
(6) Termenul prevăzut la alin. (5) poate fi prelungit cu până la 60 de zile calendaristice, în măsura în care soluţionarea cererilor necesită proceduri complexe, în special consultarea unor autorităţi competente din străinătate. Persoana vizată este informată cu privire la prelungirea termenului înainte de expirarea termenului iniţial.
(7) Ridicarea restricţionării prelucrării instituite potrivit prevederilor alin. (4) lit. a) se realizează de către operator, concomitent cu notificarea persoanei vizate cu privire la măsura adoptată.
(8) Dispoziţiile alin. (5) nu se aplică dacă, ţinând seama de drepturile fundamentale şi interesele legitime ale persoanei fizice, o astfel de măsură este necesară şi proporţională într-o societate democratică pentru:
a) a evita obstrucţionarea bunei desfăşurări a procesului penal;
b) a nu prejudicia prevenirea, descoperirea, cercetarea, urmărirea penală şi combaterea infracţiunilor sau executarea pedepselor;
c) a proteja ordinea şi siguranţa publică;
d) a proteja securitatea naţională;

e) a proteja drepturile şi libertăţile celorlalţi.

Dreptul de a depune o plângere la o autoritate de supraveghere (art. 57 din Legea nr. 363/2018)
ART. 57
(1) În cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o vizează încalcă dispoziţiile prezentei legi, are dreptul de a se adresa cu plângere autorităţii de supraveghere.
(2) Dispoziţiile Regulamentului general privind protecţia datelor sunt aplicabile în mod corespunzător.

Dreptul de a se adresa justiției (art. 58 din Legea nr. 363/2018)
ART. 58
Fără a se aduce atingere posibilităţii de a se adresa cu plângere autorităţii de supraveghere, persoanele vizate au dreptul de a se adresa instanţei pentru apărarea oricăror drepturi garantate de prezenta lege, care le-au fost încălcate.

- **MODUL DE EXERCITARE A DREPTURILOR**

Pentru exercitarea drepturilor referitoare la prelucrări de date cu caracter personal efectuate de către U.N.I.P., se poate transmite/depune o cerere la sediul Inspectoratului General al Poliției de Frontieră Române din București, sector 6, Bulevardul Geniului, nr. 42C sau se poate transmite în format electronic la adresa: unip@igpf.ro

La nivelul Inspectoratului General al Poliției de Frontieră Române funcţionează Compartimentul Responsabil cu Protecția Datelor U.N.I.P., care are printre atribuții și soluționarea cererilor persoanelor vizate.

- **Exercitarea drepturilor persoanei vizate în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR**

ART. 32 din Legea 284/2018
(1) Drepturile persoanei vizate în contextul prelucrării datelor cu caracter personal în cadrul Sistemului de evidență a datelor PNR se exercită potrivit Regulamentului general privind protecția datelor și a legislației de punere în aplicare a acestuia, cu aplicarea prevederilor alin. (2)-(6), precum și ale art. 24-28 din Legea nr. 238/2009, republicată.
(2) Cererile formulate în exercitarea drepturilor persoanelor vizate se adresează numai UNIP. O cerere este validă numai în situația în care persoana vizată face dovada identității în condițiile legii.
(3) Pentru a comunica solicitantului informații cu privire la datele cu caracter personal prelucrate în cadrul Sistemului de evidență a datelor PNR, în situația prelucrărilor prevăzute la art. 24-29, UNIP solicită, după caz, acordul autorităților competente către care au fost transferate datele, acordul EUROPOL sau acordul entității similare din străinătate care a furnizat datele.
(4) Autoritățile competente comunică opțiunea în termen de 20 de zile de la data primirii solicitării din partea UNIP.
(5) În situația în care entitatea similară din străinătate consultată potrivit alin. (3) nu comunică un răspuns în considerarea termenelor de răspuns la cererile persoanelor vizate, UNIP răspunde solicitantului fără a indica proveniența datelor.

Operatorul de date cu caracter personal este obligat să comunice persoanei vizate informaţii privind acțiunile întreprinse în urma unei cereri depuse în temeiul articolelor 16 și 18 din Legea nr. 363/2018, respectiv art. 15-22 din RGPD, fără întârzieri nejustificate şi în termenele prevăzute de aceste acte normative, respectiv:
- în cel mult 60 de zile calendaristice – conform Legii nr. 363/2018;
- în cel mult o lună de la primirea cererii (această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor; operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii) – conform RGPD.

Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul de date informează persoana vizată, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri şi la posibilitatea de a depune o plângere în fața unei autorități de supraveghere şi de a introduce o cale de atac judiciară (conform RGPD).

În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.

Orice comunicare şi orice măsuri luate în temeiul articolelor 13, 16 și 18 din Legea nr. 363/2018, respectiv 15-22 şi 34 sunt oferite gratuit.
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:
- să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării sau pentru luarea măsurilor solicitate sau să refuze să dea curs cererii.

În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea, operatorul poate solicita furnizarea de informaţii suplimentare persoanei vizate (legitimarea - atunci când cererea se depune personal sau transmiterea unei copii după documentul de identitate – atunci când cererea se transmite prin poștă sau electronic).
Verificarea identităţii solicitantului este necesară în scopul:
- obținerii dovezii rezonabile a identităţii solicitantului/obținerii dovezii certe a relației dintre solicitant şi persoana vizată, acolo unde cererea se face în numele persoanei vizate;
- protejării datelor cu caracter personal împotriva unui acces neautorizat sau ilegal;
- asigurării persoanei vizate că operatorul ia toate măsurile tehnice şi organizatorice pentru a asigura securitatea şi confidenţialitatea datelor cu caracter personal

Informaţiile suplimentare colectate nu pot fi prelucrate în niciun alt scop decât pentru confirmarea identităţii şi se distrug în termen de 3 ani de la colectare. Operatorul poate stabili termene de păstrare mai mici.

- **EXCEPȚIILE PRIVIND EXERCITAREA DREPTURILOR**

Excepțiile privind exercitarea drepturilor sunt prevăzute atât de Legea nr. 363/2018, cât și de RGPD.
Excepțiile prevăzute de Legea nr. 363/2018 sunt:
- amânarea, restricționarea sau omiterea furnizării de informaţii la cererea persoanei vizate (Art. 15);
- limitarea dreptului de acces (Art. 17).

Măsura amânării, restricționării sau omiterii furnizării de informaţii persoanei

ART. 15
(1) Operatorul poate dispune, după caz, măsura amânării, restricţionării sau omiterii furnizării de informaţii persoanei vizate în condiţiile prevăzute la art. 14 numai dacă, ţinând seama de drepturile fundamentale şi interesele legitime ale persoanei vizate, o astfel de măsură este necesară şi proporţională într-o societate democratică pentru:
a) evitarea obstrucţionării bunei desfăşurări a procesului penal;
b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau a executării pedepselor;
c) protejarea ordinii şi siguranţei publice;
d) protejarea securităţii naţionale;
e) protejarea drepturilor şi libertăţilor celorlalţi.
(2) Măsura amânării furnizării de informaţii se dispune pe o perioadă ce nu poate depăşi un an, în situaţia în care incidenţa condiţiilor 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 informaţii a fost dispusă, operatorul transmite informaţiile prevăzute de lege.
(3) Persoana vizată este informată în scris, în cel mult 60 de zile calendaristice de la înregistrarea solicitării, cu privire la măsura amânării furnizării de informaţii şi motivul dispunerii acesteia, cu privire la termenul pentru care a fost dispusă această măsură, precum şi cu privire la faptul că se poate adresa autorităţii de supraveghere cu plângere împotriva deciziei operatorului sau poate ataca în instanţă decizia operatorului.
(4) Măsura restricţionării furnizării de informaţii se dispune în situaţia în care incidenţa condiţiilor care fac imposibilă comunicarea nu este limitată în timp. În situaţia restricţionării furnizării de informaţii, operatorul transmite persoanei vizate un răspuns. Forma şi conţinutul răspunsului sunt stabilite de fiecare operator în parte.

(5) Măsura omisiunii furnizării de informaţii se dispune în situaţia în care chiar şi simpla informare a persoanei vizate cu privire la una sau mai multe operaţiuni de prelucrare este de natură să afecteze una dintre activităţile prevăzute la alin. (1) lit. a)-d).
(6) Omisiunea furnizării de informaţii poate să fie parţială sau totală. În situaţia omisiunii parţiale, 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 activităţile prevăzute la alin. (1). În situaţia omisiunii totale, operatorul transmite persoanei vizate un răspuns. Forma şi conţinutul răspunsului sunt stabilite de fiecare operator în parte.
(7) Operatorul este obligat să ţină evidenţa situaţiilor în care a fost dispusă măsura omiterii furnizării de informaţii şi să documenteze adoptarea acestei măsuri.
(8) În luna ianuarie a fiecărui an, operatorul are obligaţia de a informa autoritatea de supraveghere cu privire la situaţia statistică a măsurilor de omisiune a furnizării de informaţii adoptate în anul precedent, defalcat pentru fiecare dintre activităţile prevăzute la alin. (1) lit. a)-d).

