ATELIERUL NR. 4

1. Securitatea și confidentialitatea datelor cu caracter personal
2. Transferul datelor cu caracter personal în afara Uniunii Europene
3. Responsabilul cu protecția datelor. DPIA
4. Sancțiuni

1. Securitatea și confidențialitatea datelor cu caracter personal

La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

Operatorul și persoana împuternicită de acesta trebuie să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

(a) pseudonimizarea și criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

(d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

1.2. Încălcarea securității datelor (Data Breach)

Art. 4 alin. (12) din Regulament o definește după cum urmează: *încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.*

Încălcările pot fi clasificate conform următoarelor trei principii:

- *încălcarea confidențialității* - în cazul în care există o dezvăluire neautorizată sau accidentală sau acces la datele personale;

- *încălcarea integrității* - în cazul în care există o modificare neautorizată sau accidentală a datelor cu caracter personal;

- încălcare a disponibilității - în cazul în care există o pierdere accidentală sau neautorizată a accesului la sau distrugerea datelor personale, de exemplu, când datele au fost șterse fie accidental, fie de către o persoană neautorizată.

Notificarea autoritatii și a personei vizate

Potrivit art. 33 din Regulament, intitulat ***Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal,*** *în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta.*

Notificarea autorității poate fi făcută și în etape, respectiv, în termenul inițial de 72 de ore, să aibă loc informarea autorității cu privire la existența breșei de securitate, oferindu-se o parte dintre informațiile deținute de către operator la acel moment, iar ulterior, operatorul să revină cu una sau mai multe completări, pe măsură ce acesta culege și el informațiile legate de incident.

În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

Producerea unei încălcări a securității datelor are drept cauză faptul că operatorul nu a luat toate măsurile tehnice și organizatorice necesare pentru a asigura securitatea acestora.

Ca urmare, acesta are obligația de a revizui măsurile luate, de a le îmbunătăți și, totodată, de a verifica eficiența lor.

Astfel de măsuri pot să constea în (re)instruirea periodică a angajaților - mai ales în situația în care breșa este urmare a conduitei unui angajat, achiziționarea de sisteme de securitate mai performante, utilizarea unor tehnici de criptare mai moderne/mai actuale, utilizarea pseudonimizării, limitarea accesului la unele categorii de date, introducerea obligativității schimbării parolei unice de acces la date la intervale de timp regulate/mai scurte, etc.

Securitatea și confidențialitatea sunt strâns legate între ele. Măsuri de securitate sunt menite să asigure confidențialitatea datelor.

2. Transferul datelor cu caracter personal în afara Uniunii Europene

Regulamentul ofera mai multe instrumente pentru încadrarea transferurilor de date din UE într-o țară terță:

- situatia în care o țară terță este declarată că oferind un nivel adecvat de protecție printr-o decizie a Comisiei Europene („decizie privind caracterul adecvat al nivelului de protecție”), ceea ce înseamnă că se pot transfera date cu o altă societate în acea țară terță fără ca exportatorul datelor să aibă obligația de a asigura garanții suplimentare sau să fie supus unor condiții suplimentare. În acest caz, transferurile într-o țară terță cu „un caracter adecvat al nivelului de protecție” va fi asimilată unei transmiteri de date în interiorul UE.

- daca nu există o decizie privind caracterul adecvat al nivelului de protecție, transferul se poate face prin asigurarea unor garanții adecvate și cu condiția ca persoanele fizice să beneficieze de drepturi opozabile și de căi de atac eficace. Printre asemenea garanții adecvate se numără:

- în cazul unui grup de întreprinderi sau de societăți implicat într-o activitate economică comună, societățile pot transfera datele cu caracter personal pe baza unor reguli corporatiste obligatorii;
acorduri contractuale cu destinatarul datelor cu caracter personal, folosind, de exemplu, clauzele contractuale standard aprobate de Comisia Europeană;

- aderarea la un cod de conduită sau la un mecanism de certificare, precum și obținerea unor angajamente obligatorii și executorii din partea destinatarului de a aplica garanții adecvate pentru protecția datelor transferate.

- daca transferul de date cu caracter personal se face într-o țară terță care nu face obiectul unei decizii privind caracterul adecvat al nivelului de protecție și dacă lipsesc garanțiile adecvate, transferul se poate realiza pe baza mai multor derogări pentru situații specifice, de exemplu, în cazul în care o persoană fizică și-a exprimat în mod explicit acordul cu privire la transferul propus după ce a primit toate informațiile necesare privind riscurile asociate transferului, daca transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță sau pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;

3. Responsabilul cu protecția datelor. DPIA

Responsabilul cu protecția datelor reprezintă o persoană care are atribuții de supraveghere a modului în care operatorul sau persoana împuternicită își indeplinește obligațiile care îi revin în temeiul Regulamentului.

