Biroul permanent al Senatului
Ep 141 11.04.2018

Parlamentul României
Senat

GRUPUL PARLAMENTAR PSD

CONSILIUL ECONOMIC ŞI SOCIAL
Înregistrat nr. 1722
Data 20.04.2018

Către

BIROUL PERMANENT AL SENATULUI

Subsemnaţii, Şerban NICOLAE, senator PSD în Circumscripţia electorală nr. 42 Bucureşti şi Adrian Nicolae DIACONU, senator PSD în Circumscripţia electorală nr. 37 Timis, în conformitate cu prevederile articolului 73 din Constituţia României şi în temeiul art. 111 din Regulamentul Senatului, solicităm **procedură de urgenţă** pentru propunerea legislativă:

" Propunere legislativă privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterea infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date"

Iniţiatori:

Şerban NICOLAE, Senator P.S.D.

Adrian Nicolae DIACONU, Senator P.S.D.

Palatul Parlamentului, Calea 13 Septembrie, nr. 1-3, Email: psdsenat2016@gmail.com, Tel: +40 21 3120 378

PARLAMENTUL ROMÂNIEI
EXPUNERE DE MOTIVE

Propunere Legislativă privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterea infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date

Descrierea situaţiei actuale:

La data de 4 mai 2016, în Jurnalul Oficial al Uniunii Europene, seria L 119, a fost publicată *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 şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului,* denumită, în continuare, Directiva (UE) 2016/680.

Art.63 din Directiva (UE) 2016/680 prevede că statele membre UE sunt ţinute să adopte şi să publice, până la data de 6 mai 2018, acte cu putere de lege şi acte administrative, pentru a se conforma respectivei directive, notificând de îndată Comisiei textele dispoziţiilor în cauză.

De asemenea, concomitent cu publicarea Directivei 2016/680, a fost publicat şi *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 protecţia datelor) [denumit, în continuare Regulamentul (UE) 2016/679 sau RGPD].*

Acesta are efect direct începând cu data de 25 mai 2018 şi nu se aplică prelucrării datelor cu caracter personal efectuate de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor, sau al executării sancţiunilor penale ori al protejării împotriva ameninţărilor la adresa ordinii şi siguranţei publice şi al prevenirii acestora.

Directiva (UE) 2016/680 urmăreşte asigurarea unui nivel omogen şi ridicat de protecţie a datelor cu caracter personal ale persoanelor fizice şi facilitarea schimbului de date cu caracter personal între autorităţile competente ale statelor membre, în scopul garantării eficienţei cooperării judiciare în materie penală şi a cooperării poliţieneşti. Directiva (UE) 2016/680 asigură un nivel de protecţie echivalent în toate

statele membre UE. Protecţia efectivă a datelor cu caracter personal în întreaga Uniune Europeană necesită nu numai consolidarea drepturilor persoanelor vizate şi a obligaţiilor celor care prelucrează date cu caracter personal, ci şi competenţe echivalente pentru monitorizarea şi asigurarea conformităţii cu normele în materie de protecţie a datelor cu caracter personal în statele membre.

Instrumentul juridic european urmăreşte facilitarea liberei circulaţii a datelor cu caracter personal între autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, inclusiv al protejării împotriva ameninţărilor la adresa ordinii şi siguranţei publice şi al prevenirii acestora în cadrul Uniunii, precum şi a transferului de astfel de date cu caracter personal către ţări terţe şi organizaţii internaţionale, asigurând, totodată, un nivel ridicat de protecţie a respectivelor date cu caracter personal.

La elaborarea Directivei 2016/680 au fost luate în considerare evoluţiile tehnologice rapide şi globalizarea, care au generat noi provocări pentru protecţia datelor cu caracter personal. Totodată, au fost avute în vedere amploarea colectării şi a schimbului de date cu caracter personal ce a crescut în mod semnificativ, precum şi tehnologia ce permite prelucrarea datelor cu caracter personal la un nivel fără precedent în cadrul activităţilor precum prevenirea, descoperirea, cercetarea, urmărirea penală şi combaterea infracţiunilor ori executarea pedepselor. Aceste evoluţii au impus realizarea unui cadru solid şi mai coerent în materie de protecţie a datelor cu caracter personal în Uniune, însoţit de o aplicare riguroasă a normelor.

Totodată, art. 59 din Directiva (UE) 2016/680, abrogă, începând cu 6 mai 2018, *Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecţia datelor cu caracter personal prelucrate în cadrul cooperării poliţieneşti şi judiciare în materie penală.* La nivel naţional, *Decizia-cadru 2008/977/JAI* a fost avută în vedere la elaborarea *Legeii nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice.*

Schimbări preconizate:

Prin prezenta iniţiativă se au în vedere următoarele:
- definirea unor termeni care sunt utilizaţi în cuprinsul iniţiativei;
- introducerea unui nou principiu, al *asigurării securităţii adecvate* prelucrării datelor cu caracter personal (spre deosebire de Regulamentul 679/2016, nu a fost introdusă *transparenţa* ca principiu în cazul prelucrărilor ce intră în domeniul de reglementare al Directivei);

- impunerea obligației privind stabilirea unor termene exprese de stocare, ștergere și revizuire a necesității stocării datelor cu caracter personal și stabilirea unor proceduri specifice în acest sens;
- instituirea procedurilor necesare pentru stabilirea distincției între persoanele vizate, delimitând în acest sens categorii precum: suspecți, persoane condamnate, persoane vătămate și alte persoane;
- stabilirea unor condiții specifice de prelucrare în măsura în care datele cu caracter personal urmează să fie prelucrate în alte scopuri decât cele care se încadrează în domeniul de reglementare al Directivei – *prevenirea, descoperirea, cercetarea, urmărirea penală și combaterea infracțiunilor, executării pedepselor și protejarea împotriva amenințărilor la adresa siguranței publice*;
- stabilirea unor condiții privind *procesul decizional individual automatizat (adoptarea unor decizii care afectează persoana vizată doar pe baza rezultatelor unor prelucrări automatizate);* astfel, o decizie întemeiată exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ, este interzisă, cu excepția cazului în care este autorizată de legea care prevede garanții adecvate pentru drepturile și libertățile persoanei vizate, cel puțin dreptul de a obține intervenția umană din partea operatorului;
- asigurarea protecției datelor începând cu momentul conceperii și în mod implicit (*privacy by design* și *privacy by default*);
- reglementarea situației *operatorilor asociați* - situația în care responsabilitatea prelucrărilor nu revine unui singur operator ci mai multor operatori care stabilesc împreună scopul/scopurile și mijloacele de prelucrare;
- ținerea evidenței activităților de prelucrare;
- evaluarea impactului asupra protecției datelor cu caracter personal;
- desemnarea Responsabilului cu protecția datelor cu caracter personal;
- transferul datelor cu caracter personal către state terțe sau organizații internaționale;
- abrogarea Legii nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice.

Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care se află în vigoare la data de 6 mai 2016 și care sunt în conformitate cu dreptul Uniunii, rămân în vigoare până la modificarea, înlocuirea sau revocarea lor.

Prin referire la alin.(2) al *art.45 - Abilitări,* din cadrul *Secțiunii 2 - Abilitări, sarcini și competențe* a Directivei (UE) 680/2016, menționăm că forma acestuia din varianta în limba română este lacunară, în sensul că a fost omisă particula negației din construcția gramaticală ce vizează competența autorității de supraveghere naționale

asupra operațiunilor de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare.

Cu toate acestea, au fost analizate variantele lingvistice ale instrumentului european în limbile engleză, franceză, italiană, germană și spaniolă, în toate dintre acestea existând particula negației, astfel că art.45 alin.(2) din Directiva (UE) 680/2016 va fi transpus prin art.52 alin.(2) din proiect, având următorul conținut:

„art.52 [...]

(2) *Prin excepție de la alin.(1), autoritatea de supraveghere nu este competentă să supravegheze operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare.*"

Ținînd cont de toate cele de mai sus, prin prezentul demers se au în vedere următoarele:

- crearea noului cadrul legal în materia protecției 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 și privind libera circulație a acestor date;
- transpunerea prevederilor Directivei 2016/680;
- abrogarea Legii nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice.

Reamintim că termenul de transpunere a Directivei (UE) 2016/680 se împlinește la data de 6 mai 2018, și învederăm faptul că obligația de transpunere a unei directive a Uniunii Europene este considerată de Comisia Europeană îndeplinită numai atunci când îi sunt comunicate actele normative naționale care asigură transpunerea integrală, astfel cum au fost publicate în Monitorul Oficial al României, Partea I.

În cazul în care nu se asigură transpunerea la termen a directivei de referință, România riscă obligarea la plata unei sume forfetare, a cărei valoare minimă este de 1.887.000 euro și/sau a unor penalități în euro pe fiecare zi de întârziere, calculate din ziua comunicării unei eventuale hotărâri de condamnare de către Curtea de Justiție a Uniunii Europene, și până în ziua în care s-ar pune capăt încălcării.

Pentru toate aceste considerente, solicităm adoptarea prezentei propuneri legislative în procedură de urgență.

Inițiatori: Senator Șerban NICOLAE

Senator Adrian Nicolae DIACONU

PROIECT

PARLAMENTUL ROMÂNIEI

SENATUL ROMÂNIEI CAMERA DEPUTAŢILOR

Lege privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterea infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date

Parlamentul României adoptă următoarea lege:

Art.1 (1) Prezenta lege reglementează prelucrarea datelor cu caracter personal în scopul realizării activităţilor de prevenire, descoperire, cercetare, urmărire penală şi combatere a infracţiunilor, de executare a pedepselor, precum şi de menţinere şi asigurare a ordinii şi siguranţei publice de către autorităţile competente, în limitele competenţelor stabilite prin lege.
(2) Prelucrarea datelor cu caracter personal pentru realizarea activităţilor prevăzute la alin. (1) se realizează numai dacă această măsură este prevăzută de lege şi este necesară pentru prevenirea unui pericol cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea infracţiunilor.

Art.2 (1) Prezenta lege are ca scop protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la protecţia datelor cu caracter personal.
(2) Prezenta lege stabileşte condiţiile în care se realizează libera circulaţie a datelor cu caracter personal în scopul realizării activităţilor prevăzute la art.1 alin.(1).
(3) Libera circulaţie a datelor cu caracter personal pe teritoriul naţional sau în relaţia cu statele membre ale Uniunii Europene, circumscrisă realizării activităţilor prevăzute la art. 1 alin.(1), nu poate fi împiedicată din motive legate de protecţia persoanei faţă de prelucrările de date cu caracter personal atât timp cât condiţiile din prezenta lege sau, după caz, din 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, denumit în continuare Regulamentul general de protecție a datelor, ori din legislația națională de punere în aplicare a acestuia sunt îndeplinite.

Art.3 (1) Prezenta lege se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la art.1.
(2) Prezenta lege 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.
(3) Prezenta lege 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 de lege.

Art.4 În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații:
a) date cu caracter personal - orice informații privind o persoană fizică identificată sau identificabilă, denumită în continuare persoană 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 mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
b) prelucrare - orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
c) restricționarea prelucrării - marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;
d) creare de profiluri - orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, corectitudinea, comportamentul, localizarea sau deplasările respectivei persoane fizice;
e) pseudonimizare - prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, în măsura în care aceste informații suplimentare sunt stocate separat și fac obiectul unor măsuri de natură tehnică și organizatorică destinate să garanteze neatribuirea unei persoane fizice identificate sau identificabile;
f) sistem de evidență a datelor - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
g) autoritate competentă - 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;
h) operator - 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;
i) persoană împuternicită de către operator - persoana fizică sau juridică, instituția/autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

j) destinatar - persoana fizică sau juridică, instituția/autoritatea publică, agenția sau un alt organism căruia îi sunt transmise datele cu caracter personal, fie că aceasta este sau nu o parte terță; sunt exceptate din înțelesul definiției autoritățile competente care pot primi date cu caracter personal în cadrul unei anchete, în conformitate cu legislația aplicabilă, iar prelucrarea datelor cu caracter personal respective de către acestea respectă normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării;
k) încălcarea securității datelor cu caracter personal - orice eveniment, acțiune sau inacțiune ce poate provoca o încălcare a securității, care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod;
l) date genetice - datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la acea persoană fizică;
m) date biometrice - date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;
n) date privind sănătatea - date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
o) autoritate de supraveghere - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
p) organizație internațională - o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe state sau în temeiul unui astfel de acord;
q) interconectare - operațiunea de a pune în legătură datele cu caracter personal cuprinse într-un fișier, bază de date sau 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;
r) evidență pasivă - fișier sau bază de date cu caracter personal constituit în scopul accesării limitate și ulterior ștergerii datelor stocate din sistemul de evidență;
s) stat membru - orice stat membru al Uniunii Europene.
ș) plan de remediere - anexă la procesul-verbal de constatare și sancționare a contravenției întocmit în condițiile prevăzute la art.59, prin care Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, stabilește măsuri și un termen de remediere;
t) măsură de remediere - soluție dispusă de ANSPDCP în planul de remediere în vederea îndeplinirii de către operator sau de către persoana împuternicită de acesta, a obligațiilor prevăzute de lege;
ț) termen de remediere - perioada de timp cuprinsă între 60 și 180 de zile de la data comunicării procesului-verbal de constatare și sancționare a contravenției, în care operatorul sau persoana împuternicită de acesta are posibilitatea remedierii neregulilor constatate și îndeplinirii obligațiilor legale.

Art.5 (1) Datele cu caracter personal trebuie să fie:
a) prelucrate în mod legal și echitabil;
b) colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate într-un mod incompatibil cu aceste scopuri;
c) adecvate, relevante și neexcesive prin raportare la scopurile în care sunt prelucrate;

d) exacte şi, dacă este necesar, actualizate; trebuie adoptate toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, să fie şterse sau rectificate fără întârziere;
e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;
f) prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.
(2) Datele cu caracter personal pot fi prelucrate pentru realizarea activităţilor prevăzute la art.1 de către acelaşi operator sau de către alt operator într-un alt scop decât cel avut în vedere la momentul colectării datelor cu caracter personal, numai dacă sunt îndeplinite cumulativ următoarele condiţii:
a) operatorul este abilitat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu cadrul normativ aplicabil;
b) prelucrarea este necesară şi proporţională în raport cu scopul respectiv, în conformitate cu cadrul normativ aplicabil.
(3) Datele cu caracter personal pot fi prelucrate de către acelaşi operator sau de către alt operator în scopul arhivării în interes public sau în scopuri ştiinţifice, statistice sau istorice legate de realizarea activităţilor prevăzute la art.1 alin.(1), cu condiţia instituirii unor garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate.
(4) Operatorul este responsabil pentru respectarea prevederilor alin.(1) – (3) şi trebuie să instituie proceduri pentru a putea demonstra respectarea acestor prevederi.

Art.6 (1) Actele normative, indiferent de nivelul de legiferare, care instituie prelucrări de date cu caracter personal în scopul realizării activităţilor prevăzute la art.1 alin.(1), trebuie să stabilească cel puţin următoarele aspecte:
a) contextul general al prelucrării şi obiectivele acesteia;
b) datele cu caracter personal care urmează să fie prelucrate;
c) scopurile prelucrării;
d) termenele de stocare generale şi, după caz, specifice, a datelor cu caracter personal.
(2) La împlinirea termenelor de stocare, datele cu caracter personal pot fi:
a) arhivate în interes public în conformitate cu legislaţia specială;
b) stocate în evidenţa pasivă pentru o durată care nu poate depăşi jumătate din termenul iniţial de stocare;
c) distruse sau şterse prin utilizarea unor proceduri ireversibile, dacă nu se încadrează în una dintre situaţiile prevăzute la lit. a) sau b).
(3) Stabilirea termenelor specifice de păstrare este obligatorie în următoarele situaţii:
a) prelucrarea datelor cu caracter personal referitoare la minori;
b) prelucrarea categoriilor speciale de date cu caracter personal;
c) prelucrarea datelor cu caracter personal a căror acurateţe nu a fost stabilită sau nu a putut fi stabilită;
d) în orice altă situaţie în care prelucrarea presupune riscuri majore pentru persoana vizată.
(4) Termenele specifice de stocare nu pot fi mai mari decât jumătate din termenul general de stocare corespunzător.
(5) Prelucrările de date cu caracter personal bazate pe utilizarea noilor tehnologii sau care sunt de natură să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice pot fi instituite în scopul realizării activităţilor prevăzute la art. 1 alin. (1) numai în temeiul unui act normativ publicat în Monitorul Oficial care să stabilească garanţii necesar a fi instituite în temeiul prezentei legi.

Art.7 (1) Operatorii dispun măsurile necesare în scopul structurării datelor cu caracter personal având în vedere următoarele criterii:
a) date referitoare la persoane în privința cărora există indicii temeinice că au săvârșit sau că urmează să săvârșească o infracțiune;
b) date referitoare la persoane condamnate pentru săvârșirea unei infracțiuni;
c) date referitoare la persoane victime ale unei infracțiuni sau persoane în privința cărora există motive să se creadă că ar putea fi victimele unei infracțiuni;
d) date referitoare la alte persoane care au legătură cu infracțiunea, precum persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracțiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informații cu privire la infracțiuni sau persoane care sunt în legătură sau asociate cu persoanele prevăzute la lit. a) sau b).
(2) Datele cu caracter personal prelucrate în temeiul prezentei legi sunt ordonate în funcție de gradul lor de acuratețe și exactitate. În acest scop, operatorii dispun măsurile necesare pentru realizarea unei distincții între date colectate ca urmare a constatării unor fapte, respectiv date a căror colectare se bazează pe percepția subiectivă a unor persoane fizice.
(3) Operatorii dispun toate măsurile necesare pentru ca datele cu caracter personal inexacte, incomplete sau care nu sunt actualizate să nu fie transmise sau puse la dispoziție.
(4) Măsurile prevăzute la alin.(3) includ și evaluări periodice în scopul asigurării calității datelor cu caracter personal prin raportare la scopul în care au fost colectate și sunt ulterior prelucrate.
(5) Termenele de evaluare sunt stabilite prin acte administrative adoptate de către operatori, cărora li se asigură o formă de publicitate. Frecvența evaluărilor este determinată de scopul în care datele cu caracter personal au fost colectate, calitatea datelor la momentul colectării, cantitatea datelor, dacă sunt prelucrate categorii speciale de date cu caracter personal. Termenele de evaluare nu pot depăși doi ani de la momentul colectării, respectiv de la precedenta evaluare.
(6) Evaluarea calității datelor cu caracter personal este obligatorie înainte ca datele cu caracter personal să fie transmise sau puse la dispoziție altui operator.
(7) În situația transmiterii de date cu caracter personal, în scopul asigurării calității datelor, operatorul poate adăuga informații care să permită autorității competente destinatare să evalueze:
a) acuratețea datelor;
b) caracterul integral al datelor;
c) utilitatea datelor raportat la scopul prelucrării;
d) dacă acestea sunt actualizate.
(8) În situația unei transmiteri neconforme cu legislația în vigoare a unor date cu caracter personal sau în cazul în care se constată că datele cu caracter personal nu au calitatea necesară, operatorul este obligat să notifice de îndată destinatarul. Datele care au făcut obiectul transmiterii sunt, după caz:
a) rectificate sau șterse;
b) restricționate la prelucrare.
(9) Restricționarea prelucrării datelor cu caracter personal prevăzută la alin.(8) se dispune doar în una dintre situațiile prevăzute la art.18 alin.(4).

Art. 8 (1) Datele cu caracter personal colectate în scopul prevăzut la art.1 alin.(1) nu pot fi prelucrate în alte scopuri, cu excepția cazurilor prevăzute în mod expres de lege.
(2) În situațiile excepționale prevăzute la alin.(1), prelucrările suplimentare de date cu caracter personal se realizează în conformitate cu dispozițiile Regulamentului General de Protecție a Datelor, cu excepția activităților prevăzute la art.3 alin.(2), situație în care se aplică dispozițiile corespunzătoare cuprinse în legi speciale.
(3) Datele cu caracter personal colectate de către autoritățile competente în alte scopuri decât cele necesare îndeplinirii activităților prevăzute la art.1 alin.(1) sunt prelucrate în conformitate cu dispozițiile

Regulamentului General de Protecție a Datelor, cu excepția activităților prevăzute la art.3 alin.(2), situație în care se aplică dispozițiile corespunzătoare cuprinse în legi speciale.
(4) Dispozițiile alin.(3) se aplică inclusiv pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

Art.9 (1) În situația prelucrării datelor cu caracter personal sub forma transferului către terți, autoritatea competentă care transferă datele cu caracter personal are obligația de a informa destinatarul datelor cu caracter personal cu privire la condițiile specifice de prelucrare și obligația de a le respecta, în măsura în care astfel de condiții sunt impuse de lege.
(2) Destinatarul datelor cu caracter personal are obligația respectării condițiilor specifice de prelucrare comunicate în conformitate cu alin.(1).
(3) În situația transferului de date cu caracter personal către destinatari din state membre ale Uniunii Europene sau către agenții, oficii și organisme instituite în conformitate cu Titlul V Capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene, nu pot fi impuse condiții specifice de prelucrare, în conformitate cu alin.(1), suplimentare față de cele prevăzute de lege pentru transferul către autorități competente din România.

Art.10 Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice, prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice se poate realiza dacă este strict necesară într-un caz determinat, dacă sunt instituite garanții adecvate pentru drepturile și libertățile persoanei vizate și dacă este îndeplinită una dintre următoarele condiții:
a) prelucrarea este prevăzută expres de lege;
b) prelucrarea este necesară pentru prevenirea unui pericol iminent cel puțin asupra vieții, integrității corporale sau sănătății persoanei vizate sau ale unei alte persoane fizice;
c) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de persoana vizată.

Art.11_(1) Adoptarea unei decizii întemeiate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ este interzisă, cu excepția cazului în care prelucrarea este reglementată expres de lege, fiind prevăzute garanții adecvate pentru drepturile și libertățile persoanei vizate, inclusiv dreptul de a obține intervenția umană din partea operatorului.
(2) Prelucrarea categoriilor de date cu caracter personal prevăzute la art. 10 în scopul adoptării de decizii în condițiile alin.(1) este interzisă, cu excepția situației în care sunt instituite măsuri corespunzătoare pentru protejarea drepturilor, a libertăților și a intereselor legitime ale persoanei vizate.
(3) Crearea de profiluri care au drept rezultat discriminarea persoanelor fizice pe baza criteriilor ce determină categoriile de date prevăzute la art.10 este interzisă.

Art.12 (1) Operatorii sunt obligați să instutuie măsurile organizatorice, tehnice și de procedură pentru a furniza persoanei vizate informațiile necesare potrivit art.13, art.16-21 și pentru a asigura transmiterea unui răspuns în legătură cu prelucrările desfășurate în condițiile art.11sau în legătură cu notificarea persoanelor vizate în cazul apariției unui incident de securitate, în condițiile art.39.
(2) Răspunsul trebuie formulat într-o formă concisă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

(3) Comunicarea informațiilor în condițiile 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;
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 informației, în special în situația categoriilor de date prevăzute la art.10 ori a datelor referitoare la minori.
(4) Operatorul este obligat să instituie măsuri organizatorice și de procedură în scopul facilitării exercitării drepturilor persoanei vizate în temeiul art.11 și art.16 – 21.
(5) Operatorul are obligația de a informa persoana vizată, în scris, cu privire la modul de soluționare 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 informațiilor 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 stabilește de la caz la caz, în funcție de următoarele criterii:
a) obiectul cererii;
b) intervalul de timp scurs de la formularea cererii precedente;
c) existența unor prelucrări suplimentare de date cu caracter personal, prin raportare la cele desfășurate la momentul formulării cererii precente.
(8) Caracterul nefondat sau excesiv al cererii, în condițiile alin.(6), trebuie demonstrat de operator.
(9) În cazul în care identitatea persoanei care formulează o cerere în temeiul art.16 sau art.18 nu a putut fi stabilită cu exactitate, operatorul îi solicită acestuia informații suplimentare necesare pentru confirmarea identității.
(10) Informațiile suplimentare colectate potrivit alin.(9) nu pot fi prelucrate în niciun alt scop decât pentru confirmarea identității și se distrug în termen de 3 ani de la colectare. Operatorul poate stabili termene de păstrare mai mici.

Art.13 Operatorii sunt obligați să instituie măsuri organizatorice, tehnice și de procedură în scopul punerii la dispoziția persoanelor interesate, a următoarelor 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 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.

Art.14 La cerere, operatorul comunică persoanei vizate informațiile prevăzute la art.13, precum 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.15 (1) Operatorul poate dispune, după caz, măsura amânării, restricționării sau omiterii furnizării de informații persoanei vizate în condițiile art.14 numai dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:
a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;
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 celorlați.
(2) 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.
(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 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.
(4) 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.
(5) 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 prevăzute la alin.(1) lit.a)-d).
(6) 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 prevăzute la alin.(1). În situația omisiunii totale, operatorul transmite persoanei vizate un răspuns. Forma și conținutul răspunsului sunt stabilite de fiecare operator în parte.
(7) Operatorul este obligat să țină evidența situațiilor în care a fost dispusă măsura omiterii furnizării de informații și să documenteze adoptarea acestei măsuri.
(8) În luna ianuarie a fiecărui an, operatorul are obligația de a informa autoritatea de supraveghere cu privire la situația statistică a măsurilor de omisiune a furnizării de informații adoptate în anul precedent, defalcat pentru fiecare dintre activitățile prevăzute la alin.(1) lit.a)-d).

Art.16 (1) 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.
(2) 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,

în condițiile art.12 alin.(2) și (3), 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.17 (1) Dispozițiile art.16 nu se aplică dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:
a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;
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.
(2) Măsura limitării dreptului de acces poate să fie totală sau parțială și se dispune cu privire la una sau mai multe operațiuni de prelucrare în situația cărora dezvăluirea este de natură să afecteze una dintre activitățile prevăzute la alin.(1).
(3) În situația prevăzută la alin.(2) persoana vizată poate fi informată cu privire la categoriile de prelucrări care nu sunt de natură a afecta activitățile prevăzute la alin.(1), motivul adoptării acestei măsuri, precum și cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a se adresa instanței.
(4) Prin excepție de la dispozițiile alin.(3), motivul adoptării măsurii de limitare a dreptului de acces nu se comunică în situația în care dezvăluirea acestuia este de natură să afecteze una dintre activitățile prevăzute la alin.(1) lit.a)-d).
(5) Operatorul este obligat să țină evidența cazurilor în care a fost dispusă măsura de limitare a dreptului de acces și să documenteze adoptarea acestei măsuri.
(6) În luna ianuarie a fiecărui an, operatorul are obligația de a informa autoritatea de supraveghere cu privire la situația statistică a cazurilor în care a fost adoptată măsura de limitare a dreptului de acces în anul precedent, defalcat pentru fiecare dintre activitățile prevăzute la alin.(1) .

Art.18 (1) 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.
(2) Persoana vizată are dreptul de a solicita completarea datelor cu caracter personal care o privesc inclusiv prin furnizarea unei declarații suplimentare.
(3) Operatorul are obligația de a șterge, prin proceduri ireversibile, din oficiu sau la cererea persoanei vizate, datele cu caracter personal a căror prelucrare nu este conformă dispozițiilor art. 1 alin.(2), art.5 sau art.10 ori care trebuie șterse în virtutea îndeplinirii unei obligații prevăzute expres de lege.

