****

**Linii directorii privind prelucrarea**

**datelor personale în domeniul aplicării legii**

**Conținut**

Introducere

A. Cadrul legal

i. Legislația Republicii Moldova

ii. Legislația europeană

B. Conținutul recomandărilor

1. Domeniul de aplicare

2. Aplicarea principiilor de bază privind prelucrarea datelor

3. Utilizarea legală a datelor personale

4. Deosebirea dintre diferiți subiecți de date și diferite date

 i. Subiecții de date

 ii. Categorii de date

 iii. Prelucrarea datelor sensibile

5. Păstrarea datelor

6. Informația furnizată persoanelor

7. Drepturile subiectului de date

8. Fișiere jurnal

9. Transferurile internaționale

10. Responsabilul de protecția datelor (DPO)

**Introducere**

Textul care urmează trebuie mai degrabă considerat un set de recomandări sau linii directorii decât un cod de conduită care, de fapt, nu este un instrument aplicabil și adecvat implementării legislației în cauză.

Scopul acestor recomandări este de a evidenția problemele cele mai importante care pot apărea în utilizarea datelor personale în domeniul polițienesc, a scoate în evidență elementele cheie care trebuie luate în seamă în acest context și de a furniza niște linii directorii practice speciale. Conținutul acestor linii directorii se poate aplica atât datelor pe suport de hârtie, cât și celor electronice (ținând cont de faptul că protecția persoanelor fizice trebuie să fie neutră din punct de vedere tehnologic și nu ar trebui să depindă̆ de tehnicile utilizate, astfel cum este stipulat la considerentul 18 al Directivei (UE) 2016/680).

Obiectul Directivei (UE) 2016/680 și al Capitolului VII al Proiectului de lege privind protecția datelor cu caracter personal în constituie reglementarea prelucrării datelor de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv protecția împotriva și prevenirea amenințărilor la adresa ordinii publice cu respectarea caracterului special al acestor activități. Cu alte cuvinte, această legislație special este menită să garanteze că la utilizarea datelor de către poliție s-a asigurat un echilibru între obiectivele de bază de interes public și respectul pentru drepturile persoanelor la viață privată și protecția datelor.

**A. Cadrul legal**

Legislația Republicii Moldova

Legea privind protecția datelor cu caracter personal (traducerea neoficială a Proiectului de lege adoptat de Parlament în prima lectură la data de 30.11.2018) – „Proiectul de lege”

Legea cu privire la Procuratură (din 25 februarie 2016)

Legea nr. 320 din 27.12.2012 cu privire la activitatea poliției și statul polițistului

Legea nr 333-XVI din 10.11.2006 privind statutul ofițerului de urmărire penală

Însă pot fi relevante și alte acte legislative, cum ar fi Codul de procedură penală (nr. 122 din 14.03.2003) și Legea privind activitatea special de investigații (nr. 59 din 29.03.2012).

Legislația europeană

Directiva (EU) 2016/680 a Parlamentului european și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

**B. Conținutul recomandărilor**

1. Domeniul de aplicare

Pentru a face mai clar domeniul de aplicare al obiectului acestei legislații speciale, trebuie reiterate considerentul 12 al Directivei (EU) 2016/680: *„Activitățile desfășurate de politie sau de alte autorități de aplicare a legii, inclusiv activitățile polițienești desfășurate fără̆ a cunoaște dinainte dacă un incident constituie o infracțiune, se concentrează̆ în principal asupra prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor. Activitățile respective pot include, de asemenea, exercitarea autorității prin aplicarea unor masuri coercitive, precum activitățile polițienești desfășurate cu ocazia unor manifestații, evenimente sportive majore și revolte. De asemenea, activitățile menționate includ menținerea legii și ordinii ca atribuții ale poliției sau ale altor autorități de aplicare a legii atunci când aceasta se impune pentru a se asigura protecția împotriva amenințărilor la adresa securității publice și la adresa intereselor fundamentale ale societății protejate prin lege și pentru prevenirea acestor amenințări, care pot conduce la o infracțiune.”* Spre deosebire de aceasta, prevederile legislației din domeniul de aplicare a legii nu se aplică activităților ce țin de securitatea națională și, prin urmare, activitățile desfășurate de agențiile sau unitățile ce se ocupă cu asigurarea securității naționale, cum ar fi agențiile/serviciile de Informații.

O legătură strânsă cu domeniul de aplicare al acestei legislații are și desemnate autorităților competente, autoritățile care sunt împuternicite să desfășoare activitățile sus menționate și cărora le este încredințată îndeplinirea acestor atribuții publice. Este important de identificat autoritatea competentă, întrucât cel mai probabil, aceste autorități vor asuma rolul de operator sau cel puțin operator asociat în sensul legislației privind protecția datelor. În acest context, orice autoritate publică cu competențe de investigare și/sau urmărire penală,de a impune pedepse precum și orice altă organizație (cum ar fi o companie privată/un contractant – dacă aceasta se permite în sistemul juridic național – de ex., penitenciar privat), împuternicită prin lege să exercite aceste competențe într-o modalitate în care le oferă controlul asupra datelor, întrucât un operator de date, spre deosebire de o persoană împuternicită de operator, trebuie considerată drept o autoritate competentă. Ulterior, această definiție trebuie să includă poliția, instanțele de judecată, instituțiile penitenciare și orice altă persoană (sau instituție/agenție) care are funcții statutare pentru oricare din scopurile de aplicare a legii precum și organele de ocrotire a legii ca și organe de urmărire penală.