3.1. Situații când este necesară numirea unui responsabil cu protecția datelor

Există situații în care este obligatorie desemnarea un responsabil cu protecția datelor. Aceste situații sunt prevăzute de art. 37 din Regulament:

(a) când prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

(b) când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau

(c) când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni.

Potrivit art. 37 alin. (5) responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile stabilite de Regulament.

DPO poate proveni din rândurile angajaților operatorului sau poate fi contractat extern.

3.2. Funcția și sarcinile responsabilului cu protecția datelor

Art. 38 intitulat *Funcția responsabilului cu protecția datelor* face următoarele mențiuni:

Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

Exemple de obligații care îi revin în acest sens operatorului și persoanei împuternicite:

- responsabilul este invitat să participe în mod regulat la ședințele conducerii la nivel înalt și la nivel mediu;

- prezența responsabilului este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor; toate informațiile relevante trebuie să îi fie trimise în timp util acestuia;

- avizului responsabilului trebuie să i se acorde o importanță deosebită; în caz de dezacord, grupul de lucru recomandă, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul responsabilului;

- responsabilul trebuie să fie consultat de îndată ce a avut loc o încalcare a securității datelor sau un alt incident.

Responsabilul cu protecția datelor are nevoie de:

- sprijin activ al funcției responsabilului din partea managementului superior;

- timp suficient pentru îndeplinirea sarcinilor;

- sprijin în ceea ce privește resursele financiare și infrastructura;

- informarea tuturor angajaților, astfel încât să se asigure că este cunoscută existența și funcționarea responsabilului;

- pregatire continuă, pentru ca acesta să fie la curent cu evoluțiile în domeniu.

Independența responsabilului cu protecția datelor

Art. 38 alin. (3), ***Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor***

sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

Potrivit art 38. alin. (5), ***Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.***

Obligația de confidențialitate este una dintre cele mai importante obligații care îi revin acestuia. Această obligație privește atât datele cu caracter personal la care are acces în vederea îndeplinirii atribuțiilor care îi revin - de regulă, este vorba despre toate categoriile de date prelucrate la nivelul organizației – cât și arhitectura internă a sistemului de prelucrare al acestora: măsurile tehnice și organizatorice luate la nivel intern pentru a se asigura conformarea cu Regulamentul, politicile - evident, cu excepția acelora care trebuie să aibă un caracter public.

Obligația de confidențialitate există indiferent dacă responsabilul este un angajat al operatorului sau al persoanei împuternicite, ori dacă el este numit extern.

Art. 38 alin. (6), a- conflictul de interese: Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

3.3. Sarcinile responsabilului cu protecția datelor

Art. 39 din Regulament cuprinde sarcinile care îi revin responsabilului cu protecția datelor:

Astfel, responsabilul cu protecția datelor are, cel puțin, următoarele sarcini:

(a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul Regulamentului și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării Regulamentului, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator 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;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;

(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

3.4 Evaluarea impactului asupra protecției datelor DPIA (DATA PROTECTION IMPACT ASSESSMENT)

Evaluarea impactului asupra protecției datelor cu caracter personal – DPIA (data protection impact assessment) este o operațiune anterioară prelucrării datelor cu caracter personal, prin care operatorii fac o analiză completă și concretă atât a datelor pe care urmează să le prelucreze, cât și a condițiilor în care se va face prelucrarea, pentru a vedea care sunt cele mai bune metode de prelucrare a datelor, de respectare a principiilor Regulamentului, a drepturilor persoanelor vizate și, totodată, de protejare a acestor date.

Ea le permite operatorilor să identifice măsurile optime de securitate.

Reglementarea procedurii se regăsește în art. 35 din Regulament, care prevede:

(1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

Grupul de lucru art. 29 apreciază că o DPIA **poate fi utilă, de asemenea, pentru a evalua impactul unui produs al tehnologiei asupra protecției datelor**, de exemplu, al unui element de hardware sau software, atunci când este posibil ca acesta să fie utilizat de diferiți operatori de date pentru a efectua diferite operațiuni de prelucrare.