(4) Operatorul are obligația de a restricționa prelucrarea datelor cu caracter personal în 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.
(5) Operatorul este obligat să comunice persoanei vizate, în condițiile art.12 alin.(2) și (3), în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, confirmarea sau, după caz, infirmarea soluționării cererilor formulate potrivit alin.(1), (2) sau (3), motivele pe care se întemeiază măsura infirmării, precum și faptul că se poate adresa cu plângere la autoritatea de supraveghere sau poate ataca în instanță decizia operatorului.
(6) Termenul prevăzut la alin.(5) poate fi prelungit cu până la 60 de zile calendaristice în măsura în care soluționarea cererilor necesită proceduri complexe, în special consultarea unor autorități competente din străinătate. Persoana vizată este informată cu privire la prelungirea termenului înainte de expirarea termenului inițial.
(7) Ridicarea restricționării prelucrării instituite potrivit alin.(4) lit.a), se realizează de către operator, concomitent cu notificarea persoanei vizate cu privire la măsura adoptată.
(8) Dispozițiile alin.(5) nu se aplică dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:
a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;
b) a nu prejudicia prevenirea, descoperirea, cercetarea, urmărirea penală și combaterea infracțiunilor sau executarea pedepselor;
c) a proteja ordinea și siguranța publică;
d) a proteja securitatea națională;
e) a proteja drepturile și libertățile celorlalți.

Art.19 (1) În situația rectificării datelor cu caracter personal potrivit art.18 alin.(1) operatorul are obligația să verifice modul în care acestea au fost colectate.
(2) În cazul în care datele cu caracter personal au fost colectate prin transfer de la o autoritate competentă, operatorul are obligația să transmită acesteia o notificare cu privire la rectificarea datelor.
(3) În situația rectificării, ștergerii ori restricționarii datelor cu caracter personal potrivit art.18 alin.(1), (3) sau (4), operatorul are obligația să verifice dacă acestea au fost transmise unui terț sau unui destinatar anterior rectificării.
(4) În cazul în care datele cu caracter personal au fost transmise unui terț sau unui destinatar anterior rectificării, operatorul are obligația să transmită acestuia o notificare cu privire la rectificarea, ștergerea ori restricționarea datelor cu caracter personal, după caz.
(5) Destinatarul sau terțul situat pe teritoriul României, ori căruia i se aplică legea română, are obligația de a dispune o măsură similară celei cu privire la care a fost notificat, cu excepția incidenței, în cazul ștergerii ori restricționării datelor cu caracter personal, a uneia dintre următoarele situații:
a) datele sunt necesare pentru prevenirea, descoperirea, cercetarea, urmărirea penală și combaterea infracțiunilor ori executarea pedepselor, altele decât cele pentru care au fost transmise;
b) datele sunt necesare pentru derularea altor proceduri judiciare sau administrative direct legate de prevenirea, descoperirea, cercetarea, urmărirea penală și combaterea infracțiunilor ori executarea pedepselor;
c) datele sunt necesare pentru prevenirea unui pericol iminent și grav la adresa ordinii și siguranței publice.
(6) În situația incidenței vreuneia dintre situațiile prevăzute la alin.(5) lit.a)-c), persoana vizată este informată cu aplicarea, după caz, a dispozițiilor art.14, cu privire la măsura adoptată, motivele pe care se întemeiază măsura infirmării, precum și cu privire la faptul că se poate adresa cu plângere autorității de supraveghere sau poate ataca în instanță decizia operatorului.

Art.20 (1) În situațiile prevăzute la art.15, art.17 alin.(3) sau art.19 alin.(6), persoana vizată se poate adresa autorității de supraveghere pentru exercitarea drepturilor prevăzute de lege.
(2) Operatorul are obligația de a informa persoana vizată cu privire la posibilitatea prevăzută la alin.(1).
(2) În situația prevăzută la alin.(1), autoritatea de supraveghere poate declanșa o investigație.
(3) La finalizarea investigației, autoritatea de supraveghere informează persoana vizată cu privire la aspectele constatate, precum și cu privire la posibilitatea de a se adresa instanței de judecată.

Art.21 Exercitarea drepturilor prevăzute la art.13, art.16 și art.17 nu poate fi limitată de faptul că datele cu caracter personal sunt cuprinse în hotărâri judecătorești, în cazierul judiciar sau în dosare de urmărire penală, cu excepția situațiilor expres prevăzute de lege.

Art.22 (1) 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 respectarea tuturor normelor privind protecția datelor cu caracter personal cuprinse în prezenta lege.
(2) Măsurile adoptate potrivit alin.(1) trebuie să fie proporționale cu operațiunile de prelucrare realizate de către operator și includ politici corespunzătoare de protecție a datelor cu caracter personal.

Art.23 (1) În scopul punerii în aplicare în mod eficient a principiilor de protecție a datelor cu caracter personal, precum și pentru reducerea la minim a prelucrărilor de date cu caracter personal, dar și în scopul integrării garanțiilor necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentei legi și pentru a proteja drepturile persoanelor vizate, operatorul este obligat ca, la momentul stabilirii mijloacelor de prelucrare cât 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.
(2) Pentru îndeplinirea obiectivelor alin.(1), operatorul evaluează, la momentul stabilirii mijloacelor de prelucrare, în scopul identificării măsurilor tehnice și organizatorice adecvate, cel puțin posibilitatea introducerii unei soluții de pseudonimizare ori a unei alte soluții tehnice cu efect similar.
(3) 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.
(4) Obligația prevăzută la alin.(3) vizează:
a) volumul de date cu caracter personal colectate;
b) gradul de prelucrare a acestora;
c) perioada de stocare;
d) accesibilitatea acestora .
(5) Prin măsurile dispuse potrivit alin.(3) și (4) operatorul trebuie să se asigure că datele cu caracter personal nu sunt accesibile, fără intervenție umană, unui număr nedefinit de utilizatori.

Art.24 (1) Operatorii asociați se desemnează printr-un act normativ, în cuprinsul căruia se stabilesc, în comun, scopurile și mijloacele de prelucrare a datelor cu caracter personal.
(2) Actul normativ prevăzut la alin.(1) trebuie să cuprindă o delimitare a responsabilităților ce revin fiecăruia dintre operatorii asociați în condițiile prezentei legi.
(3) Actul normativ prevăzut la alin.(1) trebuie să cuprindă cel puțin următoarele aspecte:
a) modalitatea de exercitare a drepturilor persoanelor vizate, în raport cu oricare dintre operatori;
b) îndatoririle fiecăruia dintre operatorii asociați cu privire la furnizarea informațiilor prevăzute la art.13;
c) punctul de contact unic pentru persoanele vizate.
(4) În situația în care scopurile și mijloacele de prelucrare nu sunt stabilite prin act normativ, responsabilitățile ce revin în condițiile prezentei legi operatorilor asociați pot fi stabilite prin intermediul unui act juridic. Acesta trebuie să cuprindă elementele prevăzute la alin.(3) și este supus obligației de punere la dispoziția persoanelor vizate. Obligația de punere la dispoziție trebuie îndeplinită cu minimum 5 zile înainte de intrarea în vigoare a respectivului act juridic.

Art.25 (1) Desemnarea persoanelor împuternicite de către operator este posibilă doar dacă există suficiente garanții pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentei legi și să asigure protecția drepturilor persoanei vizate.
(2) Desemnarea, de către o persoană împuternicită de către operator, a unei alte persoane împuternicite în scopul realizării uneia sau mai multor operațiuni de prelucrare nu este posibilă decât cu acordul scris al operatorului. Acordul scris poate fi emis doar dacă sunt îndeplinite condițiile prevăzute la alin.(1).
(3) Persoana împuternicită de către operator are obligația de a informa operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de către operator.
(4) Desemnarea prevăzută la alin.(1) sau, după caz, alin.(2) se realizează prin intermediul unui contract sau protocol încheiat între părți, care trebuie să detalieze:
a) obiectul și durata prelucrării;
b) natura și scopul prelucrării;
c) tipul de date cu caracter personal și categoriile de persoane vizate;
d) obligațiile și drepturile operatorului.
(5) Protocolul sau, după caz, contractul prevăzut la alin.(4) este supus obligației de punere la dispoziția persoanelor vizate și trebuie să stabilească, în sarcina persoanei împuternicite de către operator, următoarele obligații:
a) să acționeze numai la instrucțiunile operatorului;
b) să garanteze faptul că persoanele autorizate să prelucreze date cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate corespunzătoare;
c) să asiste operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei vizate;
d) să șteargă sau să returneze, din dispoziția operatorului, toate datele cu caracter personal după încetarea furnizării serviciilor de prelucrare a datelor cu caracter personal și să elimine copiile existente, cu excepția cazului în care există o dispoziție legală expresă care îl abilitează să stocheze în continuare datele;
e) să pună la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea dispozițiilor prezentului articol;
f) să respecte condițiile prevăzute la alin. (2)-(4) pentru recrutarea unei alte persoane împuternicite de către operator.
(6) Protocolul sau, după caz, contractul prevăzut la alin.(4) poate fi pus la dispoziția persoanelor vizate, la cerere, în format electronic.
(7) Persoana împuternicită de către operator este considerată operator în cazul în care, prin încălcarea dispozițiilor prezentei legi, aceasta stabilește scopurile și mijloacele de prelucrare pentru datele cu caracter personal puse la dispoziție de către operator.

(8) În situaţia prevăzută la alin.(7), operatorul este exonerat de răspundere numai în situaţia în care demonstrează că persoana împuternicită de operator a acţionat cu rea credinţă.

Art.26 (1) Se interzice persoanei împuternicite de către operator să prelucreze datele cu caracter personal cu depăşirea instrucţiunilor primite de la operator, cu excepţia situaţiilor prevăzute expres de lege.
(2) Orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de către operator, care are acces la date cu caracter personal, nu poate să le prelucreze decât pe baza instrucţiunilor operatorului, cu excepţia situaţiilor prevăzute expres de lege.

Art.27 (1) Operatorul este obligat să ţină evidenţa tuturor categoriilor de activităţi de prelucrare aflate în responsabilitatea sa.
(2) Evidenţa prevăzută la alin.(1) cuprinde următoarele informaţii:
a) denumirea şi datele de contact ale operatorului şi, după caz, ale operatorului asociat şi ale responsabilului cu protecţia 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 ţări terţe sau organizaţii internaţionale;
d) o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal care sunt prelucrate;
e) dacă este cazul, menţiuni cu privire la desfăşurarea activităţii de creare de profiluri;
f) dacă este cazul, categoriile de transferuri de date cu caracter personal către un stat terţ sau o organizaţie internaţională;
g) indicarea temeiului juridic al operaţiunii de prelucrare, inclusiv al transferurilor de date cu caracter personal efectuate;
h) dacă este posibil, termenele limită preconizate pentru ştergerea diferitelor categorii de date cu caracter personal;
i) dacă este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art.35.

Art.28 (1) Persoana împuternicită de către operator este obligată să ţină evidenţa tuturor categoriilor de activităţi de prelucrare aflate în responsabilitatea sa.
(2) Evidenţa prevăzută la alin.(1) cuprinde următoarele informaţii:
a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acţionează această persoană şi, după caz, cele ale responsabilului cu protecţia datelor cu caracter personal;
b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;
c) după caz, transferurile de date cu caracter personal către un stat terţ sau către o organizaţie internaţională, inclusiv indicarea statului terţ sau a organizaţiei internaţionale respective, atunci când au primit instrucţiuni explicite în acest sens de la operator;
d) dacă este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art.35.

Art.29 (1) Evidenţele prevăzute la art.27 şi 28 se păstrează în format de hârtie şi în format electronic.
(2) Operatorul sau persoana împuternicită de către operator au obligaţia de a pune la dispoziţia autorităţii de supraveghere, la solicitarea acesteia, evidenţele prevăzute la art.27 şi 28.

Art.30 (1) Operatorul sau persoana împuternicită de către operator este obligat/obligată să înregistreze, în cadrul sistemelor de prelucrare automată, toate operațiunile de prelucrare a datelor cu caracter personal.
(2) Înregistrările prevăzute la alin.(1) trebuie să conțină cel puțin următoarele informații:
a) tipul operațiunii de prelucrare;
b) codul de identificare a utilizatorului și a stației de lucru folosite;
c) numele fișierului accesat;
d) numărul operațiunilor de prelucrare efectuate;
e) codul operației executate sau programul folosit;
f) data accesului - an, lună, zi, cu precizarea inclusiv a orei și minutului la care a fost efectuată prelucrarea.
(3) În cazul operațiunilor de prelucrare sub forma consultării sau divulgării este obligatorie înregistrarea motivului prelucrării care trebuie să permită identificarea documentului/situației concrete care a stat la baza și a justificat prelucrarea datelor cu caracter personal și, după caz, a destinatarilor datelor cu caracter personal.
(4) Înregistrările prevăzute la alin.(1) pot fi utilizate doar în următoarele situații:
a) verificarea legalității prelucrării,
b) monitorizare proprie realizată de către operator sau, după caz, de către persoana împuternicită de către operator;
c) asigurarea integrității și a securității datelor cu caracter personal;
d) în cadrul unor proceduri penale, în condițiile și cu restricțiile impuse de lege.
(5) Responsabilul cu protecția datelor cu caracter personal, în realizarea atribuțiilor sale, are acces la înregistrările prevăzute la alin. (1).
(6) Înregistrările prevăzute la alin.(1) se pun la dispoziția autorității de supraveghere, la cererea acesteia.

Art.31 Operatorul sau, după caz, persoana împuternicită de către operator sunt obligați să coopereze cu autoritatea de supraveghere, la cererea acesteia, și să dispună orice măsură necesară îndeplinirii sarcinilor acesteia.

Art.32 (1) În situația în care se intenționează introducerea unei noi prelucrări de date cu caracter personal, în special în situația în care aceasta implică utilizarea de noi tehnologii, operatorul este obligat să evalueze următoarele aspecte al prelucrării:
a) natura datelor cu caracter personal prelucrate;
b) domeniul de aplicare;
c) contextul și scopurile prelucrării.
(2) În măsura în care prelucrarea prevăzută la alin.(1) este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul este obligat ca înaintea prelucrării să efectueze o evaluare a impactului operațiunilor de prelucrare preconizate asupra datelor cu caracter personal.
(3) Pentru operațiunile de prelucrare existente, operatorii sunt obligați să realizeze evaluarea prevăzută la alin.(1) și, după caz, evaluarea impactului operațiunilor de prelucrare prevăzută la alin.(2) în termen de 2 ani de la intrarea în vigoare a prezentei legi.
(4) Evaluarea impactului operațiunilor de prelucrare prevăzută la alin.(2) cuprinde cel puțin următoarele:
a) descrierea generală a operațiunilor de prelucrare preconizate;
b) evaluarea riscurilor la adresa drepturilor și libertăților persoanelor vizate;
c) măsurile preconizate în vederea abordării riscurilor;

d) garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze respectarea dispoziţiilor prezentei legi, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale celorlalte persoane interesate.

Art.33 (1) Operatorul sau, după caz, persoana împuternicită de către operator este obligat/obligată să consulte autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidenţă a datelor în situaţiile în care:
a) evaluarea impactului asupra protecţiei datelor cu caracter personal prevăzută la art.32 indică faptul că prelucrarea ar genera un risc ridicat în absenţa măsurilor luate de operator pentru atenuarea riscului;
b) tipul de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor şi libertăţilor persoanelor vizate.
(2) În cadrul procedurilor de elaborare a proiectelor de acte normative care reglementează prelucrări de date cu caracter personal sau în baza cărora vor fi realizate astfel de prelucrări este obligatorie consultarea autorităţii de supraveghere.
(3) Autoritatea de supraveghere este abilitată să stabilească o listă a operaţiunilor de prelucrare care fac obiectul consultării prealabile prevăzute la alin.(1).
(4) Operatorul sau, după caz, persoana împuternicită de către operator transmite autorităţii de supraveghere, în termen de 30 de zile calendaristice de la finalizare dar înainte de începerea prelucrării, evaluarea prevăzută la art.32.
(5) La cererea autorităţii de supraveghere, operatorul sau, după caz, persoana împuternicită de către operator pun la dispoziţia acesteia orice informaţie în scopul evaluării conformităţii prelucrării şi a riscurilor la adresa protecţiei datelor cu caracter personal ale persoanei vizate şi a garanţiilor aferente.

Art.34 (1) În cazul în care autoritatea de supraveghere constată că operaţiunile de prelucrare pentru care este consultată potrivit art.33 încalcă dispoziţiile prezentei legi, în special în cazul în care riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, aceasta formulează şi transmite operatorului sau, după caz, persoanei împuternicite de către operator, observaţii sau recomandări în termen de cel mult 30 de zile lucrătoare de la data înregistrării cererii de consultare.
(2) În funcţie de complexitatea prelucrării preconizate, termenul prevăzut la alin.(1) poate fi prelungit cu 20 de zile lucrătoare. Autoritatea de supraveghere informează operatorul şi, după caz, persoana împuternicită de către operator, în termen de 20 zile lucrătoare de la primirea cererii de consultare, cu privire la prelungirea termenului, inclusiv cu privire la motivele acesteia.
Dreptul autorităţii de supraveghere de a formula observaţii sau recomandări, în situaţia prevăzută la alin.(1), nu afectează în niciun fel exercitarea oricăreia dintre competenţele acesteia prevăzute în Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare.

Art.35 (1) Operatorul sau, după caz, persoana împuternicită de către operator implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător;
(2) La stabilirea nivelului de securitate corespunzător, operatorul, sau, după caz, persoana împuternicită de acesta, are în vedere stadiul actual al tehnologiei şi costurile implementării şi ţine seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de gradul de ingerinţă asupra drepturilor şi libertăţilor persoanelor fizice, în special cu privire la prelucrarea categoriilor speciale de date cu caracter personal prevăzute la art.10.
(3) În situaţia prelucrărilor prin mijloace automate, operatorul sau, după caz, persoana împuternicită de către operator sunt obligaţi să realizeze o evaluare a riscurilor incidente prelucrărilor preconizate.

(4) În urmă evaluării prevăzute la alin.(3), operatorul sau, după caz, persoana împuternicită de către operator, au obligația punerii în aplicare a măsurilor menite:
a) să asigure controlul accesului la echipamentele de prelucrare utilizate pentru prelucrare, denumit în continuare controlul accesului la echipamente;
b) să asigure controlul asupra suporturilor de date, în scopul împiedicării oricărei citiri, copieri, modificări sau eliminări neautorizate a acestora, denumit în continuare controlul suporturilor de date;
c) să asigure controlul asupra introducerii de date cu caracter personal, precum și asupra inspectării, modificării sau ștergerii neautorizate a datelor cu caracter personal stocate, denumit în continuare controlul stocării;
d) să asigure controlul asupra utilizării sistemelor de prelucrare automată cu ajutorul echipamentelor de comunicare a datelor, denumit în continuare controlul utilizatorului;
e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare, denumit în continuare controlul accesului la date;
f) să asigure că este posibilă verificarea și identificarea organismelor cărora le-au fost transmise sau puse la dispoziție sau s-ar putea să le fie transmise sau puse la dispoziție date cu caracter personal utilizându-se echipamente de comunicare a datelor, denumit în continuare controlul comunicării;
g) să asigure că este posibil ca ulterior să se verifice și să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal și entitatea care le-a introdus, denumit în continuare „controlul introducerii datelor;
h) să împiedice citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date, denumit în continuare controlul transportării;
i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi, denumit în continuare recuperarea;
j) să asigure funcționarea, fiabilitatea și integritatea sistemului, prin instituirea de măsuri de raportare a defecțiunilor de funcționare, precum și de asigurare a imposibilității coruperii datelor cu caracter personal stocate din cauza funcționării defectuoase a sistemului.

Art.36 (1) În cazul în care operatorul constată o încălcare a securității datelor, notifică de îndată, fără întârzieri nejustificate, autoritatea de supraveghere.
(2) În funcție de complexitatea încălcării securității, notificarea prevăzută la alin.(1) se transmite nu mai târziu de 72 de ore. În această situație, operatorul este obligat să transmită și o justificare a întârzierii. Termenul începe să curgă de la momentul la care operatorul a luat cunoștință despre încălcarea securității datelor cu caracter personal.
(3) Notificarea prevăzută la alin.(1) nu este necesară în cazul în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice.
(4) Persoana împuternicită de către operator are obligația să informeze operatorul de îndată, fără întârzieri nejustitificate, cu privire la existența unei încălcări a securității datelor cu caracter personal.
(5) Operatorul are obligația să implementeze toate măsurile necesare pentru a se asigura că persoana împuternicită de către operator respectă și îndeplinește obligațiile ce îi revin potrivit alin.(4).
(6) Notificarea prevăzută la alin.(1) trebuie să conțină cel puțin următoarele informații:
a) o descriere a naturii încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ de persoane vizate în cauză, precum și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;
b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
c) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

d) descrierea măsurilor luate sau propuse de operator pentru a remedia încălcarea securității datelor cu caracter personal, inclusiv, dacă este cazul, a măsurilor necesare pentru a atenua eventualele efecte adverse ale acesteia.
(7) În cazul în care nu este posibilă furnizarea, în același timp, a informațiilor prevăzute la alin.(6), acestea pot fi transmise treptat, fără întârzieri nejustificate, într-un termen care să nu depășească 48 ore de la momentul transmiterii notificării inițiale.

Art.37 (1) Operatorul are obligația să documenteze toate cazurile de încălcare a securității datelor cu caracter personal și să păstreze documentele pentru o perioadă de 10 ani.
(2) Documentele prevăzute la alin.(1) trebuie să cuprindă:
a) descrierea situației în care a avut loc încălcarea securității datelor cu caracter personal,
b) descrierea efectelor acesteia;
c) descrierea măsurilor de remediere întreprinse.
(3) Documentele prevăzute la alin.(1) trebuie să permită autorității de supraveghere să verifice respectarea dispozițiilor prezentului articol.

Art.38 (1) Operatorul are obligația să transmită informațiile prevăzute la art.36 alin.(6) către entitatea care, după caz, a furnizat datele cu caracter personal sau către care au fost transmise datele cu caracter personal, în cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator.
(2) Transmiterea informațiilor potrivit alin.(1) se realizează în termenul prevăzut la art.36 alin.(2).

Art.39 (1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.
(2) Informarea prevăzută la alin.(1) trebuie să conțină o descriere, folosind un limbaj simplu și clar, a naturii încălcării securității datelor cu caracter personal și cel puțin informațiile prevăzute la art.36 alin.(6) lit.b)-d).
(3) Informarea prevăzută la alin.(1) nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:
a) operatorul a pus în aplicare măsuri tehnologice și organizatorice adecvate de protecție, incidente în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor și libertăților persoanelor vizate menționat la alin. (1) nu mai este susceptibil să se materializeze;
c) necesită un efort disproporționat; în acest caz, informarea se înlocuiește cu informarea publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.
(4) În situația primirii unei notificări potrivit art.36, autoritatea de supraveghere, luând în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate dispune operatorului să informeze persoana vizată sau, după caz, să constate că oricare dintre situațiile prevăzute la alin.(3) este incidentă.
(5) Informarea prevăzută la alin.(1) poate fi amânată, restricționată sau omisă în condițiile art.15.

Art.40 (1) Operatorul este obligat să desemneze un responsabil cu protecția datelor cu caracter personal.

(2) Sunt exceptate de la obligaţia prevăzută la alin.(1) instanţele şi celelalte autorităţi judiciare independente atunci când acţionează în exerciţiul funcţiei lor judiciare.
(3) Poate fi desemnată responsabil cu protecţia datelor persoana care îndeplineşte următoarele condiţii:
a) deţine calităţi profesionale corespunzătoare;
b) deţine cunoştinţe de specialitatea în domeniul legislaţiei şi practicilor privind protecţia datelor cu caracter personal;
c) are capacitatea de a îndeplini sarcinile prevăzute la art.42.
(4) Luând în considerare structura organizatorică şi dimensiunea lor, mai multe autorităţi competente pot desemna acelaşi responsabil cu protecţia datelor.
(5) Operatorul are obligaţia să publice datele de contact ale responsabilului cu protecţia datelor şi să le comunice autorităţii de supraveghere.

Art.41 (1) Operatorul are obligaţia de a consulta responsabilul cu protecţia datelor cu caracter personal în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal.
(2) Operatorul are obligaţia de a acorda sprijin responsabilului cu protecţia datelor cu caracter personal în îndeplinirea sarcinilor prevăzute la art.42, în special prin, dar fără a se limita la:
a) asigurarea resurselor necesare pentru îndeplinirea sarcinilor;
b) asigurarea accesului la datele cu caracter personal şi la operaţiunile de prelucrare;
c) asigurarea resurselor necesare pentru menţinerea cunoştinţelor de specialitate şi adaptarea la noile tehnologii.

Art. 42 Responsabilul cu protecţia datelor îndeplineşte următoarele sarcini principale:
a) informează şi consiliază operatorul şi angajaţii acestuia care efectuează prelucrarea cu privire la obligaţiile care le revin în temeiul prezentei legi şi al altor dispoziţii legale privind protecţia datelor cu caracter personal;
b) monitorizează respectarea dispoziţiilor prezentei legi, a altor dispoziţii legale privind protecţia datelor cu caracter personal şi a politicilor operatorului în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunilor de conştientizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;
c) consiliază, la cerere, cu privire la evaluarea impactului asupra protecţiei datelor cu caracter personal şi monitorizarea funcţionării acesteia, în conformitate cu art. 32;
d) cooperează cu autoritatea de supraveghere;
e) este desemnat persoană de contact în relaţia cu autoritatea de supraveghere privind aspectele legate de prelucrare, asigurând consultarea prealabilă prevăzută la art. 33, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.

Art.43 (1) Transferul de date cu caracter personal care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către un stat terţ sau către o organizaţie internaţională, inclusiv transferurile ulterioare către un alt stat terţ sau o altă organizaţie internaţională, poate avea loc doar cu respectarea dispoziţiilor prezentei legi şi numai dacă sunt îndeplinite următoarele condiţii:
a) transferul este necesar pentru realizarea scopurilor prevăzute la art.1 alin.(1);
b) datele cu caracter personal sunt transferate unui operator dintr-o ţară terţă, care este o autoritate competentă, în sensul art.4 lit.g), sau unei organizaţii internaţionale, înfiinţată în scopul prevăzut la art.1 alin.(1);
c) în cazul în care datele cu caracter personal au fost transmise sau au fost puse la dispoziţie de către autorităţile competente ale altui stat membru, acel stat membru a autorizat în prealabil efectuarea transferului, în conformitate cu dreptul său intern;

d) Comisia Europeană a adoptat o decizie privind caracterul adecvat al nivelului de protecţie, denumită în continuare decizie de adecvare;
e) în cazul unui transfer ulterior către un alt stat terţ sau organizaţie internaţională, autoritatea competentă care a realizat transferul iniţial sau o altă autoritate competentă din acelaşi stat membru autorizează transferul ulterior, ţinând seama în mod corespunzător de toţi factorii relevanţi.
(2) La evaluarea factorilor relevanţi pentru transfer, în condiţiile alin.(1) lit.e), se au în vedere cel puţin următoarele aspecte:
a) gravitatea infracţiunii;
b) scopul în care datele cu caracter personal au fost transferate iniţial;
c) nivelul de protecţie a datelor cu caracter personal din ţara terţă sau din organizaţia internaţională către care sunt transferate ulterior datele cu caracter personal.
(3) Autorităţile competente române autorizează transferul datelor cu caracter personal către un stat terţ sau către o organizaţie internaţională, la cererea unei autorităţi competente dintr-un stat membru, numai dacă sunt îndeplinite condiţiile prevăzute de prezenta lege.
(4) Autorizarea prevăzută la alin.(3) se transmite cu celeritate, dar nu mai târziu de 30 de zile calendaristice de la primirea cererii. În situaţia în care nu sunt îndeplinite condiţiile prevăzute de prezenta lege pentru autorizarea transferului, autorităţii competente din statul membru care a formulat cererea i se comunică motivele pentru care transferul nu poate fi autorizat.
(5) Autorităţile competente române pot realiza transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu dispoziţiile alin.(1) lit.c), numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei ameninţări imediate şi grave la adresa ordinii şi siguranţei publice a unui stat membru sau a unei ţări terţe sau a intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obţinută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile este informată fără întârziere.
(6) Dispoziţiile prezentului articol, precum şi cele ale art.44-48 se aplică pentru a se asigura că nivelul de protecţie a persoanelor fizice garantat prin prezenta lege nu este subminat.