2. Aplicarea principiilor de bază pentru protecția datelor

Principiile de bază pentru protecț a datelor trebuie respectate la prelucrarea datelor în scopurile de aplicare a legii. De fapt, ele trebuie luate în considerare chiar și în mod implicit (privacy by default) și incorporate începând din momentul conceperii sistemelor informaționale care prelucrează date în domeniul aplicării legii (privacy by design). Cu atât mai mult că colectarea și utilizarea datelor personale în scopul aplicării legii constituie o ingerință în dreptul la viață privată și protecția datelor și, ca atare, ea trebuie să se bazeze pe lege (o lege care trebuie să fie clară, previzibilă și accesibilă), să urmărească un scop legitim și să se limiteze la ceea ce este necesar și proporțional pentru a atinge acest scop legitim.

În acest sens, toate operațiunile de prelucrare a datelor trebuie să respecte principiile de necesitate, proporționalitate și limitare legată de scop. Cu alte cuvinte, prelucrarea datelor personale în cadrul activităților generale ale poliției trebuie bazată pe scopuri predefinite, specifice, clare, explicite și legitime stabilite în lege, ea trebuie să fie necesară și proporțională cu aceste scopuri legitime. Aceasta presupune că ea trebuie să constituie un mod vizat și proporțional de realizare a scopurilor. Temeiul legal nu va fi aplicabil, dacă scopul poate fi realizat în mod rezonabil prin alte metode mau puțin intrusive. Mai mult, datele personale nu trebuie prelucrate într-un mod incompatibil cu acele scopuri. Prelucrarea datelor trebuie efectuată într-o manieră legală, echitabilă și transparentă. Dadele personale prelucrate de către poliție mai trebuie să fie adecvate, relevante și neexcesive în raport cu scopurile.

În cele din urmă, ele trebuie să fie exacte, actualizate pentru a asigura cea mai înaltă calitate posibilă a datelor. Trebuie întreprins orice pas rezonabil pentru a asigura că datele inexacte, luând în considerare scopul de aplicare a legii pentru care ele se prelucrează, se șterg sau e rectifică fără întârziere.

3. Utilizarea legală a datelor personale

Primul pas spre buna implementare a legislației privind protecția datelor este de a stabili în mod clar identitatea operatorului. Dacă este cazul operatorilor asociați și/sau există o persoană împuternicită de operator, ei trebuie, de asemenea stabiliți. În majoritatea cazurilor poliția va fi, cu siguranță, unul din operatori în domeniul aplicării legii.

În al doilea rând, trebuie asigurată legalitatea procesului. Pentru a face aceasta, colectarea și utilizarea datelor personale în scopurile poliției trebuie prevăzută de lege și trebuie limitată la ceea ce este necesar și proporțional în vederea prevenirii unui pericol real sau prevenirii, investigării și urmării penale a unei anumite infracțiuni și orice excepție la această prevedere trebuie să facă obiectul unei legi naționale speciale. Mai concret, orice excepție trebuie inclusă într-o lege națională (legea în cauză trebuie să fie publică, deschisă și transparentă și, în afară de aceasta, destul de detaliată), nu trebuie descrisă în termeni generali și trebuie să constituie o măsură necesară și proporțională într-o societate democratică, servind unui scop bine definit. Scopul aplicării excepțiilor de către poliție trebuie limitat la cazurile în care neaplicarea lor ar pune în pericol îndeplinirea sarcinilor poliției sau ar periclita acțiunile întreprinse în scopurile care cad sub incidența excepțiilor, așa cum este descris mai sus.

Cu toate acestea, în principiu, în cursul îndeplinirii ambelor sarcini principale ale poliției (prevenirea unui pericol real și suprimarea unei anumite infracțiuni) trebuie să existe un raport evident și direct între prelucrarea datelor efectuată de către poliție și situația în care persoanele deja au comis sau pot comite o infracțiune și, de asemenea, trebuie să existe o legătură clară între persoana cărei date personale se prelucrează și scopul prelucrării (cum ar fi investigarea sau o sarcină specială a poliției). Această legătură precum și respectarea principiilor de protecție a datelor trebuie să poată fi dovedită în orice moment. După etapa de colectare și în cursul altor etape ale investigației este necesară o analiză minuțioasă pentru a evalua care din date urmează a fi păstrate și care șterse.

În acest context, prelucrarea datelor personale care sunt colectate la o etapă incipientă a investigației și care în procesul ei se dovedesc a nu mai fi relevante trebuie încetată (de ex., s-a dovedit nevinovăția bănuitului), și prin urmare, datele trebuie blocate sau șterse.

Această regulă nu se aplică în cazul în care este permisă utilizarea ulterioară a datelor. Orice prelucrare ulterioară a datelor în scopurile poliției, altă decât cea pentru care datele au fost inițial colectate trebuie să îndeplinească cerințele legale aplicabile prelucrării datelor personale: ea trebuie să fie prevăzută de lege, trebuie să fie relevantă pentru scopul de prelucrare care nu este compatibil cu cel inițial și trebuie efectuată pentru atingerea unui scop legitim și trebuie să fie necesară și proporțională cu scopul legitim urmărit.