Art. 35 alin. 3 menționează că evaluarea impactului asupra protecției datelor menționată la alin. 1 se impune **mai ales** în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10;

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

ANASPDCP a emis ***Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal***,[1] care cuprinde o listă a operațiunilor pentru care este necesară efectuarea evaluării:

a) prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b) prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;

c) prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, pieţe, parcuri sau alte asemenea spaţii;

d) prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;

e) prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;

f) prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);

g) prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

---

[1] Publicată în Monitorul Oficial al României nr. 919 din 31 octombrie 2018

Grupul de lucru, în Ghidul pe care l-a elaborat, referitor la *Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679,* a făcut trimitere la mai multe exemple cu privire la modul în care ar trebui să fie utilizate criteriile, pentru a stabili dacă o anumită operațiune de prelucrare necesită sau nu o DPIA:

1. un spital care prelucrează datele genetice și de sănătate ale pacienților; sunt astfel prelucrate date sensibile sau foarte personale, date referitoare la persoane vizate vulnerabile și este o prelucrare la scară largă;

2. utilizarea unui sistem de camere pentru a monitoriza comportamentul de conducere pe autostrăzi; operatorul intenționează să utilizeze un sistem inteligent de analiză video pentru a identifica autoturismele și pentru a recunoaște în mod automat plăcuțele de înmatriculare. În acest caz are loc o monitorizare sistematică și utilizarea inovatoare sau aplicarea unor soluții tehnologice sau organizaționale;

3. colectarea de date personale de pe platformele de comunicare pentru generarea de profiluri; în acest caz are loc o evaluare sau punctare, datele sunt prelucrate la scară largă, corelarea sau combinarea unor seturi de date; sunt date sensibile sau foarte personale.

3.5. Conținutul unui studiu de impact

DPIA trebuie să cuprindă:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

4. Sancțiuni

Încălcarea Regulamentului poate duce la aplicarea de amenzi administrative și de măsuri corective.

Art. 83 din Regulament face trimitere la condițiile generale pentru impunerea amenzilor administrative: *Fiecare autoritate de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările obligațiilor stabilite de Regulament este, în fiecare caz, eficace, proporțională și disuasivă.*

Criterii pentru aplicarea amenzilor:

(a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

(b) dacă încălcarea a fost comisă intenționat sau din neglijență;

(c) orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

(d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia;

(e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

(f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;

(g) categoriile de date cu caracter personal afectate de încălcare;

(h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

(i) în cazul în care măsurile menționate la art. 58 alin. (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;

(j) aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

(k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

În ceea ce privește **cuantumul amenzilor,** Regulamentul prevede următoarele categorii de amenzi, cu două praguri distincte:

1. amenzi administrative de până la 10.000.000 euro sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare atunci când încălcarea vizează:

(a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu art. 8 – care reglementează condițiile aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale, art. 11 – prelucrarea care nu necesită identificare, art. 25-39 – care privesc sarcinile operatorului, ale persoanei împuternicite și ale responsabilului cu protecția datelor, respectiv art. 42 și 43 – care privesc aspecte legate de certificare;

(b) obligațiile organismului de certificare;

(c) obligațiile organismului de monitorizare.

2. amenzi administrative de până la 20.000.000 euro sau, în cazul unei întreprinderi, de până la 4% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare atunci când încălcarea vizează:

(a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu art. 5, 6, 7 și 9;

(b) drepturile persoanelor vizate în conformitate cu art. 12-22;

(c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu art. 44-49;

(d) orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX;

(e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către autoritatea de supraveghere în temeiul art. 58 alin. (2), sau neacordarea accesului, încălcând art. 58 alin.(1).

În plus, se mai arată la art. 83 alin. (6) că, aceeași amendă administrativă se aplică și pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu art. 58 alin. (2).

Toate aceste amenzi pot fi aplicate în cazul operatorilor persoane private.

În ceea ce privește situația operatorilor persoane de drept public, Regulamentul menționează că *fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv.*

Potrivit art. 58 alin. (2), autoritățile naționale pot impune următoarele măsuri corective:

(a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile Regulamentului;

(b) de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile Regulamentului;

(c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul Regulamentului;

(d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile Regulamentului, specificând, după caz, modalitatea și termenul-limită pentru aceasta;

(e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;

(f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;

(g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul art. 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu art. 17 alin. (2) și cu art. 19;

(h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;

(i) de a impune amenzi administrative în conformitate cu art. 83, în completarea sau în locul măsurilor menționate mai sus, în funcție de circumstanțele fiecărui caz în parte;

(j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională.

Autoritatea are posibilitatea de a dispune una sau mai multe măsuri corective pentru încălcarea Regulamentului, urmărind totodată conformarea operatorului sau a persoanei împuternicite la măsurile dispuse.

În acest sens, ANSPDCP utilizează planul de remediere – o anexă la procesul-verbal de constatare şi sancţionare a contravenţiei[2], prin care autoritatea stabileşte măsurile corective care se impun şi un termen de remediere, termen care poate fi de cel mult 90 zile de la data comunicării procesului-verbal.

[2] Modelul se regăsește în anexa la Legea nr. 190/2018.