Art.44 (1) Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională este întotdeauna posibil, în condiţiile art.43 alin.(1) lit.d), atunci când Comisia Europeană a decis că statul terţ, un teritoriu ori una sau mai multe diviziuni administrativ-teritoriale determinate din acel stat terţ sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat.
(2) Transferurile realizate în condiţiile alin.(1) nu necesită autorizări speciale.
(3) Autorităţile competente au obligaţia, în situaţia transferurilor prevăzute la alin.(1), să monitorizeze şi să respecte întocmai dispoziţiile actelor de punere în aplicare adoptate de Comisia Europeană.
(4) Decizia Comisiei Europene de abrogare, modificare sau suspendare a unei decizii de adecvare nu aduce atingere transferurilor de date cu caracter personal către ţara terţă, către teritoriul sau către unul sau mai multe sectoare determinate din acea ţară terţă sau către organizaţia internaţională în cauză în conformitate cu articolele 37 şi 38.
(5) Autorităţile competente române au obligaţia monitorizării listei statelor terţe, a teritoriilor şi diviziunilor administrativ-teritoriale determinate din statele terţe şi a organizaţiilor internaţionale în cazul cărora Comisia Europeană a decis că nivelul de protecţie adecvat este asigurat sau nu mai este asigurat.

Art.45 (1) Prin excepţie de la dispoziţiile art.43 alin.(1) lit.d), în absenţa unei decizii adoptate de Comisia Europeană, transferul de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc atunci când:
a) au fost stabilite garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal printr-un act cu caracter juridic obligatoriu sau

b) operatorul a evaluat toate circumstanţele aferente transferului de date cu caracter personal şi a concluzionat că există garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal.
(2) În scopul îndeplinirii condiţiilor prevăzute la alin.(1) lit.b), operatorul trebuie să ţină cont de următoarele:
a) situaţia generală privind respectarea drepturilor omului şi a libertăţilor fundamentale;
b) legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind ordinea şi siguranţa publică, apărarea, securitatea naţională şi dreptul penal, precum şi punerea în aplicare a acestei legislaţii;
c) accesul autorităţilor publice la datele cu caracter personal;
d) legislaţia privind protecţia datelor cu caracter personal;
e) măsurile privind asigurarea securităţii datelor cu caracter personal;
f) legislaţia privind transferul ulterior de date cu caracter personal către o altă ţară terţă sau organizaţie internaţională;
g) drepturile efective şi opozabile ale persoanelor vizate şi reparaţii efective pe cale administrativă şi judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate.
(3) Operatorul informează autoritatea de supraveghere cu privire la transferurile realizate în condiţiile alin.(1) lit.b).
(4) Operatorul are obligaţia să ţină evidenţa transferurilor realizate în condiţiile alin.(1) lit.b), precizând cel puţin următoarele:
a) data şi ora transferului;
b) informaţii cu privire la autoritatea competentă destinatară;
c) informaţii cu privire la justificarea transferului;
d) datele cu caracter personal transferate.
(5) Documentaţia prevăzută la alin.(4) se păstrează pentru o perioadă de 10 ani şi, la cerere, se pune la dispoziţia autorităţii de supraveghere.

Art.46 (1) Prin excepţie de la dispoziţiile art.45 alin.(1) şi în cazul în care nu pot fi îndeplinite condiţiile prevăzute la art.44, un transfer sau o categorie de transferuri de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc numai în condiţiile în care transferul este necesar pentru:
a) protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane, cum ar fi prevenirea unui pericol iminent cel puţin asupra vieţii, integrităţii corporale sau sănătăţii acestora;
b) protejarea intereselor legitime ale persoanei vizate, în cazul în care există o dispoziţie legală expresă în acest sens;
c) prevenirea unei ameninţări imediate şi grave la adresa ordinii şi siguranţei publice a unui stat membru sau a unei ţări terţe;
d) în cazuri individuale în scopurile stabilite la art.(1) alin.(1);
e) într-un caz individual pentru descoperirea, exercitarea sau apărarea unui drept în instanţă privind scopurile stabilite la art. 1 alin. (1).
(2) Se interzice transferul datelor cu caracter personal în condiţiile alin.(1) lit.d) şi e) în cazul în care în urma evaluărilor realizate de autoritatea competentă română care transferă datele cu caracter personal se stabileşte că drepturile şi libertăţile fundamentale ale persoanei vizate prevalează asupra interesului public, în special în situaţia în care există indicii privind posibila afectare a dreptului la viaţă al persoanei.
(3) În situaţia transferurilor realizate în condiţiile alin.(1), dispoziţiile art.45 alin.(4) şi (5) se aplică în mod corespunzător.

Art.47 (1) În cazuri individuale specifice, dacă sunt îndeplinite toate condiţiile referitoare la transferul de date cu caracter personal prevăzute de prezenta lege, operatorul poate transfera date cu caracter personal

către entități din state terțe care nu sunt autorități competente în înțelesul prezentei legi, numai dacă sunt îndeplinite următoarele condiții:
a) transferul este strict necesar pentru exercitarea unei atribuții prevăzute de lege în sarcina autorității competente române, în scopul îndeplinirii activităților prevăzute la art. 1 alin. (1);
b) autoritatea competentă română stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața interesului public care impune transferul în cazul respectiv;
c) din evaluările realizate de către autoritatea competentă română rezultă că transferul către o autoritate din țara terță, care este competentă în scopul îndeplinirii activităților prevăzute la art.1 alin.(1), este ineficient sau necorespunzător, în special din cauză că transferul nu poate fi realizat în timp util;
d) autoritatea din țara terță, care este competentă în scopul îndeplinirii activităților prevăzute la art.1 alin.(1), este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau necorespunzătoare;
e) autoritatea competentă română informează destinatarul cu privire la scopul sau scopurile determinate exclusive în care aceasta din urmă poate să prelucreze datele cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară.
(2) Transferul în condițiile alin.(1) este posibil numai dacă destinatarul se angajează în scris să nu prelucreze datele cu caracter în alt scop decât cel pentru care au fost transmise, circumscris îndeplinirii scopurilor prevăzute la art.(1) alin.(1).
(3) Dispozițiile alin.(1) nu afectează transferurile de date cu caracter personal stabilite prin tratate încheiate în domeniul cooperării judiciare în materie penală sau al cooperării polițienești internaționale.
(4) Autoritatea competentă română informează periodic, cel puțin o dată pe an, autoritatea de supraveghere cu privire la transferurile efectuate în temeiul prezentului articol.
(5) În situația transferurilor realizate în condițiile alin.(1), dispozițiile art.43 alin.(4) și (5) se aplică în mod corespunzător.

Art.48 Autoritățile competente dispun măsuri corespunzătoare pentru:
a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației privind protecția datelor cu caracter personal;
b) acordarea de asistență internațională reciprocă în asigurarea respectării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificări, transferul reclamațiilor, asistență în anchete și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;
c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop consolidarea cooperării internaționale în vederea asigurării respectării legislației din domeniul protecției datelor cu caracter personal;
d) promovarea schimburilor de legislație și practici în materie de protecție a datelor cu caracter personal și a documentării cu privire la acestea, inclusiv în ceea ce privește eventualele conflictele de jurisdicție cu țările terțe.

Art.49 (1) Pentru realizarea activităților de cercetare și combatere a infracțiunilor 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 interconectate.
(2) În scopul prevăzut la alin.(1), interconectarea 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.

(3) Interconectările prevăzute la alin. (1) şi (2) sunt posibile numai cu acordul prealabil al autorităţii de supraveghere.
(4) În scopul prevăzut la alin. (1), interconectarea sistemelor de evidenţă a datelor cu caracter personal sau a mijloacelor automate de prelucrare a datelor cu caracter personal se poate realiza şi cu sistemele de evidenţă sau cu mijloacele automate de prelucrare a datelor cu caracter personal deţinute de alţi operatori, entităţi de drept privat.
(5) Interconectările prevăzute la alin. (4) sunt permise numai în scopul efectuării urmăririi penale, în baza unei ordonanţe emise de procurorul competent să efectueze ori să supravegheze, într-un caz determinat, urmărirea penală ori, în cazul judecării unei infracţiuni, de judecătorul anume desemnat de la instanţa căreia îi revine competenţa de a judeca fondul cauzei pentru care sunt prelucrate datele cu caracter personal respective.
(6) Accesul direct sau printr-un serviciu de comunicaţii electronice la un sistem de evidenţă a datelor cu caracter personal care face obiectul interconectării, potrivit alin. (1), este permis numai în condiţiile legii şi cu respectarea prevederilor art. 1 alin. (1).

Art.50 (1) În cazul activităţilor de prevenire a infracţiunilor, de menţinere şi de asigurare a ordinii şi siguranţei publice, sistemele de evidenţă a datelor cu caracter personal sau mijloacele automate de prelucrare a datelor cu caracter personal pot fi interconectate cu:
a) Registrul naţional de evidenţă a persoanelor;
b) Registrul naţional de evidenţă a paşapoartelor simple;
c) Registrul naţional de evidenţă a permiselor de conducere şi a vehiculelor înmatriculate.
(2) În cazul activităţilor prevăzute la alin. (1), sistemele de evidenţă a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care le deţin operatorii, pentru scopuri similare ori corelate, pot fi interconectate.
(3) Interconectările prevăzute la alin.(1) şi (2) se aduc la cunoştinţa autorităţii de supraveghere.
(4) În cazul activităţilor prevăzute la alin.(1), se pot interconecta sistemele de evidenţă a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care le deţin pentru scopuri diferite, numai cu acordul prealabil al autorităţii de supraveghere.

Art.51 (1) Supravegherea prelucrărilor de date cu caracter personal efectuate în temeiul prezentei legi, în scopul protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii Europene, se realizează de către autoritatea de supraveghere.
(2) Autoritatea de supraveghere cooperează cu autorităţi similare din alte state membre, precum şi cu Comisia, în conformitate cu art.54.

Art. 52 (1) Autoritatea de supraveghere monitorizează şi controlează sub aspectul legalităţii prelucrările de date cu caracter personal care intră sub incidenţa prezentei legi.
(2) Prin excepţie de la alin.(1), autoritatea de supraveghere nu este competentă să supravegheze operaţiunile de prelucrare ale instanţelor atunci când acestea acţionează în exerciţiul funcţiei lor judiciare.
(3) În acest scop, autoritatea de supraveghere îndeplineşte sarcinile prevăzute la art. 57 alin. (1) lit. b), c) şi t) din Regulamentul (UE) 2016/ 679, precum şi următoarele:
a) promovează acţiuni de conştientizare în rândurile operatorilor şi ale persoanelor împuternicite de aceştia cu privire la obligaţiile care le revin în temeiul prezentei legi;

b) furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul prezentei legi 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 cu art.57, 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 și informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul alin.(3) al art.20 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 prezentei legi;
f) desfășoară investigații privind aplicarea prezentei legi, 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 articolele 33-34.

Art. 53 (1) În exercitarea competențelor de investigare, autoritatea 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.
(2) Autorității de supraveghere îi revin 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 prezentei legi;
b) de a dispune operatorului sau persoanei împuternicite de către operator să asigure conformitatea operațiunilor de prelucrare cu prevederile prezentei legi, specificând, după caz, modalitatea și termenul-limită pentru aceasta, în special dispunând rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării, în conformitate cu articolul 18;
c) de a dispune limitarea temporară sau definitivă ori interdicția prelucrărilor.
(3) Autoritatea de supraveghere oferă consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolele 33-34 și emite avize, din proprie inițiativă sau la cerere, Parlamentului, Guvernului sau altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal.

Art.54 (1) Autoritatea de supraveghere cooperează cu instituții similare din străinătate și asigură reprezentarea în cadrul Comitetului European pentru Protecția Datelor.
(2) Dispozițiile Legii nr.102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, referitoare la cooperarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal cu instituții similare din străinătate, sunt aplicabile în mod corespunzător.

Art.55 (1) În cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o vizează încalcă dispozițiile prezentei legi, are dreptul de a se adresa cu plângere autorității de supraveghere
(2) Dispozițiile Regulamentului General privind Protecția Datelor sunt aplicabile în mod corespunzător.

Art.56 Fără a se aduce atingere posibilității de a se adresa cu plângere autorității de supraveghere, persoanele vizate au dreptul de a se adresa instanței pentru apărarea oricăror drepturi garantate de prezenta lege, care le-au fost încălcate.

Art.57 În scopul apărării drepturilor sale, persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație, care nu are scop lucrativ, constituită în condițiile legii, ale cărei obiective statutare sunt de interes public și care este activă în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor cu caracter personal, să depună plângerea în numele său și să exercite în numele său drepturile prevăzute de prezenta lege.

Art.58 (1) Orice persoană care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni de prelucrare ilegale sau a oricărei acțiuni care încalcă dispozițiile prezentei legi are dreptul de a obține despăgubiri, în condițiile legii, pentru prejudiciul cauzat de operator sau de o altă autoritate competentă.
(2) Dacă, în situația prelucrărilor automate de date cu caracter personal, nu este posibilă determinarea operatorului de date cu caracter personal care a cauzat prejudiciul, fiecare dintre operatorii de date cu caracter personal implicați în operațiunea de prelucrare este considerat a fi responsabil.

Art.59 (1) Constituie contravenție încălcarea de către operator sau, după caz, de către persoana împuternicită de operator, a obligațiilor acestora în conformitate cu articolele 11 și 22-42 din prezenta lege.
(2) Constituie contravenție încălcarea de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor art. 10 din prezenta lege.
(3) Contravențiile prevăzute la alin. (1) și (2) se sancționează cu amendă de până la 100.000 lei.
(4) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a principiilor de bază pentru prelucrare, prevăzute la art.5.
(5) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a drepturilor persoanelor vizate în conformitate cu articolele 12 – 21.
(6) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor referitoare la transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44 – 49.
(7) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor emise de către autoritatea de supraveghere în temeiul art.53 alin.(2) sau neacordarea accesului autorității de supraveghere, prin încălcarea dispozițiilor art.53 alin.(1).
(8) Contravențiile prevăzute la alin. (4) –(7) se sancționează cu amendă de până la 200.000 lei.

Art.60 (1) În cazul constatării încălcării prevederilor prezentei legi de către operator sau, după caz, de către persoana împuternicită de operator, autoritatea de supraveghere încheie un proces-verbal de constatare și sancționare a contravenției prin care se aplică sancțiunea mustrării, conform art.58 alin.(2) lit. b) din Regulamentul general privind protecția datelor și la care anexează un plan de remediere.
(2) Termenul de remediere se stabilește în funcție de riscurile asociate prelucrării, precum și demersurile necesar a fi îndeplinite pentru asigurarea conformității prelucrării.
(3) În termen de 10 zile de la data expirării termenului de remediere, autoritatea de supraveghere poate să reia controlul.
(4) În cazul în care operatorul sau, după caz, persoana împuternicită de operator, constată că nu poate îndeplini în termenul stabilit, din motive întemeiate, o parte din măsurile dispuse prin planul de

remediere, notifică autoritatea de supraveghere cu privire la acest aspect cu cel puţin 10 zile înainte de expirarea termenului, putând solicita totodată prelungirea termenului iniţial.
(5) Autoritatea de supraveghere analizează solicitarea de prelungire a termenului şi comunică răspunsul operatorului sau, după caz, persoanei împuternicite de către operator, în termen de 7 zile de la primirea cererii.
(6) Dacă autoritatea de supraveghere consideră justificată cererea operatorului sau, după caz, a persoanei împuternicite de către operator, poate prelungi termenul de remediere cu până la 30 de zile. În caz contrar, se aplică prevederile de la alin.(3).
(7) Responsabilitatea îndeplinirii măsurilor de remediere revine operatorului sau, după caz, persoanei împuternicite de operator care, potrivit legii, poartă răspunderea contravenţională pentru faptele constatate.
(8) Modelul planului de remediere care se anexează la procesul-verbal de constatare şi sancţionare a contravenţiei este prevăzut în Anexa la prezenta lege.

Art.61 Dacă, la reluarea controlului, autoritatea de supraveghere constată faptul că operatorul nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere, aceasta, în funcţie de circumstanţele fiecărui caz în parte, poate aplica sancţiunea contravenţională a amenzii.

Art. 62 La data intrării în vigoare a prezentei legi, Legea nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, republicată în Monitorul Oficial al României, Partea I, nr. 474 din 12 iulie 2012 se abrogă.

Art. 63 Prevederile art.59 intră în vigoare la 30 de zile de la data publicării prezentei legi în Monitorul Oficial al României, Partea I.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 şi ale art. 76 alin. (1) din Constituţia României, republicată:

PREŞEDINTELE
CAMEREI DEPUTAŢILOR

Liviu Nicolae DRAGNEA

PREŞEDINTELE
SENATULUI

Călin-Constantin-Anton
POPESCU-TĂRICEANU

Anexa

Plan de remediere
ziua ..... luna ..... anul .....

Modul de îndeplinire a măsurilor de remediere

Nr.	**Fapta săvârșită**	**Măsuri de remediere**	**Termen de remediere**	**Mod de îndeplinire**

Alte mențiuni

.....
.....
.....
.....
.....
.....
.....

Agent constatator/
Persoană competentă,

.....
(numele, prenumele,
semnătura)

Contravenient

.....
(numele,prenumele,semnătura)

Ștampila

	Articol/ Paragraf/ Litera	DIRECTIVA (UE) 2016/680 A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării, urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului	CORESPONDENŢĂ TEXT	OBSERVAŢII
1.	Art. 1 Obiect şi obiective	*CAPITOLUL I Dispoziţii generale* *Articolul 1* Obiect şi obiective (1) Prezenta directivă stabileşte normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor, inclusiv al protejării împotriva ameninţărilor la adresa securităţii publice şi al prevenirii acestora.	Art.1 (1) Prezenta lege reglementează prelucrarea datelor cu caracter personal în scopul realizării activităţilor de prevenire, descoperire, cercetare, urmărire penală şi combatere a infracţiunilor, de executare a pedepselor, precum şi de menţinere şi asigurare a ordinii şi siguranţei publice de către autorităţile competente, în limitele competenţelor stabilite prin lege. (2) Prelucrarea datelor cu caracter personal pentru realizarea activităţilor prevăzute la alin. (1) se realizează numai dacă această măsură este prevăzută de lege şi este necesară pentru prevenirea unui pericol cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea infracţiunilor.	
2.		(2) În conformitate cu prezenta directivă, statele membre: (a) protejează drepturile şi libertăţile fundamentale ale persoanelor fizice, în special dreptul acestora la protecţia datelor cu caracter personal; şi	Art.2 (1) Prezenta lege are ca scop protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la protecţia datelor cu caracter personal.	

3.		(b) se asigură că schimbul de date cu caracter personal de către autoritățile competente în cadrul Uniunii, în cazul în care schimbul respectiv de informații este impus de dreptul Uniunii sau de dreptul intern, nu este limitat sau interzis din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.	(2) Prezenta lege stabilește condițiile în care se realizează libera circulație a datelor cu caracter personal în scopul realizării activităților prevăzute la art.1 alin.(1). (3) Libera circulație a datelor cu caracter personal pe teritoriul național sau în relația cu statele membre ale Uniunii Europene, circumscrisă realizării activităților prevăzute la art. 1 alin.(1), nu poate fi împiedicată din motive legate de protecția persoanei față de prelucrările de date cu caracter personal atât timp cât condițiile din prezenta lege sau, după caz, din Regulamentul UE 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, denumit în continuare Regulamentul general de protecție a datelor, ori din legislația națională de punere în aplicare a acestuia sunt îndeplinite.	
4.		(3) Prezenta directivă nu împiedică statele membre să prevadă garanții sporite față de cele stabilite în prezenta directivă pentru protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente.		Nu necesită transpunere deoarece prezenta lege prevede garanții sporite; a se vedea, în acest sens, art. 14, 15, 24 etc.
5.	**Art. 2**	**Domeniul de aplicare**	Art.3 (1) Prezenta lege se aplică prelucrării datelor cu caracter personal de către autoritățile competente în	

	Domeniul de aplicare	(1) Prezenta directivă se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1).	scopurile prevăzute la art.1.	
6.		(2) Prezenta directivă 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 urmează să facă parte dintr-un sistem de evidență a datelor.	(2) Prezenta lege 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.	
7.		(3) Prezenta directivă nu se aplică prelucrării datelor cu caracter personal: a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;	(3) Prezenta lege 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 de lege.	
8.		(b) de către instituțiile, organele, oficiile și agențiile Uniunii		Nu necesită transpunere. Norma se adresează organismelor și instituțiilor UE.
9.	*Articolul 3* **Definiții**	În sensul prezentei directive: „date cu caracter personal" înseamnă orice informații privind 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 mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.	Art.4 În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: a) date cu caracter personal - orice informații privind o persoană fizică identificată sau identificabilă, denumită în continuare persoană 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 mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;	

10.		„prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;	b) prelucrare - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;	
11.		„restricţionarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;	c) restricţionarea prelucrării - marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;	
12.		„creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, localizarea sau deplasările respectivei persoane fizice;	d) creare de profiluri - orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a preconiza aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, corectitudinea, comportamentul, localizarea sau deplasările respectivei persoane fizice;	
13.		„pseudonimizare" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, în măsura în care aceste informaţii suplimentare sunt stocate separat şi fac obiectul unor măsuri de natură tehnică şi organizatorică destinate să garanteze neatribuirea unei persoane fizice identificate sau identificabile;	e) pseudonimizare - prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, în măsura în care aceste informaţii suplimentare sunt stocate separat şi fac obiectul unor măsuri de natură tehnică şi organizatorică destinate să garanteze neatribuirea unei persoane fizice identificate sau identificabile;	
14.		„sistem de evidenţă a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice	f) sistem de evidenţă a datelor - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;	

15.		„autoritate competentă" înseamnă: a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracţiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva ameninţărilor la adresa securităţii publice şi de prevenire a acestora; sau (b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică şi competenţe publice în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor, inclusiv al protejării împotriva ameninţărilor la adresa securităţii publice şi al prevenirii acestora;	g) autoritate competentă - orice autoritate publică sau orice alt organism sau entitate investită cu exerciţiul autorităţii de stat, competentă în materie de prevenire, descoperire, cercetare, urmărire penală şi combatere a infracţiunilor sau de executare a pedepselor, inclusiv în materia menţinerii şi asigurării ordinii şi siguranţei publice;	
16.		„operator" înseamnă autoritatea competentă care, singură sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele de prelucrare sunt stabilite prin dreptul Uniunii sau prin dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul Uniunii sau prin dreptul intern;	h) operator - autoritatea competentă care, singură sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele de prelucrare sunt stabilite printr-un act normativ, operatorul sau criteriile specifice pentru determinarea acestuia se stabilesc prin actul normativ de referinţă;	
17.		„persoană împuternicită de către operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;	i) persoană împuternicită de către operator - persoana fizică sau juridică, instituţia/autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;	
18.		„destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau un alt organism căruia îi sunt transmise datele cu caracter personal, fie că aceasta este sau nu o parte terţă; sunt exceptate, cu toate acestea,	j) destinatar - persoana fizică sau juridică, instituţia/autoritatea publică, agenţia sau un alt organism căruia îi sunt transmise datele cu caracter personal, fie că aceasta este sau nu o parte terţă; sunt	

		autoritățile publice care pot primi date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul intern, iar prelucrarea datelor cu caracter personal respective de către acestea respectă normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării;		exceptate din înțelesul definiției autoritățile competente care pot primi date cu caracter personal în cadrul unei anchete, în conformitate cu legislația aplicabilă, iar prelucrarea datelor cu caracter personal respective de către acestea respectă normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării;	
19.		„încălcarea securității datelor cu caracter personal" înseamnă o încălcare a securității, care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod;	k)	încălcarea securității datelor cu caracter personal - orice eveniment, acțiune sau inacțiune ce poate provoca o încălcare a securității, care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod;	
20.		„date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la acea persoană fizică;	i)	date genetice - datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la acea persoană fizică;	
21.		„date biometrice" înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;	m)	date biometrice - date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;	
22.		„date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;	n)	date privind sănătatea - date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;	
23.		„autoritate de supraveghere" înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 41	o)	autoritate de supraveghere - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;	

24.		„organizaţie internaţională" înseamnă o organizaţie şi organismele sale subordonate reglementate de dreptul internaţional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe ţări sau în temeiul unui astfel de acord.	p) organizaţie internaţională - o organizaţie şi organismele sale subordonate reglementate de dreptul internaţional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe state sau în temeiul unui astfel de acord;	
			q) interconectare - operaţiunea de a pune în legătură datele cu caracter personal cuprinse într-un fişier, bază de date sau sistem de evidenţă automat cu cele cuprinse într-unul sau mai multe fişiere, baze de date sau sisteme de evidenţă automate care sunt gestionate de operatori diferiţi sau de către acelaşi operator, dar având scopuri diferite, similare sau corelate, după caz;	
			r) evidenţă pasivă - fişier sau bază de date cu caracter personal constituit în scopul accesării limitate şi ulterior ştergerii datelor stocate din sistemul de evidenţă;	
			s) stat membru - orice stat membru al Uniunii Europene.	
			ş) plan de remediere – anexă la procesul-verbal de constatare şi sancţionare a contravenţiei întocmit în condiţiile prevăzute la art.59, prin care Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, stabileşte măsuri şi un termen de remediere;	
			t) măsură de remediere – soluţie dispusă de ANSPDCP în planul de remediere în vederea îndeplinirii de către operator sau de către persoana împuternicită de acesta, a obligaţiilor prevăzute de lege;	
			ţ) termen de remediere – perioada de timp cuprinsă între 60 şi 180 de zile de la data comunicării procesului-verbal de constatare şi sancţionare a contravenţiei, în care operatorul sau persoana împuternicită de acesta are posibilitatea remedierii neregulilor constatate şi	