4. Deosebirea dintre diferiți subiecți de data și diferite date

i. Subiecții de date

Prelucrarea datelor personale ce vizează diferite categorii de subiecți de date este inerentă pentru prelucrarea datelor personale în domeniul cooperării judiciare în materie penală și cooperării polițienești. Prin urmare, se recomandă ca în prelucrarea de către poliție să se facă o deosebire dintre datele personale ale diferitor categorii de persoane, cum ar fi bănuiții, persoanele condamnate pentru infracțiuni, victimele, terții cum ar fi martorii. Acest lucru este relevant și pentru scopul specific pentru care datele se colectează.

ii. Categoriile de date

Datele pot fi clasificate în diferite categorii. Una din clasificări presupune divizarea lor în categorii de date factuale temeinice și date neprobate bazate pe opinie/evaluare personală. Acest lucru este important deoarece efectuarea prelucrăriii poate fi diferită pentru fiecare caz. De exemplu, declarațiile victimelor și martorilor care conțin date personale sunt întemeiate pe percepțiile subiective ale persoanei care le depune. Aceste declarații nu sunt întotdeauna verificabile și pot fi contestate în timpul procesului legal. În asemenea cazuri cerința privind exactitatea datelor nu se aplică conținutului declarației, ci doar la simplul fapt că o anumită declarație a fost depusă. Mai mult, cerința de a menține datele personale actualizate trebuie, de asemenea, pertractată în acest context. Dacă o hotărâre de condamnare a unei persoane a fost anulată de o instanță de apel, poliția trebuie să facă modificări în înregistrările sale. Însă, ea nu va schimba în mod retrospectiv declarațiile martorilor chiar dacă instanța contactează că ele nu sunt fiabile.

iii. Prelucrarea datelor sensibile

Categoriile speciale de date, cum ar fi datele genetice, datele personale legate de infracțiuni, proceduri penale și condamnări și măsurile de securitate relevante, datele biomentrice care identifică în mod unic o persoană, datele personale ce dezvăluie informații privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, datele privind sănătatea sau viața sexuală pot fi prelucrate numai dacă acest lucru este prevăzut de lege, în sensul necesității unui temei legal prevăzut de legislația națională, și dacă au fost implementate garanții adecvate pentru a contracara potențialul risc de discriminare sau efectele juridice negative care aduc atingere drepturilor și libertățile subiectului de date.

Celelalte condiții privind prelucrarea legală a datelor sensibile includ protecția intereselor vitale ale subiecților de date sau ale altei persoane fizice (aceasta include, fără îndoială, și sănătatea și viața unei ființe umane, dar poate fi interpretată astfel încât să includă drepturile juridice, cum ar fi dreptul la apărare a unei persoane fizice) și situația în care aceste date sensibile sunt făcute publice în mod manifest de către persoana vizată. Trebuie de evidențiat că condiția din urmă trebuie interpretată astfel încât să presupună că subiectul de date este conștient că datele respective vor fi publice și accesibile oricărei persoane, inclusiv autorităților publice (cum ar fi poliția). În cazul existenței unei îndoieli, trebuie aplicată o interpretare îngustă, întrucât se presupune că subiectul de date a renunțat în mod voluntar la protecția specială pentru datele sensibile, punându-le la dispoziția publicului, inclusiv a autorităților publice.

În cazurile precum publicarea datelor personale într-o biografie în presă sau pe un site web, intenția este clară și se poate de presupus cu siguranță că subiectul de date și-a publicat datele în mod conștient. În alte cazuri este mai dificil de determinat. De exemplu, înregistrarea într-o rețea de socializare ar putea include acceptul anumitor reguli de protecție a datelor cu caracter personal care prevăd că toți partenerii furnizorului (inclusiv autoritățile naționale de poliție) au accesul la datele personale. În asemenea cazuri majoritatea utilizatorilor nu iau act în mod activ de acest lucru și, de fapt, nu sunt conștienți că datele lor sunt disponibile autorităților de poliție.

În ceea ce privește problema garanțiilor legale necesare, este de notat că ele pot fi asigurate prin cerințe materiale sau procedurale suplimentare. Ca cerințe materiale suplimentare pot fi considerate limitările suplimentare legate de scopul prelucrării (de ex., pentru anumite categorii de infracțiuni) sau în cazul măsurilor preventive unei situații urgente (de ex., un pericol iminent susceptibil să aibă consecințe grave pentru interesele vitale ale mai multor persoane). Mai mult, trebuie să fie posibilă colectarea acelor date numai în legătură cu alte date privind persoana fizică vizată. Garanții procedurale suplimentare ar putea fi autorizarea dată de instanță sau de un alt organ independent și interdicția transmiterii acelor date.

Aceste garanții pot fi însoțite în cel mai bun caz de garanții suplimentarecu caracter tehnic, cum ar fi măsuri suplimentare de securitate și măsuri cu caracter organizațional, pentru a asigura confidențialitatea și integritatea datelor precum și reguli mai stricte cu privire la accesul personalului autorității competente. Ele trebuie ajustate la fiecare operațiune de prelucrare a datelor, luând în considerare specificul și se recomandă utilizarea multiplelor niveluri de protecție pentru acele categorii de date (de ex., mainframe-uri separate, perioade mai scurte de păstrare a datelor, etc.). Este importantă prevenirea accesului neautorizat sau nedorit la acele categorii de date.

În esență, principiul necesității trebuie aplicat în mod specific și trebuie asigurată revizuirea justificărilor precise și întemeiate pentru prelucrarea datelor sensibile în scopul determinării echilibrului dintre dreptul la viață privată și interesul public. Astfel, este necesară asigurarea unui echilibru a intereselor, luând în considerare scopul investigării, contextul și caracterul datelor, pentru a determina dacă și în ce măsură poliția poate prelucra date personale. Spre exemplu, se recomandă deosebirea cazurilor în care datele biometrice se prelucrează de poliție în scopurile de identificare (atunci când, de exemplu, ar putea fi suficiente două amprente digitale) și cazurilor în care aceasta se fac în scopul investigării infracțiunilor (unde ar putea fi necesare mai multe amprente digitale).

Efectuarea unei evaluări a impactului asupra protecției datelor (DPIA), care oricum trebuie efectuată dacă un tip de prelucrare este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, poate fi recomandată și pentru a facilita asigurarea faptului că garanțiile adecvate sunt puse în aplicare. Operatorul de date trebuie să evalueze și să demonstreze dacă scopul prelucrării poate fi realizat într-o manieră care are un impact mai scăzut asupra dreptului la viața privată și protecția datelor și dacă prelucrarea categoriilor speciale de date nu prezintă niciun risc de discriminare pentru subiectul de date.