Limitarea dreptului de acces
ART. 17
(1) Dispoziţiile art. 16 nu se aplică dacă, ţinând seama de drepturile fundamentale şi interesele legitime ale persoanei fizice, o astfel de măsură este necesară şi proporţională într-o societate democratică pentru:
a) evitarea obstrucţionării bunei desfăşurări a procesului penal;
b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau a executării pedepselor;
c) protejarea ordinii şi siguranţei publice;
d) protejarea securităţii naţionale;
e) protejarea drepturilor şi libertăţilor celorlalţi.
(2) Măsura limitării dreptului de acces poate să fie totală sau parţială şi se dispune cu privire la una sau mai multe operaţiuni de prelucrare în situaţia cărora dezvăluirea este de natură să afecteze una dintre activităţile prevăzute la alin. (1).
(3) În situaţia prevăzută la alin. (2), persoana vizată poate fi informată cu privire la categoriile de prelucrări care nu sunt de natură a afecta activităţile prevăzute la alin. (1), motivul adoptării acestei măsuri, precum şi cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a se adresa instanţei.
(4) Prin excepţie de la dispoziţiile alin. (3), motivul adoptării măsurii de limitare a dreptului de acces nu se comunică în situaţia în care dezvăluirea acestuia este de natură să afecteze una dintre activităţile prevăzute la alin. (1) lit. a)-d).
(5) Operatorul este obligat să ţină evidenţa cazurilor în care a fost dispusă măsura de limitare a dreptului de acces şi să documenteze adoptarea acestei măsuri.
(6) În luna ianuarie a fiecărui an, operatorul are obligaţia de a informa autoritatea de supraveghere cu privire la situaţia statistică a cazurilor în care a fost adoptată măsura de limitare a dreptului de acces în anul precedent, defalcat pentru fiecare dintre activităţile prevăzute la alin. (1).

- **AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

Potrivit Legii nr. 102/2005, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.) are ca principal obiectiv apărarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă intimă, familială şi privată în legătură cu prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Legalitatea prelucrărilor de date cu caracter personal care cad sub incidenţa Regulamentului și a Legii nr. 363/2018 este monitorizată şi controlată de Autoritatea de supraveghere.
Coordonatele de contact ale A.N.S.P.D.C.P. sunt :
Sediul în B-dul G-ral Gheorghe Magheru 28-30, sector 1, cod poștal 010336, București
Telefon: 031.805.92.11, 031.805.92.12; Fax: 031.805.96.02; Internet: www.dataprotection.ro
E-mail: anspdcp@dataprotection.ro

- **EXERCITAREA DREPTURILOR PERSOANEI VIZATE PRIN REPREZENTARE**

ART. 80 din RGPD
1) Persoana vizată are dreptul de a mandata un organism, o organizaţie sau o asociaţie fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu dreptul intern, ale căror

obiective statutare sunt de interes public, care sunt active în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menţionate la articolele 77, 78 şi 79, precum şi să exercite dreptul de a primi despăgubiri menţionat la articolul 82 în numele persoanei vizate, dacă acest lucru este prevăzut în dreptul intern.
(2) Statele membre pot prevedea că orice organism, organizaţie sau asociaţie menţionată la alineatul (1) din prezentul articol , independent de mandatul unei persoanei vizate, are dreptul de a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul articolului 77 şi de a exercita drepturile menţionate la articolele 78 şi 79, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.

ART. 59 din Legea nr. 363/2018
În scopul apărării drepturilor sale, persoana vizată are dreptul de a mandata un organism, o organizaţie sau o asociaţie, care nu are scop lucrativ, constituită în condiţiile legii, ale cărei obiective statutare sunt de interes public şi care este activă în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor cu caracter personal, să depună plângerea în numele său şi să exercite în numele său drepturile prevăzute de prezenta lege.

Această secțiune a fost a fost actualizată la data de 01.10.2024.