			îndeplinirii obligațiilor legale.	
25.		Statele membre garantează că datele cu caracter personal: (a) **sunt** prelucrate în mod legal și echitabil;	Art.5 (1) Datele cu caracter personal trebuie să fie: a) prelucrate în mod legal și echitabil;	
26.		b) sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate într-un mod incompatibil cu aceste scopuri;	b) colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate într-un mod incompatibil cu aceste scopuri;	
27.	*Articolul 4* **Principii referitoare la prelucrarea datelor cu caracter personal**	c) sunt adecvate, relevante și neexcesive în ceea ce privește scopurile în care sunt prelucrate;	c) adecvate, relevante și neexcesive prin raportare la scopurile în care sunt prelucrate;	
28.		d) sunt exacte și, dacă este necesar, sunt actualizate; trebuie să se ia toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, să fie șterse sau rectificate fără întârziere;	d) exacte și, dacă este necesar, actualizate; trebuie adoptate toate măsurile rezonabile pentru a asigura faptul că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, să fie șterse sau rectificate fără întârziere;	
29.		e) sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;	e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;	
30.		f)sunt prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.	f) prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.	
31.		(2) Prelucrarea de către același operator sau de către un altul, în oricare dintre scopurile stabilite la articolul 1 alineatul (1), altele decât cele pentru care datele cu	(2) Datele cu caracter personal pot fi prelucrate pentru realizarea activităților prevăzute la art.1 de către același operator sau de către alt operator într-un alt scop decât cel avut în vedere la momentul colectării datelor cu	

		caracter personal au fost colectate, este permisă în măsura în care: a) operatorul este autorizat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu dreptul Uniunii sau cu dreptul intern; şi	caracter personal, numai dacă sunt îndeplinite cumulativ următoarele condiţii: a) operatorul este abilitat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu cadrul normativ aplicabil;	
32.		b) prelucrarea este necesară şi proporţională în raport cu respectivul alt scop, în conformitate cu dreptul Uniunii sau cu dreptul intern.	b) prelucrarea este necesară şi proporţională în raport cu scopul respectiv, în conformitate cu cadrul normativ aplicabil.	
33.		(3) Prelucrarea de către acelaşi operator sau de către un altul poate include arhivarea în interes public sau în scopuri ştiinţifice, statistice sau istorice pentru scopurile stabilite la articolul 1 alineatul (1), cu condiţia unor garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate.	(3) Datele cu caracter personal pot fi prelucrate de către acelaşi operator sau de către alt operator în scopul arhivării în interes public sau în scopuri ştiinţifice, statistice sau istorice legate de realizarea activităţilor prevăzute la art.1 alin.(1), cu condiţia instituirii unor garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate.	
34.		(4) Operatorul este responsabil de respectarea alineatelor (1), (2) şi (3) şi poate demonstra acest lucru.	(4) Operatorul este responsabil pentru respectarea prevederilor alin.(1) – (3) şi trebuie să instituie proceduri pentru a putea demonstra respectarea acestor prevederi.	
35.	*Articolul 5* **Termene pentru stocare şi revizuire**	Statele membre garantează stabilirea unor termene corespunzătoare pentru ştergerea datelor cu caracter personal sau pentru o revizuire periodică a necesităţii de stocare a datelor cu caracter personal. Respectarea acestor termene este asigurată prin măsuri procedurale	Art.6 (1) Actele normative, indiferent de nivelul de legiferare, care instituie prelucrări de date cu caracter personal în scopul realizării activităţilor prevăzute la art.1 alin.(1), trebuie să stabilească cel puţin următoarele aspecte: a) contextul general al prelucrării şi obiectivele acesteia; b) datele cu caracter personal care urmează să fie prelucrate; c) scopurile prelucrării; d) termenele de stocare generale şi, după caz, specifice, a datelor cu caracter personal. (2) La împlinirea termenelor de stocare, datele cu caracter personal pot fi:	

			a) arhivate în interes public în conformitate cu legislaţia specială; b) stocate în evidenţa pasivă pentru o durată care nu poate depăşi jumătate din termenul iniţial de stocare; c) distruse sau şterse prin utilizarea unor proceduri ireversibile, dacă nu se încadrează în una dintre situaţiile prevăzute la lit. a) sau b). (3) Stabilirea termenelor specifice de păstrare este obligatorie în următoarele situaţii: a) prelucrarea datelor cu caracter personal referitoare la minori; b) prelucrarea categoriilor speciale de date cu caracter personal; c) prelucrarea datelor cu caracter personal a căror acurateţe nu a fost stabilită sau nu a putut fi stabilită; d) în orice altă situaţie în care prelucrarea presupune riscuri majore pentru persoana vizată. (4) Termenele specifice de stocare nu pot fi mai mari decât jumătate din termenul general de stocare corespunzător. (5) Prelucrările de date cu caracter personal bazate pe utilizarea noilor tehnologii sau care sunt de natură să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice pot fi instituite în scopul realizării activităţilor prevăzute la art. 1 alin. (1) numai în temeiul unui act normativ publicat în Monitorul Oficial care să stabilească garanţii necesar a fi instituite în temeiul prezentei legi.	
36.	*Articolu l 6* **Distinc ţ ia între**	Statele membre garantează că, după caz şi în măsura posibilului, operatorul face distincţie clară între datele cu caracter personal ale diferitelor categorii de persoane vizate, precum: a) persoane în privinţa cărora există motive serioase să	Art.7 (1) Operatorii dispun măsurile necesare în scopul structurării datelor cu caracter personal având în vedere următoarele criterii: a) date referitoare la persoane în privinţa cărora există indicii temeinice că au săvârşit sau că urmează să săvârşească o infracţiune;	

	diferitele categorii de persoane vizate	se creadă că au săvârşit sau că urmează să săvârşească o infracţiune;		
37.		b) persoane condamnate pentru săvârşirea unei infracţiuni;	b) date referitoare la persoane condamnate pentru săvârşirea unei infracţiuni;	
38.		c) victime ale unei infracţiuni sau persoane în privinţa cărora, în baza anumitor fapte, există motive să se creadă că persoanele respective ar putea fi victimele unei infracţiuni; şi	c) date referitoare la persoane victime ale unei infracţiuni sau persoane în privinţa cărora există motive să se creadă că ar putea fi victimele unei infracţiuni;	
39.		d) alte părţi care au legătură cu infracţiunea, ca de exemplu persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracţiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informaţii cu privire la infracţiuni sau persoane care sunt în legătură sau asociate cu persoanele menţionate la literele (a) şi (b).	d) date referitoare la alte persoane care au legătură cu infracţiunea, precum persoane care ar putea fi chemate să depună mărturie în cadrul anchetelor legate de infracţiuni sau în cadrul procedurilor penale ulterioare sau persoane care pot oferi informaţii cu privire la infracţiuni sau persoane care sunt în legătură sau asociate cu persoanele prevăzute la lit. a) sau b).	
40.	*Articolul 7* **Distincţia între datele cu caracter personal şi verificarea**	(1) Statele membre garantează că se face distincţie, pe cât posibil, între datele cu caracter personal bazate pe fapte şi datele cu caracter personal bazate pe evaluări personale.	(2) Datele cu caracter personal prelucrate în temeiul prezentei legi sunt ordonate în funcţie de gradul lor de acurateţe şi exactitate. În acest scop, operatorii dispun măsurile necesare pentru realizarea unei distincţii între date colectate ca urmare a constatării unor fapte, respectiv date a căror colectare se bazează pe percepţia subiectivă a unor persoane fizice.	
41.		(2) Statele membre garantează că autorităţile competente iau toate măsurile rezonabile pentru a se	(3) Operatorii dispun toate măsurile necesare pentru ca datele cu caracter personal inexacte, incomplete sau care nu sunt actualizate să nu fie transmise sau puse la	

	rea calității datelor cu caracter personal	asigura că datele cu caracter personal care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziție. În acest scop, fiecare autoritate competentă verifică, în măsura în care este posibil, calitatea datelor cu caracter personal înainte ca acestea să fie transmise sau puse la dispoziție. În măsura în care acest lucru este posibil, în cadrul tuturor transmiterilor de date cu caracter personal, se adaugă informații necesare care permit autorității competente destinatare să evalueze gradul de exactitate, caracterul integral, gradul de fiabilitate și de actualitate al datelor cu caracter personal.	dispoziție. (4) Măsurile prevăzute la alin.(3) includ și evaluări periodice în scopul asigurării calității datelor cu caracter personal prin raportare la scopul în care au fost colectate și sunt ulterior prelucrate. (5) Termenele de evaluare sunt stabilite prin acte administrative adoptate de către operatori, cărora li se asigură o formă de publicitate. Frecvența evaluărilor este determinată de scopul în care datele cu caracter personal au fost colectate, calitatea datelor la momentul colectării, cantitatea datelor, dacă sunt prelucrate categorii speciale de date cu caracter personal. Termenele de evaluare nu pot depăși doi ani de la momentul colectării, respectiv de la precedenta evaluare. (6) Evaluarea calității datelor cu caracter personal este obligatorie înainte ca datele cu caracter personal să fie transmise sau puse la dispoziție altui operator. (7) În situația transmiterii de date cu caracter personal, în scopul asigurării calității datelor, operatorul poate adăuga informații care să permită autorității competente destinatare să evalueze: a) acuratețea datelor; b) caracterul integral al datelor; c) utilitatea datelor raportat la scopul prelucrării; d) dacă acestea sunt actualizate.	
42.		(3) În cazul în care se constată transmiterea unor date cu caracter personal incorecte sau transmiterea unor date cu caracter personal în mod ilegal, acest lucru se comunică de îndată destinatarului. Într-un astfel de caz, datele cu caracter personal sunt rectificate sau șterse sau	(8) În situația unei transmiteri neconforme cu legislația în vigoare a unor date cu caracter personal sau în cazul în care se constată că datele cu caracter personal nu au calitatea necesară, operatorul este obligat să notifice de îndată destinatarul. Datele care au făcut obiectul transmiterii sunt, după caz: a) rectificate sau șterse;	

		prelucrarea este restricționată în conformitate cu articolul 16.	b) restricționate la prelucrare. (9) Restricționarea prelucrării datelor cu caracter personal prevăzută la alin.(8) se dispune doar în una dintre situațiile prevăzute la art. 18 alin. (4).	
43.	*Articolul 18* **Legalitatea prelucrării**	(1) Statele membre garantează legalitatea prelucrării numai dacă și în măsura în care aceasta este necesară pentru îndeplinirea unei sarcini de către o autoritate competentă în scopurile stabilite la articolul 1 alineatul (1) și că aceasta se întemeiază pe dreptul Uniunii sau pe dreptul intern.	Art. 1 (2) Prelucrarea datelor cu caracter personal pentru realizarea activităților prevăzute la alin. (1) se realizează numai dacă această măsură este prevăzută de lege și este necesară pentru prevenirea unui pericol iminent cel puțin asupra vieții, integrității corporale sau sănătății unei persoane ori a proprietății acesteia, precum și pentru combaterea unei anumite infracțiuni.	
44.		(2) Dreptul intern care reglementează prelucrarea care intră sub incidența prezentei directive precizează cel puțin obiectivele prelucrării, datele cu caracter personal care urmează să fie prelucrate și scopurile prelucrării.	Art.6 (1) Actele normative, indiferent de nivelul de legiferare, care instituie prelucrări de date cu caracter personal în scopul realizării activităților prevăzute la art.1 alin.(1) trebuie să stabilească cel puțin următoarele aspecte: a) contextul general al prelucrării și obiectivele acesteia; b) datele cu caracter personal care urmează să fie prelucrate; c) scopurile prelucrării; d) termenele de stocare, generale și, după caz, specifice, a datelor cu caracter personal.	
45.	*Articolul 9* **Condiții specifice de**	(1) Datele cu caracter personal colectate de autoritățile competente în scopurile stabilite la articolul 1 alineatul (1) nu se prelucrează în alte scopuri decât cele stabilite la articolul 1 alineatul (1), cu excepția cazurilor în care o astfel de prelucrare este autorizată în temeiul dreptului Uniunii sau al dreptului intern. În cazurile în care datele cu caracter personal sunt prelucrate în alte scopuri,	Art. 8 (1) Datele cu caracter personal colectate în scopul prevăzut la art.1 alin.(1) nu pot fi prelucrate în alte scopuri, cu excepția cazurilor prevăzute în mod expres de lege. (2) În situațiile excepționale prevăzute la alin.(1), prelucrările suplimentare de date cu caracter personal se realizează în conformitate cu dispozițiile Regulamentului General de Protecție a Datelor, cu excepția activităților prevăzute la art.3 alin.(2), situație	

	prelucr are	prelucrării respective i se aplică Regulamentul (UE) 2016/679, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.	în care se aplică dispozițiile corespunzătoare cuprinse în legi speciale.	
46.		(2) În cazul în care autoritățile competente sunt împuternicite prin dreptul intern să îndeplinească alte atribuții decât cele aferente scopurilor stabilite la articolul 1 alineatul (1), pentru prelucrarea în astfel de scopuri se aplică Regulamentul (UE) 2016/679, inclusiv în ce privește prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu excepția cazului în care prelucrarea este efectuată în cadrul unei activități care nu intră sub incidența dreptului Uniunii.	(3) Datele cu caracter personal colectate de către autoritățile competente în alte scopuri decât cele necesare îndeplinirii activităților prevăzute la art.1 alin.(1) sunt prelucrate în conformitate cu dispozițiile Regulamentului General de Protecție a Datelor, cu excepția activităților prevăzute la art.3 alin.(2), situație în care se aplică dispozițiile corespunzătoare cuprinse în legi speciale. (4) Dispozițiile alin.(3) se aplică inclusiv pentru prelucrarea datelor cu caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.	
47.		(3) Statele membre garantează că, în cazul în care dreptul Uniunii sau dreptul intern aplicabil autorității competente care a transmis datele prevede condiții specifice de prelucrare, autoritatea competentă care a transmis datele informează destinatarul respectivelor date cu caracter personal cu privire la aceste condiții și la obligația de a le respecta.	Art.9 (1) În situația prelucrării datelor cu caracter personal sub forma transferului către terți, autoritatea competentă care transferă datele cu caracter personal are obligația de a informa destinatarul datelor cu caracter personal cu privire la condițiile specifice de prelucrare și obligația de a le respecta, în măsura în care astfel de condiții sunt impuse de lege. (2) Destinatarul datelor cu caracter personal are obligația respectării condițiilor specifice de prelucrare comunicate în conformitate cu alin.(1).	
48.		(4) Statele membre garantează că autoritatea competentă care a transmis datele nu aplică condițiile prevăzute la alineatul (3) destinatarilor din alte state membre sau agențiilor, oficiilor și organismelor instituite în conformitate cu titlul V capitolele 4 și 5 din	(3) În situația transferului de date cu caracter personal către destinatari din state membre ale Uniunii Europene sau către agenții, oficii și organisme instituite în conformitate cu Titlul V Capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene, nu pot fi impuse condiții specifice de prelucrare, în conformitate cu	

		TFUE, altele decât cele aplicabile transmiterii similare de date în statul membru al autorității competente care a transmis datele.	alin.(1), suplimentare față de cele prevăzute de lege pentru transferul către autorități competente din România.	
49.	*Articolul 10* **Prelucrarea de categorii speciale de date cu caracter personal**	Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice este autorizată numai atunci când este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate și numai atunci când: a) este autorizată de dreptul Uniunii sau de dreptul intern;	Art.10 Prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice, prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice se poate realiza dacă este strict necesară într-un caz determinat, dacă sunt instituite garanții adecvate pentru drepturile și libertățile persoanei vizate și dacă este îndeplinită una dintre următoarele condiții: a) prelucrarea este prevăzută expres de lege;	
50.		b) este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice; sau	b) prelucrarea este necesară pentru prevenirea unui pericol iminent cel puțin asupra vieții, integrității corporale sau sănătății persoanei vizate sau ale unei alte persoane fizice;	
51.		c) prelucrarea respectivă se referă la date care sunt făcute publice în mod manifest de persoana vizată.	c) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de persoana vizată.	
52.	*Articolul*	(1) Statele membre garantează că o decizie întemeiată exclusiv pe prelucrarea automată, inclusiv crearea de	Art.11 (1) Adoptarea unei decizii întemeiate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru persoana vizată	

	III **Procesul decizional individual automatizat**	profiluri, care produce un efect juridic negativ pentru persoana vizată sau care o afectează în mod semnificativ, este interzisă, cu excepţia cazului în care este autorizată de dreptul Uniunii sau de dreptul intern care se aplică operatorului şi care prevede garanţii adecvate pentru drepturile şi libertăţile persoanei vizate, cel puţin dreptul de a obţine intervenţia umană din partea operatorului.	sau care o afectează în mod semnificativ este interzisă, cu excepţia cazului în care prelucrarea este reglementată expres de lege, fiind prevăzute garanţii adecvate pentru drepturile şi libertăţile persoanei vizate, inclusiv dreptul de a obţine intervenţia umană din partea operatorului.	
53.		2) Deciziile menţionate la alineatul (1) din prezentul articol nu se întemeiază pe categoriile speciale de date cu caracter personal menţionate la articolul 10, cu excepţia cazului în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, a libertăţilor şi a intereselor legitime ale persoanei vizate.	(2) Prelucrarea categoriilor de date cu caracter personal prevăzute la art. 10 în scopul adoptării de decizii în condiţiile alin.(1) este interzisă, cu excepţia situaţiei în care sunt instituite măsuri corespunzătoare pentru protejarea drepturilor, a libertăţilor şi a intereselor legitime ale persoanei vizate.	
54.		(3) În conformitate cu dreptul Uniunii, este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice pe baza categoriilor speciale de date cu caracter personal menţionate la articolul 10.	(3) Crearea de profiluri care au drept rezultat discriminarea persoanelor fizice pe baza criteriilor ce determină categoriile de date prevăzute la art.10 este interzisă.	
55.	***CAPITOLUL III Drepturile persoanei vizate***	(1) Statele membre garantează faptul că operatorul ia măsuri rezonabile pentru a transmite persoanei vizate orice informaţii menţionate la articolul 13 şi transmite acesteia orice comunicare în legătură cu articolele 11, 14-18 şi 31 referitoare la prelucrare, într-o formă concisă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Informaţiile se transmit prin orice mijloace adecvate, inclusiv prin mijloace electronice. Ca	Art.12 (1) Operatorii sunt obligaţi să instituie măsurile organizatorice, tehnice şi de procedură pentru a furniza persoanei vizate informaţiile necesare potrivit art.13, art.16-21 şi pentru a asigura transmiterea unui răspuns în legătură cu prelucrările desfăşurate în condiţiile art.11 sau în legătură cu notificarea persoanelor vizate în cazul apariţiei unui incident de securitate, în condiţiile art.39. (2) Răspunsul trebuie formulat într-o formă concisă,	

	Articolul 12 **Comunicare şi modalităţi de exercitare a drepturilor persoanei vizate**	regulă generală, operatorul transmite informaţiile în acelaşi format în care a fost primită cererea.	inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. (3) Comunicarea informaţiilor în condiţiile alin.(2) se realizează în acelaşi format în care cererea a fost formulată, cu următoarele excepţii: a) identitatea solicitantului nu poate fi stabilită cu exactitate; 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.	
56.		(2) Statele membre garantează faptul că operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 11 şi 14-18.	(4) Operatorul este obligat să instituie măsuri organizatorice şi de procedură în scopul facilitării exercitării drepturilor persoanei vizate în temeiul art.11 şi art.16 – 21.	
57.		3) Statele membre garantează faptul că operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate.	(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.	
58.		(4) Statele membre garantează faptul că transmiterea informaţiilor în conformitate cu articolul 13 şi orice comunicare transmisă şi măsură luată în temeiul articolelor 11, 14-18 şi 31 este gratuită. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit	(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 ţină cont de costurile administrative pentru transmiterea sau comunicarea informaţiilor sau pentru luarea măsurilor	

		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 informațiilor sau a comunicărilor sau pentru luarea măsurilor solicitate; sau (b) poate refuza să dea curs cererii.	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 stabilește de la caz la caz, în funcție de următoarele criterii: a) obiectul cererii; b) intervalul de timp scurs de la formularea cererii precedente; c) existența unor prelucrări suplimentare de date cu caracter personal, prin raportare la cele desfășurate la momentul formulării cererii precente.	
59.		Operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.	(8) Caracterul nefondat sau excesiv al cererii, în condițiile alin.(6), trebuie demonstrat de operator.	
60.		(5) În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la articolul 14 sau 16, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.	(9) În cazul în care identitatea persoanei care formulează o cerere în temeiul art.16 sau art.18 nu a putut fi stabilită cu exactitate, operatorul îi solicită acestuia informații suplimentare necesare pentru confirmarea identității. (10) Informațiile suplimentare colectate potrivit alin.(9) nu pot fi prelucrate în niciun alt scop decât pentru confirmarea identității și se distrug în termen de 3 ani de la colectare. Operatorul poate stabili termene de păstrare mai mici.	
61.	*Articolul 13* **Informații care**	(1) Statele membre garantează că operatorul pune la dispoziția persoanelor vizate cel puțin următoarele informații: (a) identitatea și datele de contact ale operatorului;	Art.13 Operatorii sunt obligați să instituie măsuri organizatorice, tehnice și de procedură în scopul punerii la dispoziția persoanelor interesate persoanei vizate, a următoarelor categorii de informații: a) identitatea și datele de contact ale operatorului;	

	se pun la dispoziț ia persoan ei vizate sau se comuni că acesteia		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 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.	
62.	(b)	datele de contact ale responsabilului cu protecția datelor, după caz;		
63.	(c)	scopurile în care sunt prelucrate datele cu caracter personal;		
64.	(d)	dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;		
65.	(e)	existența dreptului de a solicita operatorului acces la datele cu caracter personal referitoare la persoana vizată ori rectificarea sau ștergerea acestor date sau restricționarea prelucrării lor.		
66.		(2) În plus față de informațiile menționate la alineatul (1), statele membre garantează prin lege că operatorul comunică persoanei vizate, în anumite cazuri, următoarele informații suplimentare, pentru a permite acesteia exercitarea drepturilor sale:	Art.14 La cerere, operatorul comunică persoanei vizate informațiile prevăzute la art.13, precum și următoarele informații suplimentare: a) temeiul juridic al prelucrării;	

		(a) temeiul juridic al prelucrării;		
67.		(b) perioada pentru care vor fi stocate datele cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili respectiva perioadă;	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;	
68.		(c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv în țări terțe sau organizații internaționale;	c) dacă este cazul, categoriile de destinatari ai datelor cu caracter personal, inclusiv din state terțe sau organizații internaționale;	
69.		(d) în cazul în care este necesar, informații suplimentare, în special atunci când datele cu caracter personal sunt colectate fără știrea persoanei vizate.	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.	
70.		(3) Statele membre pot adopta măsuri legislative de amânare, restricționare sau omitere a furnizării de informații persoanei vizate în conformitate cu alineatul (2) în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama de drepturile fundamentale și de interesele legitime ale persoanei fizice, pentru: (a) evitarea obstrucționării cercetărilor, anchetelor sau a procedurilor oficiale sau juridice;	Art.15 (1) Operatorul poate dispune, după caz, măsura amânării, restricționării sau omiterii furnizării de informații persoanei vizate în condițiile art.14 numai dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru: a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;	
71.		(b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;	b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau a executării pedepselor;	
72.		(c) protejarea securității publice;	c) protejarea ordinii și siguranței publice;	
73.		(d) protejarea securității naționale;	d) protejarea securității naționale;	

74.		(c) protejarea drepturilor şi libertăţilor celorlalţi.	c) protejarea drepturilor şi libertăţilor celorlaţi.	
75.		(4) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care pot intra, integral sau parţial, sub incidenţa oricăreia dintre literele de la alineatul (3).	(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).	
76.	*Articolul 14* **Dreptul de acces al persoanei vizate**	Sub rezerva articolului 15, statele membre garantează dreptul persoanei vizate de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii: (a) scopurile şi temeiul juridic al prelucrării;	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 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;	
77.	(b)	categoriile de date cu caracter personal vizate;	b) categoriile de date cu caracter personal vizate;	
78.	(c)	destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele cu caracter personal, în special destinatarii din ţări terţe sau organizaţii internaţionale;	c) destinatarii sau categoriile de destinatari cărora le-au fost divulgate datele cu caracter personal, în special destinatarii din state terţe sau organizaţii internaţionale;	
79.	(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;	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;	
80.	(e)	existenţa dreptului de a solicita de la operator rectificarea sau ştergerea datelor cu caracter personal,	e) dreptul de a solicita de la operator rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării datelor cu caracter	

		sau restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată;	personal referitoare la persoana vizată;	
81.	(f)	dreptul de a depune o plângere în fața autorității de supraveghere și datele de contact ale autorității de supraveghere;	f) dreptul de a depune o plângere la autoritatea de supraveghere și datele de contact ale acesteia;	
82.	(g)	comunicarea datelor cu caracter personal care sunt în curs de prelucrare și a oricărei informații disponibile cu privire la originea datelor.	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.	
83.	*Articolu l 15* **Limitarea dreptului de acces**	(1) Statele membre pot adopta măsuri legislative care limitează, integral sau parțial, dreptul de acces al persoanei vizate în măsura și atât timp o astfel de limitare, parțială sau totală, constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama de drepturile fundamentale și de interesele legitime ale respectivei persoane fizice, pentru:	Art.17 (1) Dispozițiile art.16 nu se aplică dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:	
84.		(a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;	a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;	
85.	(b)	a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;	b) evitarea prejudicierii prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau a executării pedepselor;	
86.	(c)	protejarea securității publice;	c) protejarea ordinii și siguranței publice;	
87.	(d)	protejarea securității naționale;	d) protejarea securității naționale;	
88.	(e)	protejarea drepturilor și libertăților celorlalți.	e) protejarea drepturilor și libertăților celorlalți.	