Mai mult, trebuie de menționat că este interzisă colectarea și prelucrarea datelor sensibile în contextul creării de profiluri, cu excepția cazului în care aceste date sunt necesare și proporționale cu scopurile legale și specifice prelucrării și atât timp cât legea națională prevede garanții adecvate. În acest context, în afara măsurilor descrise în mod detaliat mai sus, poate fi recomandată utilizarea tehnologiilor de creștere a confidențialității (Privacy Enhancing Technologies – PET) și efectuarea mai frecventă a controalelor legalității prelucrării. Acest lucru ar putea fi asigurat, de exemplu, prin instituirea măsurilor pentru a respinge ipoteza că persoanele aparțin unei organizații criminale din cauza că locuiesc într-o localitate unde activează o organizație criminală sau în care persoanele au aceeași origine etnică.

5. Păstrarea datelor

Datele personale trebuie prelucrate atâta timp cât ele servesc scopului pentru care au fost colectate. Datele stocate trebuie să fie adecvate, actualizate, necesare, relevante și neexcesive în raport cu scopurile pentru care ele au fost colectate.

Principiul necesității trebuie aplicat pe tot parcursul prelucrării. Stocarea poate fi permisă numai atunci când o analiză denotă că datele personale sunt strict necesare pentru realizarea scopurilor polițienești.

Din această perspectivă, datele personale trebuie prelucrate atâta timp cât ele servesc scopului specific, iar atunci când ele nu mai sunt necesare pentru acest scop, ele trebuie șterse, cu excepția cazului în care legea prevede o prelucrare ulterioară și ele sunt considerate relevate pentru un scop care nu este compatibil cu scopul inițial de prelucrare. În mod alternativ, păstrarea poate fi permisă într-o formă care nu permite identificarea subiecților de date.

Întrebarea, dacă anumite date au servit scopul lor și nu mai sunt necesare, apare, în special, atunci când stocarea datelor este permisă pentru scopuri preventive (activități polițienești de prevenire a infracțiunilor). Este specific pentru asemenea scopuri ca stocarea să se bazeze numai pe o evaluare a riscurilor în legătură cu un anumit subiect de date. În astfel de cazuri, nu există un punct de încheiere, spre deosebire de o anchetă penală, care în mod automat necesită o decizie privind ștergerea datelor personale colectate în timpul anchetei. Totuși, principiul necesității impune o revizuire a estimării inițiale după o perioadă de timp adecvată. Decizia de păstrare a datelor pentru o altă perioadă ar trebui să fie bine întemeiată, iar raționamentul ar trebui documentat pentru a face decizia de revizuire inteligibilă.

În afară de aceasta, în cazul în care termenele pentru ștergerea datelor personale în fișierele de date specifice nu sunt stabilite direct în conformitate cu legislația națională, atunci ar trebui să se efectueze o revizuire periodică a necesității de stocare.

Legislația națională ar trebui să prevadă criterii clare și transparente pentru evaluarea necesității de a păstra în continuare datele personale (cum ar fi necesitatea de a ține seama de actualizările referitoare la deciziile judiciare sau în cazul reabilitării persoanelor condamnate etc.), precum și pentru cerințele procedurale, astfel încât principiile calității datelor să fie respectate în mod eficient pentru a evita orice abuz. În acest scop, ori de câte ori se efectuează o astfel de revizuire periodică, ar trebui să se urmărească implicarea responsabilului de protecția datelor (DPO) în aplicarea acestor criterii – printre altele, în vederea unui posibil audit intern - și informația cu privire la orice decizie de a păstra în continuare datele și motivele, care stau la baza acesteia, ar trebui păstrate și puse la dispoziția autorității de supraveghere competente.

În plus, trebuie de făcut o distincție între categoriile de date în baza contribuției lor efective la realizarea scopurilor urmărite și trebuie să se utilizeze criterii obiective pentru stabilirea duratei perioadei maxime de stocare sau a revizuirii periodice. De exemplu, dacă este relevant în lumina unui anumit caz, trebuie luat în considerare tipul sau gravitatea infracțiunii sau a riscului existent.

Mai mult ca atât, având în vedere deosebirile dintre diferitele categorii de persoane vizate (victime, bănuiți, persoane condamnate pentru o infracțiune, martori, experți, alte persoane implicate) prevăzute în legislația privind protecția datelor în domeniul aplicării legii, acestea trebuie să fie reflectate și în stocarea datelor respective. În acest sens, distincțiile obligatorii trebuie să conducă la adoptarea unui regim gradual de diferite perioade de timp pentru diferite categorii de persoane vizate. O atenție deosebită trebuie acordată și protecției minorilor în acest context. Bazele de date existente și viitoare trebuie să fie (re)organizate într-un mod care să permită realizarea distincțiilor necesare între diferitele categorii de persoane vizate.

Din această perspectivă, ținând cont de faptul că protecția datelor necesită confidențialitatea începând din momentul conceperii, termenele maxime precum și revizuirile periodice prevăzute de legislația națională trebuie implementate prin intermediul sistemului de tehnologii informaționale bine structurat anume în ceea ce privește „protecția datelor începând din momentul conceperii”.