89.		(2) Statele membre pot adopta măsuri legislative pentru a stabili categoriile de prelucrare care se pot încadra, integral sau parțial, sub incidența literelor (a)-(e) de la alineatul (1).		Nu este cazul
90.		(3) În cazurile prevăzute la alineatele (1) și (2), statele membre garantează că operatorul informează în scris persoana vizată, fără întârzieri nejustificate, cu privire la refuzarea sau limitarea accesului și la motivele refuzului sau ale limitării. Astfel de informații pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile de la alineatul (1). Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.	(2) Măsura limitării dreptului de acces poate să fie totală sau parțială și se dispune cu privire la una sau mai multe operațiuni de prelucrare în situația cărora dezvăluirea este de natură să afecteze una dintre activitățile prevăzute la alin.(1). (3) În situația prevăzută la alin.(2) persoana vizată poate fi informată cu privire la categoriile de prelucrări care nu sunt de natură a afecta activitățile prevăzute la alin.(1), motivul adoptării acestei măsuri, precum și cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a se adresa instanței. (4) Prin excepție de la dispozițiile alin.(3), motivul adoptării măsurii de limitare a dreptului de acces nu se comunică în situația în care dezvăluirea acestuia este de natură să afecteze una dintre activitățile prevăzute la alin.(1) lit.a)-d).	
91.		4) Statele membre garantează că operatorul justifică motivele de fapt și de drept pe care se întemeiază decizia. Aceste informații se pun la dispoziția autorităților de supraveghere.	(5) Operatorul este obligat să țină evidența cazurilor în care a fost dispusă măsura de limitare a dreptului de acces și să documenteze adoptarea acestei măsuri. (6) În luna ianuarie a fiecărui an, operatorul are obligația de a informa autoritatea de supraveghere cu privire la situația statistică a cazurilor în care a fost adoptată măsura de limitare a dreptului de acces în anul precedent, defalcat pentru fiecare dintre activitățile prevăzute la alin.(1).	
92.	Articolul 16 Dreptul	1) Statele membre garantează persoanei vizate dreptul de a obține de la operator, fără întârzieri nejustificate,	Art.18 (1) 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.	

	la rectificarea sau la ştergerea datelor cu caracter personal şi la restricţionarea prelucrării	rectificarea datelor cu caracter personal inexacte care o privesc. Ţinându-se seama de scopurile prelucrării, statele membre garantează persoanei vizate dreptul de a obţine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.	(2) Persoana vizată are dreptul de a solicita completarea datelor cu caracter personal care o privesc inclusiv prin furnizarea unei declaraţii suplimentare.	
93.		2) Statele membre impun operatorului obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate şi garantează persoanei vizate dreptul de a obţine de la operator ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, în cazul în care prelucrarea încalcă dispoziţiile adoptate în temeiul articolului 4, 8 sau 10, sau în cazul în care datele cu caracter personal trebuie şterse pentru îndeplinirea unei obligaţii legale care îi revine operatorului.	(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 art.10 ori care trebuie şterse în virtutea îndeplinirii unei obligaţii prevăzute expres de lege.	
94.		(3) În loc de ştergere, operatorul restricţionează prelucrarea datelor cu caracter personal în cazul în care:	(4) Operatorul are obligaţia de a restricţiona prelucrarea datelor cu caracter personal în 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; sau	a) exactitatea datelor cu caracter personal este contestată de persoana vizată, iar exactitatea sau inexactitatea datelor respective nu poate fi stabilită cu certitudine;	
95.		(b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.	b) datele cu caracter personal trebuie să fie păstrate ca mijloace de probă.	
96.		În cazul în care prelucrarea este restricționată în conformitate cu litera (a) de la primul paragraf, operatorul informează în acest sens persoana vizată înainte de ridicarea restricțiilor de prelucrare.	Art.18 alin.(5) Operatorul este obligat să comunice persoanei vizate, în condițiile art.12 alin.(2) și (3), în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, confirmarea sau, după caz, infirmarea soluționării cererilor formulate potrivit alin.(1), (2) sau (3), motivele pe care se întemeiază măsura infirmării, precum și faptul că se poate adresa cu plângere la autoritatea de supraveghere sau poate ataca în instanță decizia operatorului.	
97.		(4) Statele garantează că operatorul informează în scris persoana vizată cu privire la orice refuz de rectificare sau de ștergere a datelor cu caracter personal sau de restricționare a prelucrării și cu privire la motivele refuzului. Statele membre pot adopta măsuri legislative care restricționează, integral sau parțial, obligația de a furniza astfel de informații în măsura în care o astfel de restricționare a prelucrării constituie o măsură necesară și proporțională într-o societate democratică, ținându-se seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice vizate pentru:	(5) Operatorul este obligat să comunice persoanei vizate, în condițiile art.12 alin.(2) și (3), în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, confirmarea sau, după caz, infirmarea soluționării cererilor formulate potrivit alin.(1), (2) sau (3), motivele pe care se întemeiază măsura infirmării, precum și faptul că se poate adresa cu plângere la autoritatea de supraveghere sau poate ataca în instanță decizia operatorului. (6) Termenul prevăzut la alin.(5) poate fi prelungit cu până la 60 de zile calendaristice în măsura în care soluționarea cererilor necesită proceduri complexe, în special consultarea unor autorități competente din străinătate. Persoana vizată este informată cu privire la prelungirea termenului înainte de expirarea termenului inițial. (7) Ridicarea restricționării prelucrării instituite potrivit alin.(4) lit.a), se realizează de către operator,	

			concomitent cu notificarea persoanei vizate cu privire la măsura adoptată. (8) Dispozițiile alin.(5) nu se aplică dacă, ținând seama de drepturile fundamentale și interesele legitime ale persoanei fizice, o astfel de măsură este necesară și proporțională într-o societate democratică pentru:	
98.	(a)	a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau juridice;	a) a evita obstrucționarea cercetărilor, anchetelor sau procedurilor oficiale sau judiciare;	
99.	(b)	a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau executarea pedepselor;	b) a nu prejudicia prevenirea, descoperirea, cercetarea, urmărirea penală și combaterea infracțiunilor sau executarea pedepselor;	
100.	(c)	a proteja securitatea publică;	c) a proteja ordinea și siguranța publică;	
101.	(d)	a proteja securitatea națională;	d) a proteja securitatea națională;	
102.	(e)	a proteja drepturile și libertățile celorlalți.	e) a proteja drepturile și libertățile celorlalți.	
103.		Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a depune o plângere la autoritatea de supraveghere sau de a introduce o cale de atac judiciară.	Art.18 alin.(5) Operatorul este obligat să comunice persoanei vizate, în condițiile art.12 alin.(2) și (3), în termen de cel mult 60 de zile calendaristice de la înregistrarea solicitării, confirmarea sau, după caz, infirmarea soluționării cererilor formulate potrivit alin.(1), (2) sau (3), motivele pe care se întemeiază măsura infirmării, precum și faptul că se poate adresa cu plângere la autoritatea de supraveghere sau poate ataca în instanță decizia operatorului.	
104.		(5) Statele membre garantează comunicarea de către operator a rectificării datelor cu caracter personal inexacte autorității competente de la care provin datele cu caracter personal inexacte	Art.19 (1) În situația rectificării datelor cu caracter personal potrivit art.18 alin.(1) operatorul are obligația să verifice modul în care acestea au fost colectate. (2) În cazul în care datele cu caracter personal au fost colectate prin transfer de la o autoritate competentă, operatorul are obligația să transmită acesteia o notificare cu privire la rectificarea datelor.	

105.		(6) Statele membre garantează faptul că operatorul informează destinatarii cu privire la rectificarea sau ştergerea datelor cu caracter personal sau cu privire la restricţionarea prelucrării, în temeiul alineatelor (1), (2) şi (3), precum şi faptul că destinatarii rectifică sau şterg datele cu caracter personal sau restricţionează prelucrarea datelor cu caracter personal atunci când le revine responsabilitatea pentru acestea.	(3) În situaţia rectificării, ştergerii ori restricţionării datelor cu caracter personal potrivit art.18 alin.(1), (3) sau (4), operatorul are obligaţia să verifice dacă acestea au fost transmise unui terţ sau unui destinatar anterior rectificării. (4) În cazul în care datele cu caracter personal au fost transmise unui terţ sau unui destinatar anterior rectificării, operatorul are obligaţia să transmită acestuia o notificare cu privire la rectificarea, ştergerea ori restricţionarea datelor cu caracter personal, după caz. (5) Destinatarul sau terţul situat pe teritoriul României, ori căruia i se aplică legea română, are obligaţia de a dispune o măsură similară celei cu privire la care a fost notificat, cu excepţia incidenţei, în cazul ştergerii ori restricţionării datelor cu caracter personal, a uneia dintre următoarele situaţii: a) datele sunt necesare pentru prevenirea, descoperirea, cercetarea, urmărirea penală şi combaterea infracţiunilor ori executarea pedepselor, altele decât cele pentru care au fost transmise; b) datele sunt necesare pentru derularea altor proceduri judiciare sau administrative direct legate de prevenirea, descoperirea, cercetarea, urmărirea penală şi combaterea infracţiunilor ori executarea pedepselor; c) datele sunt necesare pentru prevenirea unui pericol iminent şi grav la adresa ordinii şi siguranţei publice. (6) În situaţia incidenţei vreuneia dintre situaţiile prevăzute la alin.(5) lit.a)-c), persoana vizată este informată cu aplicarea, după caz, a dispoziţiilor art.14, cu privire la măsura adoptată, motivele pe care se întemeiază măsura infirmării, precum şi cu privire la faptul că se poate adresa cu plângere autorităţii de supraveghere sau poate ataca în instanţă decizia operatorului.	

106.	*Articolul 17* **Exercitarea drepturilor de către persoana vizată şi verificarea de către autoritatea de supraveghere**	(1) În cazurile menţionate la articolul 13 alineatul (3), la articolul 15 alineatul (3) şi la articolul 16 alineatul (4), statele membre adoptă măsuri prin care se prevede că drepturile persoanei vizate pot fi, de asemenea, exercitate prin intermediul autorităţii de supraveghere competente.	Art.20 (1) În situaţiile prevăzute la art.15, art.17 alin.(3) sau art.19 alin.(6), persoana vizată se poate adresa autorităţii de supraveghere pentru exercitarea drepturilor prevăzute de lege.	
107.		2) Statele membre garantează că operatorul informează persoana vizată cu privire la posibilitatea de a-şi exercita drepturile prin intermediul autorităţii de supraveghere în temeiul alineatului (1).	(2) Operatorul are obligaţia de a informa persoana vizată cu privire la posibilitatea prevăzută la alin.(1).	
108.		(3) Atunci când este exercitat dreptul menţionat la alineatul (1), autoritatea de supraveghere informează persoana vizată cel puţin că au fost realizate toate	(2) În situaţia prevăzută la alin.(1), autoritatea de supraveghere poate declanşa o investigaţie. (3) La finalizarea investigaţiei, autoritatea de supraveghere informează persoana vizată cu privire la	

		verificările necesare sau o revizuire de către autoritatea de supraveghere. Autoritatea de supraveghere informează, de asemenea, persoana vizată în legătură cu dreptul acesteia de a introduce o cale de atac.	aspectele constatate, precum şi cu privire la posibilitatea de a se adresa instanţei de judecată.	
109.	*Articolul 18* **Drepturile persoanei vizate în cadrul investigaţiilor şi procedurilor penale**	Statele membre garantează că drepturile menţionate la articolele 13, 14 şi 16 se exercită în conformitate cu dreptul intern în cazul în care datele cu caracter personal sunt conţinute într-o hotărâre judecătorească sau într-un cazier sau dosar prelucrat pe parcursul investigaţiilor şi procedurilor penale.	Art.21 Exercitarea drepturilor prevăzute la art.13, art.16 şi art.17 nu poate fi limitată de faptul că datele cu caracter personal sunt cuprinse în hotărâri judecătoreşti, în cazierul judiciar sau în dosare de urmărire penală, cu excepţia situaţiilor expres prevăzute de lege.	
110.	***CAPITOLUL IV*** ***Operatorul şi persoana***	(1) Statele membre garantează că, ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate la adresa drepturilor şi libertăţilor persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezenta directivă.	Art.22 (1) Operatorul, ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de gradul de ingerinţă în drepturile şi libertăţile persoanelor fizice, este obligat să aplice măsurile tehnice şi organizatorice adecvate pentru a asigura şi a fi în măsură să demonstreze respectarea tuturor normelor privind protecţia datelor cu caracter personal cuprinse în prezenta lege.	

	împuternicită de către operator **Secţiunea 1** **Obligaţii generale** *Articolul 19* **Obligaţiile operatorului**	Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.		
111.		(2) Atunci când sunt proporţionale în raport cu operaţiunile de prelucrare, măsurile menţionate la alineatul (1) includ punerea în aplicare de către operator a unor politici corespunzătoare de protecţie a datelor.	(2) Măsurile adoptate potrivit alin.(1) trebuie să fie proporţionale cu operaţiunile de prelucrare realizate de către operator şi includ politici corespunzătoare de protecţie a datelor cu caracter personal.	
112.	*Articolul 20* Asigura	(1) Statele membre garantează că, având în vedere stadiul actual al tehnologiei, costurile de punere în aplicare, precum şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu	Art.23 (1) În scopul punerii în aplicare în mod eficient a principiilor de protecţie a datelor cu caracter personal, precum şi pentru reducerea la minim a prelucrărilor de date cu caracter personal, dar şi în scopul integrării garanţiilor necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentei legi şi pentru a proteja	

	rea protecţiei datelor începând cu momentul conceperii şi în mod implicit	grade diferite de probabilitate şi de gravitate la adresa drepturilor şi libertăţilor persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât la momentul stabilirii mijloacelor de prelucrare, cât şi la cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minim a datelor şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentei directive şi a proteja drepturile persoanelor vizate.	drepturile persoanelor vizate, operatorul este obligat ca, la momentul stabilirii mijloacelor de prelucrare cât şi la cel al prelucrării efective, să pună în aplicare măsuri tehnice şi organizatorice adecvate, având în vedere: a) stadiul actual al tehnologiei; b) costurile de punere în aplicare; c) natura, domeniul de aplicare, contextul şi scopurile prelucrării; d) riscurile cu grade diferite de probabilitate şi de gravitate la adresa drepturilor şi libertăţilor persoanelor fizice pe care le prezintă prelucrarea. (2) Pentru îndeplinirea obiectivelor alin.(1), operatorul evaluează, la momentul stabilirii mijloacelor de prelucrare, în scopul identificării măsurilor tehnice şi organizatorice adecvate, cel puţin posibilitatea introducerii unei soluţii de pseudonimizare ori a unei alte soluţii tehnice cu efect similar.	
113.		2) Statele membre garantează că operatorul pune în aplicare măsuri tehnice şi 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. Obligaţia respectivă se aplică volumului de date cu caracter personal colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor. În special, măsurile respective trebuie să asigure că, în mod implicit, datele cu caracter personal nu sunt accesibile, fără intervenţia persoanei fizice, unui număr nedefinit de persoane fizice	(3) Operatorul are obligaţia de a pune în aplicare măsuri tehnice şi 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. (4) Obligaţia prevăzută la alin.(3) vizează: a) volumul de date cu caracter personal colectate; b) gradul de prelucrare a acestora; c) perioada de stocare; d) accesibilitatea acestora . (5) Prin măsurile dispuse potrivit alin.(3) şi (4) operatorul trebuie să se asigure că datele cu caracter personal nu sunt accesibile, fără intervenţie umană, unui număr nedefinit de utilizatori.	
114.	*Articolu*	(1) Statele membre garantează faptul că, atunci când doi sau mai mulţi operatori stabilesc în comun scopurile	Art.24 (1) Operatorii asociaţi se desemnează printr-un act normativ, în cuprinsul căruia se stabilesc, în comun, scopurile şi mijloacele de prelucrare a datelor cu caracter	

	121 **Operatori asociaţi**	şi mijloacele de prelucrare, aceştia sunt operatori asociaţi. Aceştia stabilesc într-un mod transparent responsabilităţile care revin fiecăruia în vederea respectării prezentei directive, în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de furnizare a informaţiilor prevăzute la articolul 13, prin intermediul unui acord între ei, cu excepţia cazului şi în măsura în care responsabilităţile operatorilor sunt stabilite de dreptul Uniunii sau de dreptul intern care li se aplică. Acordul desemnează punctul de contact pentru persoanele vizate. Statele membre pot desemna care dintre operatorii asociaţi poate acţiona ca punct unic de contact pentru exercitarea de către persoanele vizate a drepturilor lor.	personal. (2) Actul normativ prevăzut la alin.(1) trebuie să cuprindă o delimitare a responsabilităţilor ce revin fiecăruia dintre operatorii ascociaţi în condiţiile prezentei legi. (3)" Actul normativ prevăzut la alin.(1) trebuie să cuprindă cel puţin următoarele aspecte: a) modalitatea de exercitare a drepturilor persoanelor vizate, în raport cu oricare dintre operatori; b) îndatoririle fiecăruia dintre operatorii asociaţi cu privire la furnizarea informaţiilor prevăzute la art. 13; c) punctul de contact unic pentru persoanele vizate. (4) În situaţia în care scopurile şi mijloacele de prelucrare nu sunt stabilite prin act normativ, responsabilităţile ce revin în condiţiile prezentei legi operatorilor asociaţi pot fi stabilite prin intermediul unui act juridic. Acesta trebuie să cuprindă elementele prevăzute la alin.(3) şi este supus obligaţiei de punere la dispoziţia persoanelor vizate. Obligaţia de punere la dispoziţie trebuie îndeplinită cu minimum 5 zile înainte de intrarea în vigoare a respectivului act juridic.	
115.		(2) Indiferent de termenii acordului menţionat la alineatul (1), statele membre pot să prevadă dispoziţii potrivit cărora persoana vizată îşi exercită drepturile cu privire la şi în raport cu fiecare dintre operatori în conformitate cu dispoziţiile adoptate în temeiul prezentei directive	(3) Actul normativ prevăzut la alin.(1) trebuie să cuprindă cel puţin următoarele aspecte: a) modalitatea de exercitare a drepturilor persoanelor vizate, în raport cu oricare dintre operatori; b) (...)	
116.	*Articolu 122*	(1) Statele membre garantează că, atunci când o prelucrare urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane	Art.25 (1) Desemnarea persoanelor împuternicite de către operator este posibilă doar dacă există suficiente garanţii pentru punerea în aplicare a măsurilor tehnice şi organizatorice adecvate, astfel încât prelucrarea să	

	Persoana împuternicită de către operator	împuternicite care să ofere garanţii suficiente pentru punerea în aplicare a măsurilor tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele prezentei directive şi să asigure protecţia drepturilor persoanei vizate.	îndeplinească cerinţele prezentei legi şi să asigure protecţia drepturilor persoanei vizate.	
117.		(2) Statele membre garantează că persoana împuternicită de către operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii scrise generale, persoana împuternicită de către operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de către operator, oferind astfel operatorului posibilitatea de a formula obiecţii faţă de aceste modificări.	(2) Desemnarea, de către o persoană împuternicită de către operator, a unei alte persoane împuternicite în scopul realizării uneia sau mai multor operaţiuni de prelucrare nu este posibilă decât cu acordul scris al operatorului. Acordul scris poate fi emis doar dacă sunt îndeplinite condiţiile prevăzute la alin.(1). (3) Persoana împuternicită de către operator are obligaţia de a informa operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de către operator.	
118.		(3). Statele membre garantează că prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern, care are caracter obligatoriu pentru persoana împuternicită de către operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de	(4) Desemnarea prevăzută la alin.(1) sau, după caz, alin.(2) se realizează prin intermediul unui contract sau protocol încheiat între părţi, care trebuie să detalieze: a) obiectul şi durata prelucrării; b) natura şi scopul prelucrării; c) tipul de date cu caracter personal şi categoriile de persoane vizate; d) obligaţiile şi drepturile operatorului. (5) Protocolul sau, după caz, contractul prevăzut la alin.(4) este supus obligaţiei de punere la dispoziţia	

		persoane vizate, precum și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede, în special, că persoana împuternicită de operator:	persoanelor vizate și trebuie să stabilească, în sarcina persoanei împuternicite de către operator, următoarele obligații:	
119.	(a)	acționează numai la instrucțiunile operatorului;	a) să acționeze numai la instrucțiunile operatorului;	
120.	(b)	garantează faptul că persoanele autorizate să prelucreze date cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate corespunzătoare;	b) să garanteze faptul că persoanele autorizate să prelucreze date cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate corespunzătoare;	
121.		(c asistă operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei izate;	c) să asiste operatorul prin orice mijloace adecvate pentru a asigura respectarea dispozițiilor privind drepturile persoanei vizate;	
122.	(d)	la alegerea operatorului, șterge sau returnează toate datele cu caracter personal operatorului după încetarea furnizării serviciilor de prelucrare a datelor și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede stocarea datelor cu caracter personal;	d) să șteargă sau să returneze, din dispoziția operatorului, toate datele cu caracter personal după încetarea furnizării serviciilor de prelucrare a datelor cu caracter personal și să elimine copiile existente, cu excepția cazului în care există o dispoziție legală expresă care îl abilitează să stocheze în continuare datele;	
123.	(e)	pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea prezentului articol;	e) să pună la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea dispozițiilor prezentului articol;	
124.	(f)	respectă condițiile menționate la alineatele (2) și (3) pentru recrutarea unei alte persoane împuternicite de către operator.	f) să respecte condițiile prevăzute la alin. (2)-(4) pentru recrutarea unei alte persoane împuternicite de către operator.	
125.		(4) Contractul sau un alt act juridic menționat la alineatul (3) se întocmește în scris și poate fi pus la	(6) Protocolul sau, după caz, contractul prevăzut la alin.(4) poate fi pus la dispoziția persoanelor vizate, la cerere, în format electronic.	

		dispoziţie în format electronic.		
126.		(5) În cazul în care o persoană împuternicită de către operator stabileşte, cu încălcarea prezentei directive, scopurile şi mijloacele de prelucrare, persoana împuternicită este considerată ca fiind operator în ceea ce priveşte prelucrarea respectivă.	(7) Persoana împuternicită de către operator este considerată operator în cazul în care, prin încălcarea dispoziţiilor prezentei legi, aceasta stabileşte scopurile şi mijloacele de prelucrare pentru datele cu caracter personal puse la dispoziţie de către operator. (8) În situaţia prevăzută la alin.(7), operatorul este exonerat de răspundere numai în situaţia în care demonstrează că persoana împuternicită de operator a acţionat cu rea credinţă.	
127.	*Articolul 23* **Desfăşurarea activităţii de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de către**	Statele membre garantează că persoana împuternicită de către operator şi orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de către operator care are acces la datele cu caracter personal prelucrează datele respective numai la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impun aceasta.	Art.26 (1) Se interzice persoanei împuternicite de către operator să prelucreze datele cu caracter personal cu depăşirea instrucţiunilor primite de la operator, cu excepţia situaţiilor prevăzute expres de lege. (2) Orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de către operator, care are acces la date cu caracter personal, nu poate să le prelucreze decât pe baza instrucţiunilor operatorului, cu excepţia situaţiilor prevăzute expres de lege.	

	operator			
128.	*Articolul 124* **Evidenţe ale activităţilor de prelucrare**	(1) Statele membre garantează că operatorul menţine o evidenţă a tuturor categoriilor de activităţi de prelucrare aflate în responsabilitatea sa. Respectiva evidenţă cuprinde toate informaţiile următoare: (a) numele şi datele de contactale operatorului şi, după caz, ale operatorului asociat şi ale responsabilului cu protecţia datelor;	Art.27 (1) Operatorul este obligat să ţină evidenţa tuturor categoriilor de activităţi de prelucrare aflate în responsabilitatea sa. (2) Evidenţa prevăzută la alin.(1) cuprinde următoarele informaţii: a) denumirea şi datele de contact ale operatorului şi, după caz, ale operatorului asociat şi ale responsabilului cu protecţia datelor;	
129.	(b)	scopurile prelucrării;	b) scopul sau scopurile prelucrării;	
130.	(c)	categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;	c) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;	
131.	(d)	o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;	d) o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal care sunt prelucrate;	
132.	(e)	acolo unde este cazul, utilizarea creării de profiluri;	e) dacă este cazul, menţiuni cu privire la desfăşurarea activităţii de creare de profiluri;	
133.	(f)	acolo unde este cazul, categoriile de transferuri de date cu caracter personal către o ţară terţă sau o organizaţie internaţională;	f) dacă este cazul, categoriile de transferuri de date cu caracter personal către un stat terţ sau o organizaţie internaţională;	
134.	(g)	indicarea temeiului juridic al operaţiunii de prelucrare, inclusiv transferurile, pentru care sunt destinate datele cu	g) indicarea temeiului juridic al operaţiunii de prelucrare, inclusiv al transferurilor de date cu caracter personal efectuate;	

		caracter personal;		
135.	(h)	acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date cu caracter personal;	h) dacă este posibil, termenele limită preconizate pentru ştergerea diferitelor categorii de date cu caracter personal;	
136.	(i)	acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la articolul 29 alineatul (1).	i) dacă este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art.35.	
137.		(2) Statele membre garantează că fiecare persoană împuternicită de către operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, evidenţă care cuprinde: (a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acţionează această persoană şi, după caz, cele ale responsabilului cu protecţia datelor;	Art.28 (1) Persoana împuternicită de către operator este obligată să ţină evidenţa tuturor categoriilor de activităţi de prelucrare aflate în responsabilitatea sa. (2) Evidenţa prevăzută la alin.(1) cuprinde următoarele informaţii: a) numele şi datele de contact ale persoanei sau persoanelor împuternicite de către operator, ale fiecărui operator în numele căruia acţionează această persoană şi, după caz, cele ale responsabilului cu protecţia datelor cu caracter personal;	
138.	(b)	categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;	b) categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;	
139.	(c)	acolo unde este cazul, transferurile de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională, inclusiv, identificarea ţării terţe sau a organizaţiei internaţionale respective, atunci când au primit instrucţiuni explicite în acest sens de la operator;	c) după caz, transferurile de date cu caracter personal către un stat terţ sau către o organizaţie internaţională, inclusiv indicarea statului terţ sau a organizaţiei internaţionale respective, atunci când au primit instrucţiuni explicite în acest sens de la operator;	
140.	(d)	acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la	d) dacă este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art.35.	

		articolul 29 alineatul (1).		
141.		(3) Evidenţele menţionate la alineatele (1) şi (2) se păstrează în scris, inclusiv în format electronic. Operatorul şi persoana împuternicită de acesta pun evidenţele la dispoziţia autorităţii de supraveghere, la cererea acesteia.	Art.29 (1) Evidenţele prevăzute la art.27 şi 28 se păstrează în format de hârtie şi în format electronic. (2) Operatorul sau persoana împuternicită de către operator au obligaţia de a pune la dispoziţia autorităţii de supraveghere, la solicitarea acesteia, evidenţele prevăzute la art.27 şi 28.	
142.	*Articolul 25* **Înregistrarea**	(1) Statele membre se asigură că se înregistrează cel puţin următoarele operaţiuni de prelucrare din cadrul sistemelor de prelucrare automată: colectarea, modificarea, consultarea, divulgarea inclusiv transferurile, combinarea şi ştergerea. Înregistrările consultărilor şi ale divulgărilor fac posibilă determinarea motivelor, a datei şi a momentului acestor operaţiuni şi, în măsura în care este posibil, identificarea persoanei care a consultat sau a divulgat date cu caracter personal şi identitatea destinatarilor acestor date cu caracter personal.	Art.30 (1) Operatorul sau persoana împuternicită de către operator este obligat/obligată să înregistreze, în cadrul sistemelor de prelucrare automată, toate operaţiunile de prelucrare a datelor cu caracter personal. (2) Înregistrările prevăzute la alin.(1) trebuie să conţină cel puţin următoarele informaţii: a) tipul operaţiunii de prelucrare; b) codul de identificare a utilizatorului şi a staţiei de lucru folosite; c) numele fişierului accesat; d) numărul operaţiunilor de prelucrare efectuate; e) codul operaţiei executate sau programul folosit; f) data accesului - an, lună, zi, cu precizarea inclusiv a orei şi minutului la care a fost efectuată prelucrarea. (3) În cazul operaţiunilor de prelucrare sub forma consultării sau divulgării este obligatorie înregistrarea motivului prelucrării care trebuie să permită identificarea documentului/situaţiei concrete care a stat la baza şi a justificat prelucrarea datelor cu caracter personal şi, după caz, a destinatarilor datelor cu caracter personal.	
143.		(2) Înregistrările sunt utilizate numai pentru verificarea legalităţii prelucrării, monitorizare proprie, asigurarea integrităţii şi a securităţii datelor cu caracter personal şi în cadrul unor proceduri penale.	(4) Înregistrările prevăzute la alin.(1) pot fi utilizate doar în următoarele situaţii: a) verificarea legalităţii prelucrării, b) monitorizare proprie realizată de către operator sau, după caz, de către persoana împuternicită de către	

			operator; c) asigurarea integrității și a securității datelor cu caracter personal; d) în cadrul unor proceduri penale, în condițiile și cu restricțiile impuse de lege. (5) Responsabilul cu protecția datelor cu caracter personal, în realizarea atribuțiilor sale, are acces la înregistrările prevăzute la alin. (1)	
144.		(3) Operatorul și persoana împuternicită de către operator pun înregistrările la dispoziția autorității de supraveghere, la cererea acesteia.	(6) Înregistrările prevăzute la alin.(1) se pun la dispoziția autorității de supraveghere, la cererea acesteia.	
145.	*Articolu l 26* **Cooperarea cu autoritatea de supraveghere**	Statele membre garantează că operatorul și persoana împuternicită de către operator cooperează cu autoritatea de supraveghere, la cererea acesteia, în îndeplinirea sarcinilor acesteia	Art.31 Operatorul sau, după caz, persoana împuternicită de către operator sunt obligați să coopereze cu autoritatea de supraveghere, la cererea acesteia, și să dispună orice măsură necesară îndeplinirii sarcinilor acesteia.	
146.	*Articolu l 27* **Evaluarea impactului asupra protecți**	(1) În cazul în care un tip de prelucrare, în special care implică utilizarea de noi tehnologii, și, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, statele membre garantează că operatorul, înainte de prelucrare, efectuează o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal.	Art.32 (1) În situația în care se intenționează introducerea unei noi prelucrări de date cu caracter personal, în special în situația în care aceasta implică utilizarea de noi tehnologii, operatorul este obligat să evalueze următoarele aspecte al prelucrării: a) natura datelor cu caracter personal prelucrate; b) domeniul de aplicare; c) contextul și scopurile prelucrării. (2) În măsura în care prelucrarea prevăzută la alin.(1) este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul este obligat ca înaintea prelucrării să efectueze o	

	ei datelor		evaluare a impactului operațiunilor de prelucrare preconizate asupra datelor cu caracter personal. (3) Pentru operațiunile de prelucrare existente, operatorii sunt obligați să realizeze evaluarea prevăzută la alin.(1) și, după caz, evaluarea impactului operațiunilor de prelucrare prevăzută la alin.(2) în termen de 2 ani de la intrarea în vigoare a prezentei legi.	
147.		(2) Evaluarea menționată la alineatul (1) cuprinde cel puțin o descriere generală a operațiunilor de prelucrare preconizate, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea abordării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze respectarea prezentei directive, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.	(4) Evaluarea impactului operațiunilor de prelucrare prevăzută la alin.(2) cuprinde cel puțin următoarele: a) descrierea generală a operațiunilor de prelucrare preconizate; b) evaluarea riscurilor la adresa drepturilor și libertăților persoanelor vizate; c) măsurile preconizate în vederea abordării riscurilor; d) garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze respectarea dispozițiilor prezentei legi, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate.	
148.	*Articolul 28* **Consultarea prealabilă a autorității de supraveghere**	(1) Statele membre garantează că operatorul sau persoana împuternicită de către operator consultă autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor care urmează a fi creat, în cazul în care: (a o evaluare a impactului asupra protecției datelor,) prevăzută la articolul 27, indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor luate de operator pentru atenuarea riscului sau	Art.33 (1) Operatorul sau, după caz, persoana împuternicită de către operator este obligat/obligată să consulte autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor în situațiile în care: a) evaluarea impactului asupra protecției datelor cu caracter personal prevăzută la art.32 indică faptul că prelucrarea ar genera un risc ridicat în absența măsurilor luate de operator pentru atenuarea riscului;	

149.	(b)	un tip de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor şi libertăţilor persoanelor vizate.	b) tipul de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor şi libertăţilor persoanelor vizate.	
150.		(2) Statele membre garantează că autoritatea de supraveghere este consultată în cadrul procesului de pregătire a unei propuneri de măsură legislativă care să fie adoptată de un parlament naţional sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrare.	(2) În cadrul procedurilor de elaborare a proiectelor de acte normative care reglementează prelucrări de date cu caracter personal sau în baza cărora vor fi realizate astfel de prelucrări este obligatorie consultarea autorităţii de supraveghere.	
151.		(3) Statele membre garantează că autoritatea de supraveghere poate stabili o listă a operaţiunilor de prelucrare care fac obiectul consultării prealabile, în conformitate cu alineatul (1).	(3) Autoritatea de supraveghere este abilitată să stabilească o listă a operaţiunilor de prelucrare care fac obiectul consultării prealabile prevăzute la alin.(1).	
152.		(4) Statele membre garantează că operatorul transmite autorităţii de supraveghere evaluarea impactului asupra protecţiei datelor în temeiul articolului 27 şi, la cererea acesteia, orice altă informaţie care permite autorităţii de supraveghere să evalueze conformitatea prelucrării şi în special riscurile la adresa protecţiei datelor cu caracter personal ale persoanei vizate şi garanţiile aferente.	(4) Operatorul sau, după caz, persoana împuternicită de către operator transmite autorităţii de supraveghere, în termen de 30 de zile calendaristice de la finalizare dar înainte de începerea prelucrării, evaluarea prevăzută la art.32. (5) La cererea autorităţii de supraveghere, operatorul sau, după caz, persoana împuternicită de către operator pun la dispoziţia acesteia orice informaţie în scopul evaluării conformităţii prelucrării şi a riscurilor la adresa protecţiei datelor cu caracter personal ale persoanei vizate şi a garanţiilor aferente.	
153.		(5) Statele membre garantează că atunci când	Art.34 (1) În cazul în care autoritatea de supraveghere constată că operaţiunile de prelucrare pentru care este	

		autoritatea de supraveghere consideră că prelucrarea preconizată, menționată la alineatul (1) din prezentul articol, ar încălca dispozițiile adoptate în temeiul prezentei directive, în special în cazul în care riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului, în termen de cel mult șase săptămâni de la primirea cererii de consultare, și, dacă este cazul, persoanei împuternicite de către operator, și își poate recurge la oricare dintre competențele menționate la articolul 47. Termenul menționat poate fi prelungit cu o lună, ținându-se seama de complexitatea prelucrării preconizate. Autoritatea de supraveghere informează operatorul și, dacă este cazul, persoana împuternicită de către operator, cu privire la prelungirea termenului respectiv, inclusiv cu privire la motivele prelungirii, în termen de o lună de la primirea cererii de consultare.	consultată potrivit art.33 încalcă dispozițiile prezentei legi, în special în cazul în care riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, aceasta formulează și transmite operatorului sau, după caz, persoanei împuternicite de către operator, observații sau recomandări în termen de cel mult 30 de zile lucrătoare de la data înregistrării cererii de consultare. (2) În funcție de complexitatea prelucrării preconizate, termenul prevăzut la alin.(1) poate fi prelungit cu 20 de zile lucrătoare. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de către operator, în termen de 20 zile lucrătoare de la primirea cererii de consultare, cu privire la prelungirea termenului, inclusiv cu privire la motivele acesteia. Dreptul autorității de supraveghere de a formula observații sau recomandări, în situația prevăzută la alin.(1), nu afectează în niciun fel exercitarea oricăreia dintre competențele acesteia prevăzute în Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare.	
154.	**Secțiunea 2 Securitatea datelor cu caracter personal**	(1) Statele membre garantează că, având în vedere stadiul actual al tehnologiei și costurile implementării și ținând seama de natura,domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și de gravitate la adresa drepturilor și libertăților persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, în special în ceea ce privește prelucrarea categoriilor	Art.35 (1) Operatorul sau, după caz, persoana împuternicită de către operator implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător; (2) La stabilirea nivelului de securitate corespunzător, operatorul, sau, după caz, persoana împuternicită de acesta, are în vedere stadiul actual al tehnologiei și costurile implementării și ține seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de gradul de ingerință asupra drepturilor și libertăților persoanelor fizice, în special cu privire la prelucrarea categoriilor speciale de date cu caracter	

	Articolul 29 **Securitatea prelucrării**	speciale de date cu caracter personal menționate la articolul 10.	personal prevăzute la art.10.	
155.		(2) În ceea ce privește prelucrarea automată, fiecare stat membru garantează că operatorul sau persoana împuternicită de către operator pune în aplicare, în urma unei evaluări a riscurilor, măsuri menite: (a să împiedice accesul persoanelor neautorizate la echipamentele de prelucrare utilizate pentru prelucrare („controlul accesului la echipamente”);	(3) În situația prelucrărilor prin mijloace automate, operatorul sau, după caz, persoana împuternicită de către operator sunt obligați să realizeze o evaluare a riscurilor incidente prelucrărilor preconizate. (4) În urmă evaluării prevăzute la alin.(3), operatorul sau, după caz, persoana împuternicită de către operator, au obligația punerii în aplicare a măsurilor menite: a) să asigure controlul accesului la echipamentele de prelucrare utilizate pentru prelucrare, denumit în continuare controlul accesului la echipamente;	
156.	(b)	să împiedice orice citire, copiere, modificare sau eliminare neautorizată a suporturilor de date („controlul suporturilor de date”);	b) să asigure controlul asupra suporturilor de date, în scopul împiedicării oricărei citiri, copieri, modificări sau eliminări neautorizate a acestora, denumit în continuare controlul suporturilor de date;	
157.	(c)	să împiedice introducerea neautorizată de date cu caracter personal și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate („controlul stocării”);	c) să asigure controlul asupra introducerii de date cu caracter personal, precum și asupra inspectării, modificării sau ștergerii neautorizate a datelor cu caracter personal stocate, denumit în continuare controlul stocării;	
158.	(d)	să împiedice utilizarea sistemelor de prelucrare automată de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor („controlul utilizatorului”);	d) să asigure controlul asupra utilizării sistemelor de prelucrare automată cu ajutorul echipamentelor de comunicare a datelor, denumit în continuare controlul utilizatorului;	

159.	(e)	să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare („controlul accesului la date");	e) să asigure faptul că persoanele autorizate să utilizeze un sistem de prelucrare automată au acces numai la datele cu caracter personal pentru care au autorizare, denumit în continuare controlul accesului la date;	
160.	(f)	să asigure că este posibilă verificarea şi identificarea organismelor cărora le-au fost transmise sau puse la dispoziţie sau s-ar putea să le fie transmise sau puse la dispoziţie date cu caracter personal utilizându-se echipamente de comunicare a datelor („controlul comunicării");	f) să asigure că este posibilă verificarea şi identificarea organismelor cărora le-au fost transmise sau puse la dispoziţie sau s-ar putea să le fie transmise sau puse la dispoziţie date cu caracter personal utilizându-se echipamente de comunicare a datelor, denumit în continuare controlul comunicării;	
161.	(g)	să asigure că este posibil ulterior să se verifice şi să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal şi entitatea care le-a introdus („controlul introducerii datelor");	g) să asigure că este posibil ca ulterior să se verifice şi să se identifice datele cu caracter personal introduse în sistemele de prelucrare automată, momentul introducerii datelor cu caracter personal şi entitatea care le-a introdus, denumit în continuare „controlul introducerii datelor;	
162.	(h)	să împiedice citirea, copierea, modificarea sau ştergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date („controlul transportării");	h) să împiedice citirea, copierea, modificarea sau ştergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportării suporturilor de date, denumit în continuare controlul transportării;	
163.	(i)	să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi („recuperarea");	i) să asigure posibilitatea recuperării sistemelor instalate în cazul unei întreruperi, denumit în continuare recuperarea;	
164.	(j)	să asigure funcţionarea sistemului, raportarea defecţiunilor de funcţionare (fiabilitate) şi imposibilitatea coruperii datelor cu caracter personal stocate din cauza funcţionării defectuoase a sistemului („integritate").	j) să asigure funcţionarea, fiabilitatea şi integritatea sistemului, prin instituirea de măsuri de raportare a defecţiunilor de funcţionare şi de asigurare a imposibilităţii coruperii datelor cu caracter personal stocate din cauza funcţionării defectuoase a sistemului.	

165.	*Articolul 30* **Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal**	(1) Statele membre garantează că, în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere fără întârzieri nejustificate și, în cazul în care este posibil, în cel mult 72 de ore după ce a luat cunoștință de aceasta, cu excepția cazului în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice. În cazul notificarea se efectuează în termen de 72 de ore, aceasta va fi însoțită de o justificare a întârzierii.	Art.36 (1) În cazul în care operatorul constată o încălcare a securității datelor, notifică de îndată, fără întârzieri nejustificate, autoritatea de supraveghere. (2) În funcție de complexitatea încălcării securității, notificarea prevăzută la alin.(1) se transmite nu mai târziu de 72 de ore. În această situație, operatorul este obligat să transmită și o justificare a întârzierii. Termenul începe să curgă de la momentul la care operatorul a luat cunoștință despre încălcarea securității datelor cu caracter personal. (3) Notificarea prevăzută la alin.(1) nu este necesară în cazul în care încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc la adresa drepturilor și libertăților persoanelor fizice.	
166.		(2) Persoana împuternicită de către operator înștiințează operatorul fără întârzieri nejustificate după ce la cunoștință de o încălcare a securității datelor cu caracter personal	(4) Persoana împuternicită de către operator are obligația să informeze operatorul de îndată, fără întârzieri nejustitificate, cu privire la existența unei încălcări a securității datelor cu caracter personal. (5) Operatorul are obligația să implementeze toate măsurile necesare pentru a se asigura că persoana împuternicită de către operator respectă și îndeplinește obligațiile ce îi revin potrivit alin.(4).	
167.		(3) Notificarea menționată la alineatul (1) trebuie, cel	(6) Notificarea prevăzută la alin.(1) trebuie să conțină	

		puţin: (a să descrie caracterul încălcării securităţii datelor cu) caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ de persoane vizate în cauză, precum şi categoriile şi numărul aproximativ de înregistrări de date cu caracter personal în cauză;	cel puţin următoarele informaţii: a) o descriere a naturii încălcării securităţii datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ de persoane vizate în cauză, precum şi categoriile şi numărul aproximativ de înregistrări de date cu caracter personal în cauză;	
168.	(b)	să comunice numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;	b) numele şi datele de contact ale responsabilului cu protecţia datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;	
169.	(c)	să descrie consecinţele probabile ale încălcării securităţii datelor cu caracter personal;	c) descrierea consecinţelor probabile ale încălcării securităţii datelor cu caracter personal;	
170.	(d)	să descrie măsurile luate sau propuse de operator pentru a remedia încălcarea securităţii datelor cu caracter personal, inclusiv, dacă este cazul, măsuri pentru a atenua eventualele efecte adverse ale acesteia.	d) descrierea măsurilor luate sau propuse de operator pentru a remedia încălcarea securităţii datelor cu caracter personal, inclusiv, dacă este cazul, a măsurilor necesare pentru a atenua eventualele efecte adverse ale acesteia.	
171.		(4) În cazul în care şi în măsura în care furnizarea informaţiilor în acelaşi timp nu este posibilă, informaţiile pot fi furnizate treptat, fără întârzieri nejustificate.	(7) În cazul în care nu este posibilă furnizarea, în acelaşi timp, a informaţiilor prevăzute la alin.(6), acestea pot fi transmise treptat, fără întârzieri nejustificate, într-un termen care să nu depăşească 48 ore de la momentul transmiterii notificării iniţiale.	
172.		(5) Statele membre garantează că operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, menţionate la alineatul (1), care cuprind o descriere a situaţiei în care a	Art.37 (1) Operatorul are obligaţia să documenteze toate cazurile de încălcare a securităţii datelor cu caracter personal şi să păstreze documentele pentru o perioadă de 10 ani. (2) Documentele prevăzute la alin.(1) trebuie să	

		avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație trebuie să permită autorității de supraveghere să verifice respectarea prezentului articol.	cuprindă: a) descrierea situației în care a avut loc încălcarea securității datelor cu caracter personal, b) descrierea efectelor acesteia; c) descrierea măsurilor de remediere întreprinse. (3) Documentele prevăzute la alin.(1) trebuie să permită autorității de supraveghere să verifice respectarea dispozițiilor prezentului articol.	
173.		(6) Statele membre garantează că, în cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator, informațiile prevăzute la alineatul (3) se comunică operatorului din respectivul stat membru fără întârzieri nejustificate.	Art.38 (1) Operatorul are obligația să transmită informațiile prevăzute la art.36 alin.(6) către entitatea care, după caz, a furnizat datele cu caracter personal sau către care au fost transmise datele cu caracter personal, în cazul în care încălcarea securității datelor implică date cu caracter personal care au fost transmise de un operator dintr-un alt stat membru sau către un astfel de operator. (2) Transmiterea informațiilor potrivit alin.(1) se realizează în termenul prevăzut la art.36 alin.(2).	
174.	*Articolul 31* **Informarea persoanei vizate cu privire la încălcarea securității**	(1) Statele membre garantează că, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.	Art.39 (1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, operatorul informează persoana vizată, fără întârzieri nejustificate, cu privire la încălcarea securității datelor cu caracter personal.	

	datelor cu caracter personal			
175.		(2) În informarea transmisă persoanei vizate, prevăzută la alineatul (1) din prezentul articol, se include o descriere într-un limbaj simplu şi clar a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 30 alineatul (3) literele (b), (c) şi (d).	(2) Informarea prevăzută la alin.(1) trebuie să conţină o descriere, folosind un limbaj simplu şi clar, a naturii încălcării securităţii datelor cu caracter personal şi cel puţin informaţiile prevăzute la art.36 alin.(6) lit.b)-d).	
176.		(3) Informarea persoanei vizate, menţionată la alineatul (1), nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiţii:	(3) Informarea prevăzută la alin.(1) nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiţii:	
177.	(a)	operatorul a pus în aplicare măsuri tehnologice şi organizatorice adecvate de protecţie, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;	a) operatorul a pus în aplicare măsuri tehnologice şi organizatorice adecvate de protecţie, incidente în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;	
178.	(b)	operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor şi libertăţilor persoanelor vizate menţionat la alineatul (1) nu mai este	b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat la adresa drepturilor şi libertăţilor persoanelor vizate menţionat la alin. (1) nu mai este susceptibil să se materializeze;	

		susceptibil să se materializeze;		
179.	(c)	aceasta ar necesita un efort disproporţionat. În acest caz, informarea se înlocuieşte printr-o informare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.	c) necesită un efort disproporţionat; în acest caz, informarea se înlocuieşte cu informarea publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.	
180.		(4) În cazul în care operatorul nu a informat deja persoana vizată cu privire la încălcarea securităţii datelor cu caracter personal, autoritatea de supraveghere, luând în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.	(4) În situaţia primirii unei notificări potrivit art.36, autoritatea de supraveghere, luând în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate dispune operatorului să informeze persoana vizată sau, după caz, să constate că oricare dintre situaţiile prevăzute la alin.(3) este incidentă.	
181.		(5) Informarea persoanei vizate menţionată la alineatul (1) din prezentul articol poate fi amânată, restricţionată sau omisă, sub rezerva condiţiilor şi a motivelor menţionate la articolul 13 alineatul (3).	(5) Informarea prevăzută la alin.(1) poate fi amânată, restricţionată sau omisă în condiţiile art.15.	
182.	**Secţiunea 3 Responsabilul cu protecţia datelor**	(1) Statele membre garantează că operatorul desemnează un responsabil cu protecţia datelor. Statele membre pot scuti de această obligaţie instanţele şi alte autorităţi judiciare independente atunci când acţionează în exerciţiul funcţiei lor judiciare.	Art.40 (1) Operatorul este obligat să desemneze un responsabil cu protecţia datelor cu caracter personal. (2) Sunt exceptate de la obligaţia prevăzută la alin.(1) instanţele şi celelalte autorităţi judiciare independente atunci când acţionează în exerciţiul funcţiei lor judiciare.	

	Articolul 32 **Desemnarea responsabilului cu protecţia datelor**			
183.		(2) Responsabilul cu protecţia datelor este desemnat pe baza calităţilor sale profesionale şi, în special, a cunoştinţelor de specialitate în domeniul legislaţiei şi practicilor privind protecţia datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 34.	(3) Poate fi desemnată responsabil cu protecţia datelor persoana care îndeplineşte următoarele condiţii: a) deţine calităţi profesionale corespunzătoare; b) deţine cunoştinţe de specialitatea în domeniul legislaţiei şi practicilor privind protecţia datelor cu caracter personal; c) are capacitatea de a îndeplini sarcinile prevăzute la art.42.	
184.		(3) Un unic responsabil cu protecţia datelor poate fi desemnat pentru mai multe autorităţi competente, luând în considerare structura organizatorică şi dimensiunea acestora.	(4) Luând în considerare structura organizatorică şi dimensiunea lor, mai multe autorităţi competente pot desemna acelaşi responsabil cu protecţia datelor.	
185.		(4) Statele membre garantează că operatorul publică datele de contact ale responsabilului cu protecţia datelor şi le transmite autorităţii de supraveghere.	(5) Operatorul are obligaţia să publice datele de contact ale responsabilului cu protecţia datelor şi să le comunice autorităţii de supraveghere.	

186.	*Articolul 33* **Funcţia responsabilului cu protecţia datelor**	(1) Statele membre impun operatorului să se asigure că responsabilul cu protecţia datelor este consultat în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal.	Art.41 (1) Operatorul are obligaţia de a consulta responsabilul cu protecţia datelor cu caracter personal în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal.	
187.		(2) Operatorul sprijină responsabilul cu protecţia datelor în îndeplinirea sarcinilor menţionate la articolul 34, asigurându-i resursele necesare pentru executarea acestor sarcini, precum şi accesul la datele cu caracter personal şi la operaţiunile de prelucrare, şi să îşi menţină cunoştinţele de specialitate.	(2) Operatorul are obligaţia de a acorda sprijin responsabilului cu protecţia datelor cu caracter personal în îndeplinirea sarcinilor prevăzute la art.42, în special prin, dar fără a se limita la: a) asigurarea resurselor necesare pentru îndeplinirea sarcinilor; b) asigurarea accesului la datele cu caracter personal şi la operaţiunile de prelucrare; c) asigurarea resurselor necesare pentru menţinerea cunoştinţelor de specialitate şi adaptarea la noile tehnologii.	
188.	*Articolul 34* **Sarcinile responsabilului**	Statele membre garantează că operatorul încredinţează responsabilului cu protecţia datelor cel puţin următoarele sarcini: (a) informarea şi consilierea operatorului şi a angajaţilor care efectuează prelucrarea cu privire la obligaţiile care le revin în temeiul prezentei	Art. 42 Responsabilul cu protecţia datelor îndeplineşte următoarele sarcini principale: a) informează şi consiliază operatorul şi angajaţii acestuia care efectuează prelucrarea cu privire la obligaţiile care le revin în temeiul prezentei legi şi al altor dispoziţii legale privind protecţia datelor cu caracter personal;	

	cu protecți a datelor	directive și al altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor;		
189.	(b)	monitorizarea respectării prezentei directive, a altor dispoziții de drept al Uniunii sau de drept intern privind protecția datelor și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;	b) monitorizează respectarea dispozițiilor prezentei legi, a altor dispoziții legale privind protecția datelor cu caracter personal și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunilor de conștientizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;	
190.	(c)	furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 27;	c) consiliază, la cerere, cu privire la evaluarea impactului asupra protecției datelor cu caracter personal și monitorizarea funcționării acesteia, în conformitate cu art. 32;	
191.	(d)	cooperarea cu autoritatea de supraveghere;	d) cooperează cu autoritatea de supraveghere;	
192.	(e)	asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 28, precum și, dacă este cazul, acordarea consultanței cu privire la orice altă chestiune.	e) este desemnat persoană de contact în relația cu autoritatea de supraveghere privind aspectele legate de prelucrare, asigurând consultarea prealabilă prevăzută la art. 33, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.	
193.	*CAPITOLUL V Transferurile de*	1) Statele membre garantează că orice transfer de date cu caracter personal de către autoritățile competente, care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către o țară terță sau către o organizație internațională, inclusiv transferurilor	Art.43 (1) Transferul de date cu caracter personal care sunt în curs de prelucrare sau care sunt destinate prelucrării după transferul către un stat terț sau către o organizație internațională, inclusiv transferurile ulterioare către un alt stat terț sau o altă organizație internațională, poate avea loc doar cu respectarea	

	date cu caracter personal către țări terțe sau organizații internaționale *Articolul 35* **Principii generale pentru transferurile de date cu caracter personal**	ulterioare către o altă țară terță sau organizație internațională, poate avea loc numai sub rezerva respectării altor dispoziții ale prezentei directive, în cazul în care sunt îndeplinite condițiile prevăzute în prezentul capitol, și anume: (a) transferul este necesar în scopurile stabilite la articolul 1 alineatul (1);	dispozițiilor prezentei legi și numai dacă sunt îndeplinite următoarele condiții: a) transferul este necesar pentru realizarea scopurilor prevăzute la art.1 alin.(1);	
194.	(b)	datele cu caracter personal sunt transferate unui operator într-o țară terță sau unei organizații internaționale care este o autoritate competentă în sensul articolului 1	b) datele cu caracter personal sunt transferate unui operator dintr-o țară terță, care este o autoritate competentă, în sensul art.4 lit.g), sau unei organizații internaționale, înființată în scopul prevăzut la art.1	

		alineatul (1);	alin.(1);	
195.	(c)	în cazul în care datele cu caracter personal sunt transmise sau puse la dispoziție din alt stat membru, acel stat membru a autorizat în prealabil efectuarea transferului, în conformitate cu dreptul său intern;	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;	
196.	(d)	Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție, în temeiul articolului 36, sau, în absența unei astfel de decizii, există sau se oferă garanții adecvate în temeiul articolului 37 sau, în absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu articolul 36 sau a unor garanții adecvate în conformitate cu articolul 37, se aplică derogări pentru situații speciale în conformitate cu articolul 38; și	d) Comisia Europeană a adoptat o decizie privind caracterul adecvat al nivelului de protecție, denumită în continuare decizie de adecvare;	
197.	(e)	în cazul unui transfer ulterior către o altă țară terță 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, inclusiv de gravitatea infracțiunii, de scopul în care datele cu caracter personal au fost transferate inițial și de nivelul de protecție a datelor cu caracter personal din țara terță sau din organizația internațională către care sunt transferate ulterior datele cu caracter personal.	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. (2) La evaluarea factorilor relevanți pentru transfer, în condițiile alin.(1) lit.e), se au în vedere cel puțin următoarele aspecte: a) gravitatea infracțiunii; b) scopul în care datele cu caracter personal au fost transferate inițial; c) nivelul de protecție a datelor cu caracter personal din țara terță sau din organizația internațională către care sunt transferate ulterior datele cu caracter personal. (3) Autoritățile competente române autorizează transferul datelor cu caracter personal către un stat terț	

			sau către o organizaţie internaţională, la cererea unei autorităţi competente dintr-un stat membru, numai dacă sunt îndeplinite condiţiile prevăzute de prezenta lege. (4) Autorizarea prevăzută la alin.(3) se transmite cu celeritate, dar nu mai târziu de 30 de zile calendaristice de la primirea cererii. În situaţia în care nu sunt îndeplinite condiţiile prevăzute de prezenta lege pentru autorizarea transferului, autorităţii competente din statul membru care a formulat cererea i se comunică motivele pentru care transferul nu poate fi autorizat.	
198.		(2) Statele membre garantează că transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu litera (c) de la alineatul (1), sunt permise numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei ameninţări imediate şi grave la adresa securităţii publice a unui stat membru sau a unei ţări terţe sau a intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obţinută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile este informată fără întârziere.	(5) Autorităţile competente române pot realiza transferurile fără autorizarea prealabilă de către un alt stat membru, în conformitate cu dispoziţiile alin.(1) lit. e), numai dacă transferul de date cu caracter personal este necesar pentru prevenirea unei ameninţări imediate şi grave la adresa ordinii şi siguranţei publice a unui stat membru sau a unei ţări terţe sau a intereselor fundamentale ale unui stat membru, iar autorizarea prealabilă nu poate fi obţinută în timp util. Autoritatea responsabilă pentru acordarea unei autorizări prealabile este informată fără întârziere.	
199.		(3) Toate dispoziţiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecţie a persoanelor fizice garantat prin prezenta directivă nu este subminat.	(6) Dispoziţiile prezentului articol, precum şi cele ale art.44-48 se aplică pentru a se asigura că nivelul de protecţie a persoanelor fizice garantat prin prezenta lege nu este subminat.	