Aceasta ar însemna că bazele de date existente și viitoare trebuie reorganizate astfel încât să asigure ca revizuirile periodice să aibă loc în mod sistematic precum și să realizeze ștergerea automatizată a datelor după expirarea termenului limită de stocare. În cazul termenelor maxime, sistemul trebuie să asigure că datele se șterg sau se anonimizează în mod automat odată cu expirarea termenului de stocare. Până la implementarea unui asemenea sistem, autoritățile competente trebuie să implementeze măsuri organizatorice pentru a preveni orice utilizare ulterioară a acestor date. În cazuri revizuirilor periodice, sistemul trebuie în mod automat să-i amintească operatorului despre nevoia de a revizui necesitatea prelucrării ulterioare. Dacă revizuirea nu se efectuează în termenul stabilit, datele respective trebuie șterse sau pseudonimizate/mascate în mod automat.

6. Informația furnizată persoanelor

Una din obligațiile cele mai importante ale operatorilor de date este obligația de a furniza subiecților de date informația cu privire la prelucrarea datelor. Această obligație este dublă: ea necesită ca operatorul de date să furnizeze publicului informația generală cu privire la prelucrarea datelor pe care o efectuează și să ofere informație specială subiecților de date, dacă nu se aplică nicio restricție sau derogare la prelucrarea datelor.

Informația furnizată publicului larg trebuie să aibă ca scop sensibilizarea opiniei publice, să informeze publicul cu privire la drepturile persoanelor vizate, să ofere linii directorii cu privire la exercitarea drepturilor. Informația furnizată trebuie să fie accesibilă în mod eficient și larg. Ea trebuie să fie inteligibilă și ușor accesibilă și furnizată într-un limbaj clar și simplu, și să corespundă circumstanțelor prelucrării în cauză. Ca prim pas ea trebuie furnizată înainte de colectarea datelor . Acest lucru poate fi realizat prin postarea acestei informații pe site-ul oficial al autorității competente (de ex., poliția își poate publica politica proprie cu privire la înregistrarea armelor de foc).

Site-urile și celelalte mijloace ușor accesibile îndeplinesc un rol în informarea publicului. Se recomandă de postat pe aceste site-uri o politică de confidențialitate generală care ar conține informația de bază cu privire la organizare, scopul prelucrării datelor personale, posibil modele de scrisori prin care subiecții de date să-și exercite drepturile precum și informația de contact a responsabilului de protecția datelor ca și persoană de contact la depunerea solicitărilor. Mai mult, trebuie incluse și detalii cu privire la condițiile în care se aplică excepțiile la drepturile subiecților de date și modul în care ei pot depune contestații la responsabilul cu protecția datelor sau la instanță. Este sarcina operatorului să furnizeze informații care în mod adecvat evidențiază protecția datelor și drepturile subiecților de date.

La acest capitol, trebuie să se menționeze în special articolul 6 para. (3) din Legea 320 din 27.12.2012 privind activitatea poliției și statutul polițistului. Această prevedere ar trebui citită în lumina legislației privind protecția datelor. În consecință, când poliția comunică cu mass-media și / sau când vorbește în public pentru a obține asistența publicului în cadrul unei anchete penale sau pentru a informa publicul larg cu privire la o anchetă sau urmărire penală în curs de desfășurare a unei infracțiuni, ea trebuie să acționeze întotdeauna cu precauție pentru a nu divulga date personale care pot identifica persoanele fizice sau pot interfera cu alte legislații specializate (dreptul penal, procedura de drept penal) și principiul prezumției de nevinovăție.

În cazul furnizării subiecților de date a unei informații mai speciale, ea trebuie să includă detalii cu privire la prelucrarea datelor, colectarea datelor persoanelor precum și o informație cuprinzătoare privind drepturile lor astfel încât subiecții de date să fie asigurați cu detalii cum ar fi numele, datele de contact ale operatorului, persoana împuternicită de operator, destinatarii datelor, setul de date care urmează a fi prelucrat, scopul prelucrării datelor, temeiul legal pentru aceasta și informații cu privire la drepturile lor.

Cu toate acestea, obligația de a furniza informații poate face obiectul derogărilor, dacă acest lucru este prevăzut de lege. Drept urmare, furnizarea informației subiectului de date poate fi amânată, restricționată sau omisă în măsura în care acest lucru este necesar și proporțional, în conformitate cu următoarele: pentru a evita obstrucționarea unei anchete oficiale sau juridice, unei investigații sau proceduri, pentru a evita prejudicierea prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau executării sancțiunilor penale, pentru a proteja securitatea publică, pentru a proteja securitatea națională sau pentru a proteja drepturile sau libertățile altora. Ca exemplu de renunțare la obligația de a furniza informații pentru a nu aduce atingere unei activități / investigații polițienești care poate servi un caz de investigare a unei persoane care a comis un viol și prezintă un risc ridicat. În acest caz, prelucrarea datelor și păstrarea lor pe termen lung poate fi justificată fără a informa persoanele aflate sub supraveghere, dacă acest lucru ar putea prejudicia o investigație în curs sau planificată. Cu toate acestea, odată ce obiectivul monitorizării ascunse a fost atins și nu se aplică nicio altă restricție sau derogare, persoana vizată ar trebui să fie informată cu privire la faptul că el sau ea a fost supus(ă) acestei măsuri.

7. Drepturile subiecților de date

Subiectul de date are dreptul de a cunoaște dacă datele personale ce îl vizează se prelucrează și în cazul în care ele se prelucrează, să obțină comunicarea datelor sale, să aibă acces la datele sale și, prin aceasta, să poată verifica legalitatea prelucrării care este în curs de desfășurare.

Mai exact, aceasta, de asemenea, presupune dreptul de a obține în mod direct de la operator confirmarea sau infirmarea prelucrării datelor sale personale (cunoscut, de asemenea, sub termenul de „acces direct” de către subiectul de date). În cazul unui răspuns afirmativ, acesta include accesul la datele personale și anumită informație.

Atunci când subiectul de date își exercită dreptul său la acces, trebuie să-i fie furnizată o copie a informației solicitate fără întârziere, în termen de cel mult o lună de la primirea cererii, în mod gratuit, cu excepția cazului dacă cererea este în mod vădit nefondată sau excesivă, în special din cauza caracterului ei repetitiv.

Trebuie clarificat faptul că, în conformitate cu articolul 62 para. (4) din „proiectul de lege” al Repiblicii Moldova, operatorul de date este obligat să informeze fără întârzieri nejustificate subiectul de date, ceea ce este reflectat și în Directiva privind autoritățile de aplicare a legii (UE) 2016/680. În pofida acestei formulări specifice, regulile de bune practici și interpretarea oferită de UE prevăd aceleași perioade ca și în GDPR ( prevederile generale corespunzătoare din „proiectul de lege” al Republicii Moldova - a se vedea art. 13 (3)) pentru drepturile și obligațiile respective, aceastea ar trebui să se aplice și în prevederile relevante ce țin de aplicarea legii. Având în vedere acest lucru, se sugerează stabilirea în consecință a intervalului de timp de o lună, cu posibilitatea de extindere a acestuia la maximum două luni, atunci când este necesar, ținând cont de complexitatea și numărul de solicitări.

 Informația furnizată trebuie să fie concisă, inteligibilă și ușor accesibilă, scrisă într-un limbaj clar și simplu, fiind adaptată la necesitățile persoanelor vulnerabile. Dacă este posibil, ea trebuie furnizată în aceeași formă în care a fost depusă cererea.

Trebuie de menționat și faptul că ar trebui să se instituie dispoziții și proceduri relevante pentru confirmarea identității subiectului de date înainte de acordarea accesului la orice date și/sau informații privind activitățile de prelucrare vizate în cerere. Același lucru este valabil și în cazul în care persoanele vizate deleagă altcuiva de a le exercita drepturile.

Mai mult ca atât, subiectul de date este în drept să obțină rectificarea datelor ce-l vizează. Acesta este un drept esențial al subiectului de date care-i permite să modifice orice date incorecte care le vizează sau să obțină ștergerea datelor ale căror prelucrare este excesivă, nerelevată sau în alt mod ilegală. Dacă subiectul de date găsește date incorecte sau nerelevante, el trebuie să aibă dreptul de a ataca și de a asigura că ele fie sunt modificate, fie șterse.

În unele cazuri, poate fi oportună adăugarea informației suplimentare sau corective. Este important de subliniat că acest drept poate fi exercitat numai cu respectarea drepturilor altor persoane.

Dacă datele care urmează a fi corectate sau șterse au fost comunicate în alt loc, autoritățile relevante ar trebui să fie informate cu privire la modificările care trebuie făcute.

Toate modificările intenționate trebuie susținute de dovezi. În cazul în care persoanele vizate pot dovedi, utilizând documentația oficială, că datele prelucrate de poliție în legătură cu ele sunt incorecte, operatorul de date nu are dreptul de a decide dacă trebuie să le corecteze.

Cu toate acestea, legea prevede restricții la drepturile persoanelor vizate fie integral, fie parțial. Chiar și în aceste cazuri, subiectul de date ar trebui să aibă în continuare dreptul de "acces indirect". Acest lucru presupune în mod clar că legislația națională trebuie să prevadă posibilitatea exercitării drepturilor de informare, de acces sau de informare cu privire la refuzul operatorului de a rectifica sau șterge, inclusiv și cel puțin prin intermediul autorității de supraveghere competente. Acest drept trebuie distins de dreptul de a depune o plângere la autoritatea de supraveghere deoarece constituie un drept suplimentar.

Trebuie remarcat faptul că aceste restricții sau derogări de la drepturile persoanelor vizate ar trebui să se aplice numai în măsura în care sunt necesare, proporționale și interpretate în mod restrictiv și nu ar trebui să permită restricții generale la drepturile de informare și accesul subiecților de date. Se recomandă ca dispozițiile naționale relevante să definească criterii obiective pentru a stabili în ce cazuri, categorii de prelucrare și în ce condiții pot fi deținute informații suplimentare de către operatorii de date și pentru a determina care pot fi deținute integral și care parțial.

Orice solicitare a subiectului de date trebuie evaluată cu atenție de la caz la caz. Orice decizie de respingere a cererii unui subiect de date trebuie furnizată în scris (inclusiv prin mijloace electronice). Răspunsul trebuie să ofere o justificare clară a luării deciziilor care poate fi verificată de o autoritate independentă (autoritatea de supraveghere) sau de o instanță. Este posibil ca comunicarea motivelor de refuz să reprezinte un risc pentru aplicarea legii sau persoana vizată sau pentru drepturile și libertățile altora. În acest caz, acest lucru trebuie să fie documentat și furnizat autorității independente sau instanței pentru verificare, dacă este necesar. În cazul în care poliția trimite o scrisoare de refuz, aceasta trebuie să conțină numele, adresa, adresa web etc. a tuturor formelor posibile de recurs. În special, subiectul de date trebuie informat cu privire la toate opțiunile disponibile ca urmare a unei decizii de refuz, cum ar fi un recurs fie la autoritatea de supraveghere, fie la o instanță sau la o altă autoritate administrativă independentă.

În cazul în care subiectul de date contestă respingerea drepturilor sale de către poliție în fața autorității de supraveghere, atunci autoritatea de supraveghere trebuie să revizuiască toate datele și dosarele personale vizate și dosarele păstrate de poliție, precum și motivele și justificările furnizate cu privire la respingerea drepturilor subiectului de date. Ulterior, autoritatea de supraveghere trebuie să retransmită rezultatul revizuirii către subiectul de date. În acest caz, este esențial ca persoana vizată să fie cel puțin informată că a avut loc o verificare a dosarului de poliție. În mod alternativ, organul de supraveghere poate solicita poliției să elibereze subiectului de date datele conținute în dosar.