200.	*Articolul 36* **Transferuri în baza unei decizii privind caracterul adecvat al nivelului de protecţie**	(1) Statele membre garantează că transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională se poate realiza atunci când Comisia a decis că ţara terţă, un teritoriu ori unul sau mai multe sectoare determinate din acea ţară terţă sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale.	Art.44 (1) Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională este întotdeauna posibil, în condiţiile art.43 alin.(1) lit.d), atunci când Comisia Europeană a decis că statul terţ, un teritoriu ori una sau mai multe diviziuni administrativ-teritoriale determinate din acel stat terţ sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. (2) Transferurile realizate în condiţiile alin.(1) nu necesită autorizări speciale.	
201.		(2) Atunci când evaluează caracterul adecvat al nivelului de protecţie, Comisia ţine seama, în special, de următoarele elemente: (a) statul de drept, respectarea drepturilor omului şi a libertăţilor fundamentale, legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind securitatea publică, apărarea, securitatea naţională şi dreptul penal şi accesul autorităţilor publice la datele cu caracter personal, precum şi punerea în	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislaţia naţională

		aplicare a acestei legislații, a normelor de protecție a datelor, a normelor profesionale și a măsurilor de securitate, inclusiv a normelor privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara respectivă sau de organizația internațională respectivă, jurisprudența, precum și drepturile efective și opozabile ale persoanelor vizate și reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;		
202.	(b)	existența și funcționarea efectivă a uneia sau a mai multor autorități de supraveghere independente în țara terță sau sub incidența cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de sancționare, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislația națională
203.	(c)	angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente cu caracter juridic obligatoriu, precum și participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal.	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislația națională
204.		3) Comisia, după ce evaluează caracterul adecvat al	(3) Autoritățile competente au obligația, în situația transferurilor prevăzute la alin.(1), să monitorizeze și să	

		nivelului de protecție, poate decide, prin intermediul unui act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol. Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea sa teritorială și sectorială și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alineatul (2) litera (b) din prezentul articol. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2). (	respecte întocmai dispozițiile actelor de punere în aplicare adoptate de Comisia Europeană.	
205.		4) Comisia monitorizează în permanență evoluțiile din țările terțe și organizațiile internaționale care ar putea afecta funcționarea deciziilor adoptate în conformitate cu alineatul (3).	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislația națională
206.		(5) În cazul în care din informațiile disponibile, în special în urma revizuirii menționate la alineatul (3) din prezentul articol, reiese că o țară terță, un teritoriu sau un sector determinat dintr-o țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alineatului (2) din prezentul articol, Comisia, în măsura în care este necesar, abrogă,	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislația națională

		modifică sau suspendă, prin intermediul unor acte de punere în aplicare, decizia menționată la alineatul (3) din prezentul articol fără efect retroactiv. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2). Din motive imperioase de urgență justificate corespunzător, Comisia adoptă acte de punere în aplicare imediat aplicabile în conformitate cu procedura menționată la articolul 58 alineatul (3).		
207.		(6) Comisia inițiază consultări cu țara terță sau organizația internațională în vederea remedierii situației care a stat la baza deciziei luate în conformitate cu alineatul (5).	Nu necesită transpunere	Sarcinile COM nu trebuie transpuse în legislația națională
208.		(7) Statele membre garantează că o decizie luată în temeiul alineatului (5) nu aduce atingere transferurilor de date cu caracter personal către țara terță, către teritoriul sau către unul sau mai multe sectoare determinate din acea țară terță sau către organizația internațională în cauză în conformitate cu articolele 37 și 38.	(4) Decizia Comisiei Europene de abrogare, modificare sau suspendare a unei decizii de adecvare nu aduce atingere transferurilor de date cu caracter personal către țara terță, către teritoriul sau către unul sau mai multe sectoare determinate din acea țară terță sau către organizația internațională în cauză în conformitate cu articolele 37 și 38.	
209.		(8) Comisia publică în *Jurnalul Oficial al Uniunii Europene* și pe site-ul său web o listă a țărilor terțe, a	(5) Autoritățile competente române au obligația monitorizării listei statelor terțe, a teritoriilor și diviziunilor administrativ-teritoriale determinate din	

		teritoriilor şi sectoarelor determinate din ţările terţe şi a organizaţiilor internaţionale în cazul cărora a decis că nivelul de protecţie adecvat este asigurat sau nu mai este asigurat.	statele terţe şi a organizaţiilor internaţionale în cazul cărora Comisia Europeană a decis că nivelul de protecţie adecvat este asigurat sau nu mai este asigurat.	
210.	*Articolu l 37* **Transferuri sub rezerva unor garanţii adecvate**	(1) În absenţa unei decizii luate în conformitate cu articolul 36 alineatul (3), statele membre garantează că transferul de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc atunci când: (a) s-au prezentat garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal printr-un act cu caracter juridic obligatoriu; sau	Art.45 (1) Prin excepţie de la dispoziţiile art.43 alin.(1) lit.d), în absenţa unei decizii adoptate de Comisia Europeană, transferul de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc atunci când: a) au fost stabilite garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal printr-un act cu caracter juridic obligatoriu sau	
211.	(b)	operatorul a evaluat toate circumstanţele aferente transferului de date cu caracter personal şi a concluzionat că există garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal.	b) operatorul a evaluat toate circumstanţele aferente transferului de date cu caracter personal şi a concluzionat că există garanţii adecvate în ceea ce priveşte protecţia datelor cu caracter personal. (2) În scopul îndeplinirii condiţiilor prevăzute la alin.(1) lit.b), operatorul trebuie să ţină cont de următoarele: a) situaţia generală privind respectarea drepturilor omului şi a libertăţilor fundamentale; b) legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind ordinea şi siguranţa publică, apărarea, securitatea naţională şi dreptul penal, precum şi punerea în aplicare a acestei legislaţii; c) accesul autorităţilor publice la datele cu caracter personal; d) legislaţia privind protecţia datelor cu caracter personal;	

			e) măsurile privind asigurarea securităţii datelor cu caracter personal; f) legislaţia privind transferul ulterior de date cu caracter personal către o altă ţară terţă sau organizaţie internaţională; g) drepturile efective şi opozabile ale persoanelor vizate şi reparaţii efective pe cale administrativă şi judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate.	
212.		(2) Operatorul informează autoritatea de supraveghere cu privire la categoriile de transferuri în temeiul alineatului (1) litera (b).	(3) Operatorul informează autoritatea de supraveghere cu privire la transferurile realizate în condiţiile alin.(1) lit.b).	
213.		(3) Atunci când un transfer se întemeiază pe alineatul (1) litera (b), un astfel de transfer se documentează, iar documentaţia se pune la dispoziţia autorităţii de supraveghere la cerere, incluzând data şi ora transferului, informaţii cu privire la autoritatea competentă destinatară, justificarea transferului şi datele cu caracter personal transferate.	(4) Operatorul are obligaţia să ţină evidenţa transferurilor realizate în condiţiile alin.(1) lit.b), precizând cel puţin următoarele: a) data şi ora transferului; b) informaţii cu privire la autoritatea competentă destinatară; c) informaţii cu privire la justificarea transferului; d) datele cu caracter personal transferate. (5) Documentaţia prevăzută la alin.(4) se păstrează pentru o perioadă de zece ani şi, la cerere, se pune la dispoziţia autorităţii de supraveghere.	
214.	*Articolul 38* **Derogări pentru situaţii**	(1) În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie în conformitate cu articolul 37 sau a unor garanţii adecvate în conformitate cu articolul 36, statele membre garantează că un transfer sau o categorie de transferuri de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc numai în condiţiile în care transferul este necesar:	Art.46 (1) Prin excepţie de la dispoziţiile art.45 alin.(1) şi în cazul în care nu pot fi îndeplinite condiţiile prevăzute la art.44, un transfer sau o categorie de transferuri de date cu caracter personal către o ţară terţă sau către o organizaţie internaţională poate avea loc numai în condiţiile în care transferul este necesar pentru: a) protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane, cum ar fi prevenirea unui pericol iminent cel puţin asupra vieţii, integrităţii corporale sau	

	specific e	(a pentru protejarea intereselor vitale ale persoanei) vizate sau ale unei alte persoane;	sănătăţii acestora;	
215.	(b)	pentru protejarea intereselor legitime ale persoanei vizate, în cazul în care dreptul statului membru care transferă datele cu caracter personal prevede acest lucru;	b) protejarea intereselor legitime ale persoanei vizate, în cazul în care există o dispoziţie legală expresă în acest sens;	
216.	(c)	pentru prevenirea unei ameninţări imediate şi grave la adresa securităţii publice a unui stat membru sau a unei ţări terţe;	c) prevenirea unei ameninţări imediate şi grave la adresa ordinii şi siguranţei publice a unui stat membru sau a unei ţări terţe;	
217.	(d)	în cazuri individuale în scopurile stabilite la articolul 1 alineatul (1); sau	d) în cazuri individuale în scopurile stabilite la art.(1) alin.(1);	
218.	(e)	într-un caz individual pentru descoperirea, exercitarea sau apărarea unui drept în instanţă privind scopurile stabilite la articolul 1 alineatul (1).	e) într-un caz individual pentru descoperirea, exercitarea sau apărarea unui drept în instanţă privind scopurile stabilite la art. 1 alin. (1).	
219.		(2) Datele cu caracter personal nu sunt transferate dacă autoritatea competentă care transferă datele stabileşte că drepturile şi libertăţile fundamentale ale persoanei vizate în cauză prevalează asupra interesului public în cazul transferului prevăzut la alineatul (1) literele (d) şi (e).	(2) Se interzice transferul datelor cu caracter personal în condiţiile alin.(1) lit.d) şi e) în cazul în care în urma evaluărilor realizate de autoritatea competentă română care transferă datele cu caracter personal se stabileşte că drepturile şi libertăţile fundamentale ale persoanei vizate prevalează asupra interesului public, în special în situaţia în care există indicii privind posibila afectare a dreptului la viaţă al persoanei.	
220.		(3) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer trebuie să fie documentat, iar documentaţia trebuie pusă la dispoziţia autorităţii de supraveghere la cerere, incluzând data şi ora transferului,	(3) În situaţia transferurilor realizate în condiţiile alin.(1), dispoziţiile art.45 alin.(4) şi (5) se aplică în mod corespunzător.	

		informații cu privire la autoritatea competentă destinatară, justificarea transferului și datele cu caracter personal transferate		
221.	*Articolul 39* **Transferurile de date cu caracter personal către destinatari stabiliți în țări terțe**	1) Prin derogare de la articolul 35 alineatul (1) litera (b) și fără a aduce atingere niciunui acord internațional menționat la alineatul (2) din prezentul articol, dreptul Uniunii sau dreptul intern poate să prevadă că autoritățile competente menționate la articolul 3 punctul 7 litera (a) pot, în cazuri individuale și specifice, transfera date cu caracter personal direct destinatarilor stabiliți în țări terțe, dar numai în cazul în care celelalte dispoziții ale prezentei directive sunt respectate și dacă sunt îndeplinite următoarele condiții:	Art.47 (1) În cazuri individuale specifice, dacă sunt îndeplinite toate condițiile referitoare la transferul de date cu caracter personal prevăzute de prezenta lege, operatorul poate transfera date cu caracter personal către entități din state terțe care nu sunt autorități competente în înțelesul prezentei legi, numai dacă sunt îndeplinite în mod cumulativ următoarele condiții:	
222.	(a)	transferul este strict necesar pentru executarea unei sarcini de către autoritatea competentă care transferă datele, astfel cum este prevăzut de dreptul Uniunii sau de dreptul intern în scopurile prevăzute la articolul 1 alineatul (1);	a) transferul este strict necesar pentru exercitarea unei atribuții prevăzute de lege în sarcina autorității competente române, în scopul îndeplinirii activităților prevăzute la art. 1 alin. (1);	
223.	(b)	autoritatea competentă care transferă datele stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața	b) autoritatea competentă română stabilește că niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața interesului public care impune transferul în cazul respectiv;	

		interesului public care necesită transferul în cazul respectiv;		
224.	(c)	autoritatea competentă care transferă datele consideră că transferul către o autoritate din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este ineficient sau necorespunzător, în special din cauză că transferul nu poate fi realizat în timp util;	c) din evaluările realizate de către autoritatea competentă română rezultă că transferul către o autoritate din țara terță, care este competentă în scopul îndeplinirii activităților prevăzute la art.1 alin.(1), este ineficient sau necorespunzător, în special din cauză că transferul nu poate fi realizat în timp util;	
225.	(d)	autoritatea din țara terță, care este competentă în scopurile menționate la articolul 1 alineatul (1), este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau necorespunzătoare; și	d) autoritatea din țara terță, care este competentă în scopul îndeplinirii activităților prevăzute la art.1 alin.(1), este informată fără întârzieri nejustificate, cu excepția cazului în care această măsură este ineficientă sau necorespunzătoare;	
226.	(e)	autoritatea competentă care transferă datele informează destinatarul cu privire la scopul sau scopurile determinate exclusive în care aceasta din urmă poate să prelucreze datele cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară.	e) autoritatea competentă română informează destinatarul cu privire la scopul sau scopurile determinate exclusive în care aceasta din urmă poate să prelucreze datele cu caracter personal, cu condiția ca o astfel de prelucrare să fie necesară. (2) Transferul în condițiile alin.(1) este posibil numai dacă destinatarul se angajează în scris să nu prelucreze datele cu caracter în alt scop decât cel pentru care au fost transmise, circumscris îndeplinirii scopurilor prevăzute la art.(1) alin.(1).	
227.		(2) Un acord internațional menționat la alineatul (1) este orice acord internațional bilateral sau multilateral în vigoare între statele membre și țări terțe în domeniul cooperării judiciare în materie penală și al cooperării polițienești.	(3) Dispozițiile alin.(1) nu afectează transferurile de date cu caracter personal stabilite prin tratate încheiate în domeniul cooperării judiciare în materie penală sau al cooperării polițienești internaționale.	

228.		(3) Autoritatea competentă care transferă datele informează autoritatea de supraveghere cu privire la transferurile efectuate în temeiul prezentului articol.	(4) Autoritatea competentă română informează periodic, cel puțin o dată pe an, autoritatea de supraveghere cu privire la transferurile efectuate în temeiul prezentului articol.	
229.		(4) Atunci când un transfer se întemeiază pe alineatul (1), un astfel de transfer trebuie să fie documentat	(5) În situația transferurilor realizate în condițiile alin.(1), dispozițiile art.43 alin.(4) și (5) se aplică în mod corespunzător.	
230.	*Articolul 40* **Cooperarea internațională în domeniul protecției datelor cu caracter personal**	În ceea ce privește țările terțe și organizațiile internaționale, Comisia și statele membre iau măsurile corespunzătoare pentru: (a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației privind protecția datelor cu caracter personal;	Art.48 Autoritățile competente dispun măsuri corespunzătoare pentru: a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea efectivă a respectării legislației privind protecția datelor cu caracter personal;	

231.	(b)	acordarea de asistenţă internaţională reciprocă în asigurarea respectării legislaţiei din domeniul protecţiei datelor cu caracter personal, inclusiv prin notificări, transferul reclamaţiilor, asistenţă în anchete şi schimb de informaţii, sub rezerva unor garanţii adecvate pentru protecţia datelor cu caracter personal şi a altor drepturi şi libertăţi fundamentale;	b) acordarea de asistenţă internaţională reciprocă în asigurarea respectării legislaţiei din domeniul protecţiei datelor cu caracter personal, inclusiv prin notificări, transferul reclamaţiilor, asistenţă în anchete şi schimb de informaţii, sub rezerva unor garanţii adecvate pentru protecţia datelor cu caracter personal şi a altor drepturi şi libertăţi fundamentale;	
232.	(c)	implicarea părţilor interesate relevante în discuţiile şi activităţile care au ca scop consolidarea cooperării internaţionale în vederea asigurării respectării legislaţiei din domeniul protecţiei datelor cu caracter personal;	c) implicarea părţilor interesate relevante în discuţiile şi activităţile care au ca scop consolidarea cooperării internaţionale în vederea asigurării respectării legislaţiei din domeniul protecţiei datelor cu caracter personal;	
233.	(d)	promovarea schimburilor de legislaţie şi practici în materie de protecţie a datelor cu caracter personal şi a documentării cu privire la acestea, inclusiv cu privire la conflictele de jurisdicţie cu ţările terţe.	d) promovarea schimburilor de legislaţie şi practici în materie de protecţie a datelor cu caracter personal şi a documentării cu privire la acestea, inclusiv în ceea ce priveşte eventualele conflictele de jurisdicţie cu ţările terţe.	
234.			Art.49 (1) Pentru realizarea activităţilor de cercetare şi combatere a infracţiunilor sistemele de evidenţă a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care operatorii le deţin, pentru scopuri diferite, pot fi interconectate. (2) În scopul prevăzut la alin.(1), interconectarea sistemelor de evidenţă a datelor cu caracter personal sau a mijloacelor automate de prelucrare a datelor cu caracter personal, se poate realiza şi cu sistemele de evidenţă ori cu mijloacele automate de prelucrare a datelor cu caracter personal deţinute de alţi operatori, autorităţi şi instituţii publice naţionale. (3) Interconectările prevăzute la alin.(1) şi (2) sunt posibile numai cu acordul prealabil al autorităţii de supraveghere.	Necesitate pentru structurile M.A.I.

			(4) În scopul prevăzut la alin. (1), interconectarea sistemelor de evidenţă a datelor cu caracter personal sau a mijloacelor automate de prelucrare a datelor cu caracter personal se poate realiza şi cu sistemele de evidenţă sau cu mijloacele automate de prelucrare a datelor cu caracter personal deţinute de alţi operatori, entităţi de drept privat. (5) Interconectările prevăzute la alin. (4) sunt permise numai în scopul efectuării urmăririi penale, în baza unei ordonanţe emise de procurorul competent să efectueze ori să supravegheze, într-un caz determinat, urmărirea penală ori, în cazul judecării unei infracţiuni, de judecătorul anume desemnat de la instanţa căreia îi revine competenţa de a judeca fondul cauzei pentru care sunt prelucrate datele cu caracter personal respective. (6) Accesul direct sau printr-un serviciu de comunicaţii electronice la un sistem de evidenţă a datelor cu caracter personal care face obiectul interconectării, potrivit alin. (1), este permis numai în condiţiile legii şi cu respectarea prevederilor art. 1 alin. (1). Art. 50(1) În cazul activităţilor de prevenire a infracţiunilor, de menţinere şi de asigurare a ordinii şi siguranţei publice, sistemele de evidenţă a datelor cu caracter personal sau mijloacele automate de prelucrare a datelor cu caracter personal pot fi interconectate cu: a) Registrul naţional de evidenţă a persoanelor; b) Registrul naţional de evidenţă a paşapoartelor simple; c) Registrul naţional de evidenţă a permiselor de conducere şi a vehiculelor înmatriculate. (2) În cazul activităţilor prevăzute la alin. (1), sistemele de evidenţă a datelor cu caracter personal sau,	

			după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care le deţin operatorii, pentru scopuri similare ori corelate, pot fi interconectate. (3) Interconectările prevăzute la alin.(1) şi (2) se aduc la cunoştinţa autorităţii de supraveghere. (4) În cazul activităţilor prevăzute la alin.(1), se pot interconecta sistemele de evidenţă a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care le deţin pentru scopuri diferite, numai cu acordul prealabil al autorităţii de supraveghere.	
235.	***CAPITOLUL VI Autorităţi de supraveghere independente*** **Secţiunea I Statut independent** *Articolul 41* **Autoritatea de supraveghere**	1) Fiecare stat membru garantează că una sau mai multe autorităţi publice independente sunt responsabile de monitorizarea aplicării prezentei directive, în vederea protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii („autoritatea de supraveghere").	Art.51 (1) Supravegherea prelucrărilor de date cu caracter personal efectuate în temeiul prezentei legi, în scopul protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii Europene, se realizează de către autoritatea de supraveghere.	

	ghere			
236.		(2) Fiecare autoritate de supraveghere contribuie la aplicarea consecventă a prezentei directive în întreaga Uniune. În acest scop, autoritățile de supraveghere cooperează atât între ele, cât și cu Comisia, în conformitate cu capitolul VII.	(2) Autoritatea de supraveghere cooperează cu autorități similare din alte state membre, precum și cu Comisia, în conformitate cu art.54.	
237.		(3) Statele membre pot să prevadă că o autoritate de supraveghere instituită în conformitate cu Regulamentul (UE) 2016/679 constituie autoritatea de supraveghere menționată în prezenta directivă și își asumă responsabilitatea pentru sarcinile autorității de supraveghere care urmează să fie instituită în conformitate cu alineatul (1) din prezentul articol.	Nu necesită transpunere	Art. 51 (1)Supravegherea prelucrărilor de date cu caracter personal efectuate în temeiul prezentei legi, 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 ANSPDCP.
238.		(4) În cazul în care un stat membru instituie mai multe	Nu necesită transpunere	În România

		autorităţi de supraveghere, statul membru respectiv desemnează autoritatea de supraveghere care reprezintă autorităţile respective în cadrul comitetului menţionat la articolul 51.		ANSPDCP monitorizează atât aplicarea Directivei UE 2016/680, cât şi a Regulamentului General privind Protecţia Datelor.
239.	*Articolul 42* **Independenţă**	(1) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de independenţă deplină în îndeplinirea sarcinilor şi exercitarea competenţelor care le revin în conformitate cu prezenta directivă.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile legii 102/2005(legea de modificare)
240.		(2) Statele membre garantează că membrii autorităţilor lor de supraveghere, în îndeplinirea sarcinilor şi în exercitarea competenţelor care le revin în conformitate cu prezenta directivă, rămân independenţi de orice influenţă externă directă sau indirectă şi nici nu solicită, nici nu acceptă instrucţiuni de la nimeni.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.52 alin. (2))
241.		(3) Membrii autorităţilor de supraveghere din statele membre nu întreprind acţiuni incompatibile cu îndatoririle lor, iar, pe durata mandatului, nu desfăşoară activităţi incompatibile, remunerate sau nu.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.52 alin. (3))

242.		(4) Fiecare stat membru garantează că autoritatea sa de supraveghere beneficiază de resurse umane, tehnice şi financiare, de un sediu şi de infrastructura necesară pentru îndeplinirea sarcinilor şi exercitarea competenţelor în mod eficace, inclusiv a celor care urmează să fie realizate în contextul asistenţei reciproce, al cooperării şi al participării în cadrul comitetului.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile legii 102/2005(legea de modificare) Regulamentului 679/2016 (Art.52 alin. (4))
243.		(5) Fiecare stat membru garantează că autoritatea sa de supraveghere selectează şi dispune de personal propriu, care se află sub conducerea exclusivă a membrului sau membrilor autorităţii de supraveghere vizate.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.52 alin. (5))
244.		(6) Fiecare stat membru garantează că autoritatea sa de supraveghere face obiectul unui control financiar care nu aduce atingere independenţei sale şi că dispune de bugete publice anuale distincte, care pot face parte din bugetul general de stat sau naţional.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.52 alin. (6))
245.	*Articolu*	(1) Statele membre garantează că fiecare membru al autorităţilor lor de supraveghere este numit prin	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de

	143 **Condiții generale aplicabile membrilor autorității de supraveghere**	intermediul unei proceduri transparente: — de către parlament; — de către guvern; — de către șeful statului membru în cauză; sau — de către un organism independent împuternicit prin dreptul intern să facă numirea.		supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.53 alin. (1))
246.		(2) Fiecare membru dispune de calificările, experiența și competențele, în special în domeniul protecției datelor cu caracter personal, necesare pentru îndeplinirea atribuțiilor și exercitarea competențelor sale. (	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.53 alin. (2))
247.		3) Atribuțiile unui membru încetează în cazul expirării mandatului, în cazul demisiei sau destituirii în conformitate cu dreptul statului membru în cauză.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în RO s-ar dubla dispozițiile Regulamentului 679/2016 (Art.53 alin.