Cu toate acestea, trebuie subliniat faptul că competențele autorității de supraveghere menționate mai sus nu trebuie să fie interpretate greșit astfel încât, atunci când își îndeplinește sarcina de a revizui legalitatea prelucrării, autoritatea are puterea de a interveni sau modifica dosarul respectiv; adică fișierul care conține orice date cu caracter personal ale persoanei solicitante. Autoritatea de supraveghere are numai dreptul și obligația de a analiza fișierul, de a verifica legalitatea prelucrării și de a informa subiectul de date despre faptul că a fost efectuată o verificare și despre rezultat.

Instanța sau tribunalul pot avea competențe de a impune oferirea accesului, corectarea sau ștergerea datelor din dosar chiar și în cazurile de solicitări de acces redirecționate la el/ea de către poliția sau autoritatea de supraveghere.

Subiectul de date trebuie să aibă acces la o instanță pentru a introduce o cale de atac și să verifice motivele refuzului dacă nu este mulțumit de răspunsul dat de autoritatea de supraveghere. Autoritatea de supraveghere ar trebui să dispună de competențe suficiente pentru a examina dosarul de poliție în cauză și pentru a asigura comunicarea rezultatului evaluării.

Cu toate acestea, ar trebui făcută o distincție clară în cazul datelor personale cuprinse într-o hotărâre de judecată sau în alte documente referitoare la investigație sau procedurile create de o instanță sau de o altă autoritate judiciară sau în numele acesteia sunt reglementate de (lex specialis) care reglementează divulgarea informațiilor în cadrul procedurilor penale, cum ar fi Codul de Procedură Penală. În acest caz, judecătorul sau o altă autoritate judiciară este operatorul și datele personale relevante sunt conținute într-o hotărâre de judecată sau în alte documente care sunt create în cursul unei anchete sau proceduri penale și efectuate de către sau în numele judecătorului sau al autorității judiciare. Drept urmare, exercitarea drepturilor subiecților de date nu se aplică în acest caz (de ex., dreptul de acces, dreptul la ștergere etc. în raport cu un dosar de caz) deoarece se aplică o lege specială. Acest aspect trebuie luat în considerare de fiecare dată pentru a determina dacă se va aplica legislația privind protecția datelor și, prin urmare, dacă autoritatea de supraveghere își păstrează competența de a verifica legalitatea fișierelor care conțin date cu caracter personal. Altfel spus, ori de câte ori, de exemplu, o autoritate de aplicare a legii efectuează o anchetă penală inițială, care nu constituie încă un dosar penal oficial și Procuratora nu este încă implicată, cu condiția să nu existe dispoziții speciale pentru aceste cazuri în Codul de Procedură Penală, atunci autoritatea de supraveghere își poate exercita competența și poate analiza dosarul, dacă este necesar, și în conformitate cu dispozițiile prevăzute în „proiectul” legii al Republicii Moldova.

În final, trebuie subliniat faptul că atunci când autoritățile de aplicare a legii menționate mai sus acționează în calitatea lor administrativă sau mai mult până la acest punct, când desfășoară o anchetă în cadrul unei proceduri administrative și nu a unei proceduri penale, atunci se aplică prevederile generale ale legislației privind protecția datelor cu caracter personal, adică capitolele I-VI din „proiectul de lege” privind protecția datelor cu caracter personal. Totuși, acest lucru înseamnă că exercitarea drepturilor subiectului de date se va face în conformitate cu aceste dispoziții și nu conform prevederilor capitolului VII din proiectul de lege privind protecția datelor cu caracter personal. Ținînd cont de acest lucru, orice derogări și limitări (dacă este absolut necesar) asupra drepturilor subiecților de date ar trebui impuse în conformitate cu dispozițiile relevante care permit impunerea restricțiilor atât asupra obligației operatorului de a furniza informații, cât și a drepturilor subiectului de date în anumite circumstanțe, condiții și prevăzute de lege, cum ar fi: pentru a proteja prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor, protejarea independenței judiciare și a procedurilor judiciare și a altor obiective importante de interes public general (a se vedea art. 28 din „proiectul de lege” al Republicii Moldova.

8. Loggins (registrul fișier al înregistrărilor)

Ori de câte ori în domeniul de aplicare a legii funcționează un sistem automatizat (baza de date IT), trebuie respectată o procedură obligatorie de creare a fișierelor jurnal. În special, există o obligație de a păstra jurnalele cel puțin pentru operațiunile de prelucrare cum ar fi colectarea, modificarea, consultarea, dezvăluirea, inclusiv transferurile, combinarea și ștergerea. În plus, în caz de consultare și dezvăluire, jurnalele trebuie să permită stabilirea justificării, datei și orei acestor operațiuni și, în măsura în care este posibil, identificarea persoanei care a consultat sau a dezvăluit datele personale și identitatea destinatarilor unor astfel de date personale. În esență, implementarea fișierelor jurnal înseamnă menținerea metadatelor relevante pentru un proces de prelucrare a datelor personale.

Fișierele jurnal reprezintă un instrument important pentru monitorizarea protecției datelor și, prin urmare, pentru controlul tuturor operațiunilor relevante de prelucrare a datelor cu caracter personal. Cu alte cuvinte, este foarte benefic să existe posibilitatea de a urmări activitatea utilizatorului pentru a identifica utilizarea abuzivă.