				(3))
248.		(4) Un membru poate fi demis doar în cazuri de abateri grave sau în cazul în care membrul respectiv nu mai întruneşte condiţiile necesare pentru îndeplinirea atribuţiilor sale.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.53 alin. (4))
249.	*Articolul 144* **Norme privind instituirea autorităţii de supraveghere**	(1) Fiecare stat membru prevede în dreptul său următoarele: (a) instituirea autorităţii sale de supraveghere;	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit. a))
250.	(b)	calificările şi condiţiile de eligibilitate necesare pentru a fi numit membru al autorităţii sale de supraveghere;	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit. b))

251.	(e)	normele şi procedurile pentru numirea membrului sau a membrilor autorităţii sale de supraveghere;	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit. c))
252.	(d)	durata mandatului membrului sau al membrilor autorităţii sale de supraveghere, care nu poate fi mai mică de patru ani, cu excepţia primului mandat după 6 mai 2016, care poate fi mai scurt în cazul în care acest lucru este necesar pentru a proteja independenţa autorităţii de supraveghere printr-o procedură de numiri eşalonate;	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit.d))
253.	(e)	dacă şi de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor autorităţii sale de supraveghere; şi	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit. e))
254.	(f)	condiţiile care reglementează obligaţiile membrului sau membrilor şi ale personalului autorităţii sale de supraveghere, interdicţiile privind acţiunile, ocupaţiile şi beneficiile incompatibile cu acestea în cursul mandatului şi după încetarea acestuia, precum şi normele care reglementează încetarea activităţii profesionale.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (1)lit. f))

255.		(2) Membrul sau membrii şi personalul fiecărei autorităţi de supraveghere au obligaţia, în conformitate cu dreptul Uniunii sau cu dreptul intern, de a păstra atât pe parcursul mandatului, cât şi după încetarea acestuia, secretul profesional în ceea ce priveşte toate informaţiile confidenţiale de care au luat cunoştinţă în cursul îndeplinirii atribuţiilor sau al exercitării competenţelor lor. Pe durata mandatului lor, această obligaţie de păstrare a secretului profesional se aplică, în special, în ceea ce priveşte denunţarea de către persoane fizice a cazurilor de încălcare a prezentei directive.	Nu necesită transpunere	Având în vedere existenţa unei singure Autorităţi de supraveghere în România s-ar dubla dispoziţiile Regulamentului 679/2016 (Art.54 alin. (2))
256.	**Secţiunea 2 Abilităţi, sarcini şi competenţe** *Articolul 45* **Abilităţi**	1) Fiecare stat membru garantează că autoritatea sa de supraveghere este abilitată să îndeplinească sarcinile şi să exercite competenţele care îi revin în conformitate cu prezenta directivă pe teritoriul respectivului stat membru.	Art. 52 (1) Autoritatea de supraveghere monitorizează şi controlează sub aspectul legalităţii prelucrările de date cu caracter personal care intră sub incidenţa prezentei legi.	Regulamentul General de Protecţie a Datelor şi Legea nr.102/2005
257.		(2) Fiecare stat membru garantează că autorităţii sale	(2) Prin excepţie de la alin.(1), autoritatea de supraveghere nu este competentă să supravegheze	Având în vedere existenţa unei singure

		de supraveghere îi revine competența să supravegheze operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare. Statele membre pot să stabilească dispoziții potrivit cărora autorităților sale de supraveghere nu le revine competența să supravegheze operațiunile de prelucrare ale altor autorități judiciare independente atunci când acestea acționează în exercițiul funcției lor judiciare.	operațiunile de prelucrare ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare.	Autorități de supraveghere în România, s-ar dubla dispozițiile Regulamentului 679/2016 (Art.55 alin. (3)) Precizăm faptul că traducerea în limba română este greșită; autoritățile naționale au au competența de a supraveghea operațiunile de prelucrare a datelor cu caracter personal ale instanțelor atunci când acestea acționează în exercițiul funcției lor judiciare. Pentru transpunerea corectă, în spiritul Directivei (UE) 680/2016 au fost analizate variantele lingvistice ale Directivei (UE) 680/2016 în următoarele limbi: engleză, franceză, germană, italiană și

				spaniolă.
258.	*Articolu l 46* Sarcini	(1) Fiecare stat membru garantează, pe teritoriul său, că autoritatea sa de supraveghere: (a) monitorizează și asigură respectarea prezentei directive și a măsurilor de punere în aplicare aferente acesteia;	Art. 52 (1) Autoritatea de supraveghere monitorizează și controlează sub aspectul legalității prelucrările de date cu caracter personal care intră sub incidența prezentei legi.	
259.	(b)	promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare;	(3) În acest scop, autoritatea de supraveghere îndeplinește sarcinile prevăzute la art. 57 alin. (1) lit. b), c) și t) din Regulamentul (UE) 2016/ 679, precum și următoarele:	
260.	(c)	oferă consiliere, în conformitate cu dreptul intern, parlamentului național, guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;	(3) În acest scop, autoritatea de supraveghere îndeplinește sarcinile prevăzute la art. 57 alin. (1) lit. b), c) și t) din Regulamentul (UE) 2016/ 679, precum și următoarele:	
261.	(d)	promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentei directive;	a) promovează acțiuni de conștientizare în rândurile operatorilor și ale persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezentei legi;	
262.	(e)	furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul prezentei directive și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;	b) furnizează informații, la cerere, oricărei persoane vizate în legătură cu exercitarea drepturilor sale în temeiul prezentei legi și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state membre în acest scop;	
263.	(f)	tratează plângerile depuse de o persoană vizată sau de un	c) primește plângerile depuse de o persoană vizată sau de un organism, o organizație sau o asociație, în	

		organism, o organizaţie sau o asociaţie, în conformitate cu articolul 55, investighează într-o măsură adecvată obiectul plângerii şi informează persoana care a depus plângerea cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;	conformitate cu art.55 sau cu art.57, investighează într-o măsură adecvată obiectul plângerii şi informează persoana care a depus plângerea cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;	
264.	(g)	verifică legalitatea prelucrării în conformitate cu articolul 17 şi informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul alineatului (3) al articolului respectiv sau la motivele pentru care nu a avut loc verificarea;	d) verifică legalitatea prelucrării în conformitate cu art.20 şi informează persoana vizată, într-un termen rezonabil, cu privire la rezultatul verificării în temeiul alin.(3) al art.20 sau cu privire la motivele pentru care nu a avut loc verificarea;	
265.	(h)	cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă reciproc asistenţă pentru a asigura consecvenţa aplicării şi respectării prezentei directive;	e) cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă reciproc asistenţă pentru a asigura consecvenţa aplicării şi respectării prezentei legi;	
266.	(i)	desfăşoară investigaţii privind aplicarea prezentei directive, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau autoritate publică;	f) desfăşoară investigaţii privind aplicarea prezentei legi, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau autoritate publică;	
267.	(j)	monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiilor şi comunicaţiilor;	g) monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiilor şi comunicaţiilor;	
268.	(k)	oferă consiliere cu privire la operaţiunile de prelucrare menţionate la articolul 28; şi	h) oferă consiliere cu privire la operaţiunile de prelucrare menţionate la articolele 33-34.	
269.	(l)	contribuie la activităţile comitetului.	(3) În acest scop, autoritatea de supraveghere îndeplineşte sarcinile prevăzute la art. 57 alin. (1) lit. b),	

			c) și t) din Regulamentul (UE) 2016/ 679, precum și următoarele:	
270.		2) Fiecare autoritate de supraveghere facilitează depunerea plângerilor menționate la alineatul (1) litera (f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii, care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.57 alin. (2))
271.		(3) Îndeplinirea sarcinilor fiecărei autorități de supraveghere este gratuită pentru persoana vizată și pentru responsabilul cu protecția datelor.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.57 alin. (3))
272.		(4) În cazul în care o cerere este în mod vădit nefondată sau excesivă, în special când este repetitivă, autoritatea de supraveghere poate percepe o taxă rezonabilă pe baza costurilor sale administrative sau poate refuza să îi dea curs. Obligația de a demonstra caracterul evident nefondat sau excesiv al cererii respective revine autorității de supraveghere.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.57 alin. (4))
273.	*Articolul 47*	(1) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de investigare efective. Respectivele competențe includ, cel	Art. 53 (1) În exercitarea competențelor de investigare, autoritatea de supraveghere are acces la toate datele cu caracter personal prelucrate de	Legea nr.102/2005

	Competențe	puțin, competența de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.	operator și persoana împuternicită de operator, precum și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.	
274.		(2) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe corective efective, cum ar fi, de exemplu: (a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la probabilitatea ca operațiunile de prelucrare preconizate să încalce dispozițiile adoptate în temeiul prezentei directive;	(2) Autorității de supraveghere îi revin 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 prezentei legi;	
275.	(b)	de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile adoptate în temeiul prezentei directive, specificând, după caz, modalitatea și termenul-limită pentru aceasta; în special dispunând rectificarea sau ștergerea datelor cu caracter personal, sau restricționarea prelucrării, în conformitate cu articolul 16;	b) de a dispune operatorului sau persoanei împuternicite de către operator să asigure conformitatea operațiunilor de prelucrare cu prevederile prezentei legi, specificând, după caz, modalitatea și termenul-limită pentru aceasta, în special dispunând rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării, în conformitate cu articolul 18;	
276.	(c)	de a impune o limitare temporară sau definitivă, inclusiv o interdicție, în ce privește prelucrarea.	c) de a dispune limitarea temporară sau definitivă ori interdicția prelucrărilor.	
277.		(3) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de	(3) Autoritatea de supraveghere oferă consiliere operatorului în conformitate cu procedura de consultare	

		consiliere efective pentru a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la articolul 28 și de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului sau, în conformitate cu dreptul său intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal.	prealabilă menționată la articolele 33-34 și emite avize, din proprie inițiativă sau la cerere, Parlamentului, Guvernului sau altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal.	
278.		(4) Exercitarea competențelor conferite autorității de supraveghere în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute de dreptul Uniunii și de dreptul intern în conformitate cu Carta.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.58 alin. (4))
279.		(5) Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revine competența de a aduce în atenția autorităților judiciare cazurile de încălcare a dispozițiilor adoptate în temeiul prezentei directive și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri judiciare, în scopul de a asigura respectarea dispozițiilor adoptate în temeiul prezentei directive.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.57 alin. (5))
280.	*Articolu*	Statele membre garantează că autoritățile competente instituie mecanisme eficiente de încurajare a denunțării confidențiale a cazurilor de încălcare a prezentei	Nu necesită transpunere	Legea nr.102/2005

	148 **Denunțarea cazurilor de încălcare**	directive.		
281.	*Articolul 149* **Rapoarte de activitate**	Fiecare autoritate de supraveghere întocmește un raport anual cu privire la activitățile sale, care poate include o listă a cazurilor de încălcare notificate și natura sancțiunilor aplicate. Rapoartele se transmit parlamentului național, guvernului și altor autorități desemnate de dreptul intern. Rapoartele se pune la dispoziția publicului, a Comisiei și a comitetului.	Nu necesită transpunere	Legea nr.102/2005
282.	***CAPITOLUL VII Cooperarea*** *Articolul 150* **Asistență reciprocă**	(1) Fiecare stat membru garantează că autoritățile sale de supraveghere își furnizează reciproc informațiile relevante și asistență pentru a pune în aplicare și a aplica prezenta directivă în mod consecvent și instituie măsuri de cooperare eficace între ele. Asistența reciprocă se referă, în special, la cereri de informații și măsuri de supraveghere, cum ar fi cereri în vederea efectuării de consultări, inspecții și investigații.	Art. 54 (1) Autoritatea de supraveghere cooperează cu instituții similare din străinătate și asigură reprezentarea în cadrul Comitetului European pentru Protecția Datelor. (2) Dispozițiile Legii nr.102/2005, cu modificările și completările ulterioare, referitoare la cooperarea Autorității Naționale de supraveghere a Prelucrării Datelor cu Caracter Personal cu instituții similare din străinătate, sunt aplicabile în mod corespunzător.	Legea nr.102/2005

	că			
283.		(2) Fiecare stat membru garantează luarea de către fiecare autoritate de supraveghere a tuturor măsurilor corespunzătoare necesare pentru a răspunde cererii unei alte autorități de supraveghere, fără întârziere și în cel mult o lună de la data primirii cererii. Astfel de măsuri pot include, în special, transmiterea informațiilor relevante privind desfășurarea unei investigații.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (2))
284.		(3) Cererile de asistență cuprind toate informațiile necesare, inclusiv scopul și motivele care stau la baza acesteia. Informațiile care fac obiectul schimbului se utilizează numai în scopul în care au fost solicitate	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (3))
285.		(4) O autoritate de supraveghere căreia i se adresează o cerere de asistență nu poate refuza să îi dea curs, cu excepția cazului în care: (a) nu are competență cu privire la obiectul cererii sau la măsurile pe care este solicitată să le execute; sau	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (4)lit.a)
286.	(b)	a da curs cererii ar încălca prezenta directivă sau dreptul Uniunii sau dreptul intern sub incidența căruia intră autoritatea de supraveghere care a primit cererea.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla

				dispozițiile Regulamentului 679/2016 (Art.61 alin. (4)lit.b)
287.		(5) Autoritatea de supraveghere căreia i s-a adresat cererea informează autoritatea de supraveghere care a transmis cererea cu privire la rezultate sau, după caz, la progresele înregistrate ori măsurile întreprinse pentru a răspunde cererii. În cazul unui refuz în temeiul alineatului (4), autoritatea de supraveghere căreia i s-a adresat cererea explică motivele de refuz.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (5)
288.		(6) Autoritățile de supraveghere cărora li s-a adresat o cerere furnizează, de regulă, informațiile solicitate de alte autorități de supraveghere prin mijloace electronice, utilizând un formular-standard.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (6)
289.		(7) Pentru acțiunile întreprinse în urma unei cereri de asistență reciprocă autoritățile de supraveghere cărora li s-a adresat o cerere nu percep taxă. Autoritățile de supraveghere pot conveni asupra unor compensații reciproce în cazul unor cheltuieli specifice rezultate în urma acordării de asistență reciprocă în situații excepționale.	Nu necesită transpunere	Având în vedere existența unei singure Autorități de supraveghere în România s-ar dubla dispozițiile Regulamentului 679/2016 (Art.61 alin. (7)

290.		(8) Comisia poate preciza, prin intermediul unor acte de punere în aplicare, forma și procedurile pentru asistența reciprocă menționată în prezentul articol, precum și modalitățile de schimb de informații prin mijloace electronice între autoritățile de supraveghere și între autoritățile de supraveghere și comitet. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 58 alineatul (2).	Nu necesită transpunere,	cade în sarcina COM
291.	*Articolul 51* **Sarcinile comitetului**	1) Comitetul instituit prin Regulamentul (UE) 2016/679 îndeplinește, în ceea ce privește prelucrarea care intră sub incidența prezentei directive, toate sarcinile următoare: (a) oferă Comisiei consiliere cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la orice propunere de modificare a prezentei directive;	Nu necesită transpunere	
292.	(b)	examinează, din proprie inițiativă, la cererea unuia dintre membrii săi sau la cererea Comisiei, orice chestiune referitoare la aplicarea prezentei directive și emite orientări, recomandări și bune practici pentru a încuraja aplicarea consecventă a prezentei directive;	Nu necesită transpunere	
293.	(c)	elaborează orientări destinate autorităților de	Nu necesită transpunere	

		supraveghere, referitoare la aplicarea măsurilor menționate la articolul 47 alineatele (1) și (3);		
294.	(d)	emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, pentru stabilirea cazurilor de încălcare a securității datelor cu caracter personal și pentru determinarea întârzierilor Nu necesită transpunere nejustificate menționate la articolul 30 alineatele (1) și (2), precum și pentru circumstanțele speciale în care un operator sau o persoană împuternicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal;	Nu necesită transpunere	
295.	(e)	emite orientări, recomandări și bune practici, în conformitate cu litera (b) de la prezentul alineat, în ceea ce privește circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor menționate la articolul 31 alineatul (1);	Nu necesită transpunere	
296.	(f)	revizuiește aplicarea practică a orientărilor, a recomandărilor și a bunelor practici menționate la literele (b) și (c);	Nu necesită transpunere	
297.	(g)	prezintă Comisiei un aviz pentru evaluarea caracterului adecvat al nivelului de protecție dintr-o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță, sau o organizație internațională, inclusiv pentru a evalua dacă o țară terță, un teritoriu, un sector determinat sau o organizație internațională nu mai asigură un nivel de protecție adecvat.	Nu necesită transpunere	

298.	(h)	promovează cooperarea şi schimbul eficient bilateral şi multilateral de informaţii şi cele mai bune practici între autorităţile de supraveghere;	Nu necesită transpunere	
299.	(i)	promovează programe comune de formare şi facilitează schimburile de personal între autorităţile de supraveghere şi, după caz, cu autorităţile de supraveghere ale ţărilor terţe sau cu organizaţiile internaţionale;	Nu necesită transpunere	
300.	(j)	promovează schimbul de cunoştinţe şi de documente privind dreptul şi practicile în materie de protecţie a datelor cu autorităţile de supraveghere a protecţiei datelor la nivel mondial.	Nu necesită transpunere	
301.		În ceea ce priveşte litera (g) de la primul paragraf, Comisia pune la dispoziţia comitetului toată documentaţia necesară, inclusiv corespondenţa purtată cu guvernul ţării terţe, al teritoriului respectiv sau cu sectorul specific din respectiva ţară terţă, sau cu organizaţia internaţională	Nu necesită transpunere	
302.		(2) În cazul în care Comisia solicită consiliere din partea comitetului, aceasta poate indica un termen limită, ţinând seama de caracterul urgent al chestiunii.	Nu necesită transpunere	
303.		(3) Comitetul îşi transmite avizele, orientările, recomandările şi bunele practici Comisiei şi comitetului menţionat la articolul 58 alineatul (1) şi le publică.	Nu necesită transpunere	

304.		(4) Comisia informează comitetul cu privire la măsurile pe care le-a luat în urma avizelor, orientărilor, recomandărilor şi bunelor practici emise de comitet.	Nu necesită transpunere	
305.	***CAPITOLUL VIII Căi de atac, răspundere şi sancţiuni*** *Articolul 52* **Dreptul de a depune o plângere în o autoritate de supraveghere**	1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, statele membre garantează oricărei persoane vizate dreptul de a depune o plângere la o singură autoritate de supraveghere, în cazul în care persoana vizată consideră că prelucrarea datelor cu caracter personal care o vizează încalcă dispoziţiile adoptate în temeiul prezentei directive.	Art.55 (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.	

306.		(2) Statele membre garantează că, în cazul în care plângerea nu este depusă la autoritatea de supraveghere competentă în temeiul articolului 45 alineatul (1), autoritatea de supraveghere la care a fost depusă plângerea o transmite autorității de supraveghere competente, fără întârzieri nejustificate. Persoana vizată este informată cu privire la transmitere.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor
307.		(3) Statele membre garantează că autoritatea de supraveghere la care s-a depus plângerea oferă, la cerere, asistență suplimentară persoanei vizate.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor
308.		(4) Persoana vizată este informată de către autoritatea de supraveghere competentă cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a exercita o cale de atac judiciară în conformitate cu articolul 53.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor
309.	*Articolul 53* **Dreptul la o cale de atac judiciară**	(1) Fără a aduce atingere oricăror alte căi de atac administrative sau extrajudiciare, statele membre dispun că o persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor

	eficientă împotriva unei autorități de supraveghere			
310.		(2) Fără a aduce atingere oricăror alte căi de atac administrative sau extrajudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere competentă în conformitate cu articolul 45 alineatul (1) nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în conformitate cu articolul 52.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor
311.		(3) Statele membre garantează că acțiunile împotriva unei autorități de supraveghere sunt introduse în fața instanțelor din statul membru în care este stabilită autoritatea de supraveghere.	Nu necesită transpunere	Regulamentul General de Protecție a Datelor
312.	*Articolul 54* **Dreptul la o cale**	Fără a aduce atingere vreunei căi de atac administrative sau extrajudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în conformitate cu articolul 52, statele membre garantează persoanei vizate dreptul la exercitarea unei căi de atac	Art.56 Fără a se aduce atingere posibilității de a se adresa cu plângere autorității de supraveghere, persoanele vizate au dreptul de a se adresa instanței pentru apărarea oricăror drepturi garantate de prezenta lege, care le-au fost încălcate.	

	de atac judiciară eficientă împotriva unui operator sau a unei persoane împuternicite de către operator	judiciare eficiente în cazul în care aceasta consideră că, prin prelucrarea datelor sale cu caracter personal cu nerespectarea dispozițiilor adoptate în temeiul prezentei directive, au fost încălcate drepturile care îi revin în conformitate cu dispozițiile respective.		
313.	*Articolul 55* **Reprezentarea persoanelor vizate**	În conformitate cu dreptul intern procedural, statele membre garantează oricărei persoane vizate dreptul de a mandata un organism, o organizație sau o asociație, care nu are scop lucrativ și care a fost constituită în mod corespunzător în conformitate cu dreptul intern, ale cărei obiective statutare sunt de interes public și care este activă în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său și să exercite în numele său drepturile menționate la articolele 52, 53 și 54.	Art.57 În scopul apărării drepturilor sale, persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație, care nu are scop lucrativ, constituită în condițiile legii, ale cărei obiective statutare sunt de interes public și care este activă în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor cu caracter personal, să depună plângerea în numele său și să exercite în numele său drepturile prevăzute de prezenta lege.	

314.	*Articolul 56* **Dreptul la despăgubiri**	Statele membre garantează oricărei persoane care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni de prelucrare ilegale sau a oricărei acțiuni care încalcă dispozițiile adoptate în temeiul prezentei directive dreptul de a obține despăgubiri, în temeiul dreptului intern, pentru prejudiciul cauzat de operator sau de o altă autoritate competentă.	Art.58 (1) Orice persoană care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni de prelucrare ilegale sau a oricărei acțiuni care încalcă dispozițiile prezentei legi are dreptul de a obține despăgubiri, în condițiile legii, pentru prejudiciul cauzat de operator sau de o altă autoritate competentă. (2) Dacă, în situația prelucrărilor automate de date cu caracter personal, nu este posibilă determinarea operatorului de date cu caracter personal care a cauzat prejudiciul, fiecare dintre operatorii de date cu caracter personal implicați în operațiunea de prelucrare este considerat a fi responsabil.	
315.	*Articolul 57* **Sancțiuni**	Statele membre definesc normele privind sancțiunile aplicabile în cazurile de încălcare a dispozițiilor adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive.	Art.59 (1) Constituie contravenție încălcarea de către operator sau, după caz, de către persoana împuternicită de operator, a obligațiilor acestora în conformitate cu articolele 11 și 22-42 din prezenta lege. (2) Constituie contravenție încălcarea de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor art. 10 din prezenta lege. (3) Contravențiile prevăzute la alin. (1) și (2) se sancționează cu amendă de până la 100.000 lei. (4) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a principiilor de bază pentru prelucrare, prevăzute la art.5. (5) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a drepturilor persoanelor vizate în conformitate cu articolele 12 – 21. (6) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor referitoare la transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu articolele 44 – 49.	De discutat

			(7) Constituie contravenție încălcarea, de către operator sau, după caz, de către persoana împuternicită de operator, a dispozițiilor emise de către autoritatea de supraveghere în temeiul art.53 alin.(2) sau neacordarea accesului autorității de supraveghere, prin încălcarea dispozițiilor art.53 alin.(1). (8) Contravențiile prevăzute la alin. (4)–(7) se sancționează cu amendă de până la 200.000 lei. Art.60 (1) În cazul constatării încălcării prevederilor prezentei legi de către operator sau, după caz, de către persoana împuternicită de operator, autoritatea de supraveghere încheie un proces-verbal de constatare și sancționare a contravenției prin care se aplică sancțiunea mustrării, conform art.58 alin.(2) lit. b) din Regulamentul general privind protecția datelor și la care anexează un plan de remediere. (2) Termenul de remediere se stabilește în funcție de riscurile asociate prelucrării, precum și demersurile necesar a fi îndeplinite pentru asigurarea conformității prelucrării. (3) În termen de 10 zile de la data expirării termenului de remediere, autoritatea de supraveghere poate să reia controlul. (4) În cazul în care operatorul sau, după caz, persoana împuternicită de operator, constată că nu poate îndeplini în termenul stabilit, din motive întemeiate, o parte din măsurile dispuse prin planul de remediere, notifică autoritatea de supraveghere cu privire la acest aspect cu cel puțin 10 zile înainte de expirarea termenului, putând solicita totodată prelungirea termenului inițial. (5) Autoritatea de supraveghere analizează solicitarea de prelungire a termenului și comunică răspunsul operatorului sau, după caz, persoanei împuternicite de către operator, în termen de 7 zile de la primirea cererii. (6) Dacă autoritatea de supraveghere consideră	

			justificată cererea operatorului sau, după caz, a persoanei împuternicite de către operator, poate prelungi termenul de remediere cu până la 30 de zile. În caz contrar, se aplică prevederile de la alin.(3). (7) Responsabilitatea îndeplinirii măsurilor de remediere revine operatorului sau, după caz, persoanei împuternicite de operator care, potrivit legii, poartă răspunderea contravențională pentru faptele constatate. (8) Modelul planului de remediere care se anexează la procesul-verbal de constatare și sancționare a contravenției este prevăzut în Anexa la prezenta lege. Art.61 Dacă, la reluarea controlului, autoritatea 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.	
316.	*CAPITOLUL IX Acte de punere în aplicare* *Articolul 58*	(1) Comisia este asistată de comitetul înființat prin articolul 93 din Regulamentul (UE) 2016/679. Acesta reprezintă un comitet în sensul Regulamentului (UE) nr. 182/2011.	Nu necesită transpunere	Sarcina COM

	Procedura comitetului			
317.		(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011. (3) Atunci când se face trimitere la prezentul alineat, se aplică articolul 8 din Regulamentul (UE) nr. 182/2011 coroborat cu articolul 5 din același regulament.	Nu necesită transpunere	
318.	***CAPITOLUL X Dispoziții finale*** *Articolul 59* **Abrogarea Deciziei-cadru 2008/977/JAI**	(1) Decizia-cadru 2008/977/JAI se abrogă începând cu 6 mai 2018. (2) Trimiterile la decizia abrogată menționată la alineatul (1) se interpretează ca trimiteri la prezenta directivă.	Art. 62 La data intrării în vigoare a prezentei legi, Legea nr.238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, republicată în Monitorul Oficial al României, Partea I, nr. 474 din 12 iulie 2012 se abrogă.	

319.	*Articolul 60* **Actele Uniunii aflate deja în vigoare**	Dispozițiile specifice referitoare la protecția datelor cu caracter personal din actele juridice ale Uniunii care au intrat în vigoare până la 6 mai 2016 în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care reglementează prelucrarea între statele membre și accesul autorităților desemnate ale statelor membre la sistemele de informații instituite în temeiul tratatelor și care intră sub incidența prezentei directive nu sunt afectate.	Nu necesită transpunere	
320.	*Articolul 61* **Relația cu acordurile internaționale încheiate anterior în domeniul cooperării judiciar**	Acordurile internaționale care implică transferul de date cu caracter personal către țări terțe sau organizații internaționale, care au fost încheiate de statele membre înainte de 6 mai 2016 și sunt aplicabile înainte de 6 mai 2016 și care sunt în conformitate cu dreptul Uniunii, rămân în vigoare până la modificarea, înlocuirea sau revocarea lor.	Nu necesită transpunere	

	e în materie penală şi al cooperării poliţieneşti			
321.	*Articolul 62* **Rapoartele Comisiei**	(1) Până la 6 mai 2022 şi, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European şi Consiliului, un raport privind evaluarea şi revizuirea prezentei directive. Rapoartele sunt făcute publice. (	Nu necesită transpunere	Sarcina COM
322.		2) În contextul evaluărilor şi revizuirilor menţionate la alineatul (1), Comisia examinează, în special, aplicarea şi funcţionarea capitolului V privind transferul datelor cu caracter personal către ţări terţe sau organizaţii internaţionale, acordând o atenţie deosebită deciziilor adoptate în temeiul articolului 36 alineatul (3) şi al articolului 39.	Nu necesită transpunere	Sarcina COM
323.		(3) În scopul alineatelor (1) şi (2), Comisia poate solicita informaţii de la statele membre şi de la	Nu necesită transpunere	Sarcina COM

		autoritățile de supraveghere.		
324.		(4) La efectuarea evaluărilor și revizuirilor menționate la alineatele (1) și (2), Comisia ia în considerare pozițiile și concluziile Parlamentului European, ale Consiliului și ale altor organisme și surse relevante.	Nu necesită transpunere	Sarcina COM
325.		(5) Comisia transmite, dacă este necesar, propuneri corespunzătoare în vederea modificării prezentei directive, în special ținând seama de evoluțiile din domeniul tehnologiei informației și având în vedere progresele societății informaționale.	Nu necesită transpunere	Sarcina COM
326.		(6) Până la 6 mai 2019, Comisia revizuiește celelalte acte adoptate de Uniune care reglementează prelucrarea de către autoritățile competente în scopurile prevăzute la articolul 1 alineatul (1), inclusiv actele menționate la articolul 60, pentru a evalua necesitatea de a le alinia la prezenta directivă și prezintă, după caz, propunerile necesare de modificare a actelor respective pentru a asigura o abordare uniformă privind protecția datelor cu caracter personal care intră în domeniul de aplicare al prezentei directive.	Nu necesită transpunere	Sarcina COM
327.	*Articolu*	(1) Statele membre adoptă și publică, până la 6 mai 2018, actele cu putere de lege și actele administrative	Nu necesită transpunere	

	163 **Transpunerea**	necesare pentru a se conforma prezentei directive. Statele membre notifică de îndată Comisiei textele acestor dispoziții. Statele membre aplică aceste dispoziții începând cu 6 mai 2018. Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.		
328.		(2) Prin derogare de la alineatul (1), un stat membru poate prevedea că, în mod excepțional, în cazul în care acest lucru implică eforturi disproporționate, sistemele de prelucrare automată instituite înainte de 6 mai 2016 sunt aduse în conformitate cu articolul 25 alineatul (1) până la 6 mai 2023.	Nu necesită transpunere	
329.		(3) Prin derogare de la alineatele (1) și (2) din prezentul articol, un stat membru poate aduce, în circumstanțe excepționale, în conformitate cu articolul 25 alineatul (1), un sistem de prelucrare automată, în conformitate cu alineatul (2) din prezentul articol, într-un termen determinat, după încheierea perioadei menționate la alineatul (2) din prezentul articol, dacă, în caz contrar, s-ar provoca dificultăți majore pentru funcționarea respectivului sistem de prelucrare automată. Statul membru respectiv notifică Comisiei motivele respectivelor dificultăți majore și motivele pe care se întemeiază termenul determinat în care statul membru	Nu necesită transpunere	

		aduce în conformitate cu articolul 25 alineatul (1) respectivul sistem de prelucrare automată. Termenul determinat nu depășește în niciun caz 6 mai 2026.		
330.		(4) Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.	Nu necesită transpunere	
331.	*Articolul 64* **Intrarea în vigoare**	Prezenta directivă intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.	Nu necesită transpunere.	
332.			Art. 63 Prevederile art.59 intră în vigoare la 30 de zile de la data publicării prezentei legi în Monitorul Oficial al României, Partea I.	