Utilizarea fișierelor jurnal are un scop dublu: ea poate fi folosită ca măsură de descurajare a utilizării neautorizate, care poate fi eficientă numai dacă este pusă în aplicare o regulă de analiză a jurnalelor și o măsură punitivă atunci când se constată o încălcare. Prin urmare, un aspect suplimentar care trebuie luat în considerare este îmbunătățirea activității de auto-audit a operatorilor prin raportări periodice ale analizei jurnalelor, care ar putea fi realizate în mod automat și adaptate pentru domenii specifice ale activității de aplicare a legii.

Pentru ca acest instrument să servească scopul său, ar trebui elaborate și descris în detaliu în lege mai mulți parametri: conținutul, perioadele de stocarea, măsurile tehnice, auto-auditul și politicile interne care promovează conformitatea. Mai mult decât atât, legislația națională ar trebui să prevadă adoptarea de măsuri tehnice care să garanteze integritatea jurnalelor.

În ceea ce privește perioada de stocare, stabilirea unei perioade adecvate de stocare ar trebui asigurată prin stabilirea unor criterii clare sau a unor perioade fixe. O perioadă de stocare adecvată pentru jurnale trebuie să derive din scopurile utilizării fișierelor jurnal și ar trebui să asigure că este posibilă realizarea acestor scopuri. Aceasta se referă în special la verificarea legalității prelucrării care se încadrează în sarcinile autorității de supraveghere (Centrul Național pentru Protecția Datelor cu Caracter Personal). Prin urmare, perioada de stocare a jurnalelor ar trebui să ofere autorității de supraveghere suficient timp pentru a reconstitui și revizui prelucrarea datelor, monitorizarea accesului la date, ceea ce înseamnă că consultarea și dezvăluirea trebuie să se facă în mod regulat și într-o perioadă mai scurtă de timp. De regulă, nu este necesară păstrarea jurnalelor de acces atât timp cât sunt stocate datele de bază. În orice caz, atunci când se iau decizii privind perioadele de stocare adecvate, echilibrul corect trebuie asigurat pentru fiecare caz aparte în funcție de baza de date în cauză, ținând seama, pe de o parte, de faptul că o perioadă lungă de stocare pentru registre va facilita reconstituirea istoricului prelucrării și, pe de altă parte, faptul că, atunci când registrele se păstrează mai mult timp decât datele de fond, o parte din informație este menținută și mai mult (de exemplu, în procedurile penale sau în scopuri preventive, datele de fond sunt, de obicei, stocate o perioadă lungă de timp, iar subiectul de date află informația despre prelucrare într-o etapă ulterioară. În acest moment ar trebui să fie posibilă reconstituirea prelucrării datelor prin intermediul jurnalelor).

9. Tranferurile internaționale

Întrucât necesitatea schimbului de date între autoritățile de aplicare a legii din diferite state sau / și organizații / instituții internaționale este destul de comună, procedura de transferuri internaționale este strict reglementată în conformitate cu legislația privind protecția datelor cu caracter personal și în special în art. 72-74 din „proiectul de lege” din Moldova.

În principiu, transferurile pot fi autorizate fie pe baza unei decizii a Centrului privind nivelul adecvat de protecție a țării / organizației destinatar, cât și în condițiile prevăzute de legea specială sau în baza unui tratat sau acord internațional ratificat de stat. Cu toate acestea, sunt prevăzute excepții de la aceste reguli pentru situații specifice (art.73 „proiectul de lege” al Republicii Moldova) și în condiții stricte, astfel încât să permită transferul către autorități, altele decât aplicarea legii (art. 74 „proiectul de lege” al Republicii Moldova). În aceste cazuri, Centrul trebuie informat prin cerere și, respectiv, într-un interval de timp stabilit.

De menționat că, regula generală prevede că orice transfer de date ale poliției / instituție de aplicare a legii la nivel internațional ar trebui limitat la organele de aplicare a legii și ar trebui să fie necesar pentru aplicarea legii și în conformitate cu legea. În momentul transmiterii datelor, trebuie de ținut cont de faptul dacă autoritatea care primește datele, îndeplinește o funcție care i-a fost conferită de drept, legată de scopurile aplicării legii și dacă datele relevante sunt necesare pentru a-și îndeplini sarcina specifică.
Pentru a evalua acest lucru, trebuie respectate procedurile interne prevăzute de legislația procesuală penală națională, care pot include participarea activă a unor organisme și servicii mai largi de aplicare a legii, precum Ministerul de Interne, Ministerul Justiției, Procuratura Generală, judecătorii de anchetă etc.

În orice caz, ar trebui să se verifice întotdeauna dacă există un nivel adecvat de protecție a datelor în statul primitor și dacă acest stat respectă regulile relevante privind transferurile internaționale de date cu caracter personal. Aceasta include prevederea unor garanții adecvate privind protecția datelor în cazurile în care nu există dispoziții legale naționale relevante sau acorduri internaționale, în pofida faptului că acest mijloc de transfer ulterior ar trebui utilizat ca o ultimă opțiune. Cadrul transferurilor internaționale, precum dispozițiile instrumentelor juridice internaționale multilaterale, cum ar fi Convenția 108, Constituția Interpolului și documentația de susținere a acesteia cu privire la gestionarea datelor (ca „Regula INTERPOL privind prelucrarea datelor” și „Statutul Comisiei pentru controlul fișierele INTERPOL ”Reguli privind controlul informațiilor și accesul la fișierele INTERPOL”), cadre juridice regionale precum legislația instituțiilor UE și UE (în special cu privire la Europol - secțiunea 2 din capitolul V și capitolul VI privind garanțiile privind protecția datelor din Regulamentul (UE)) 2016/794, Frontex etc.) și acordurile ulterioare (acorduri bilaterale operaționale), tratate bilaterale și, în general, acordurile internaționale privind asistența reciprocă sau alte acorduri bilaterale sau multilaterale încheiate cu privire la cooperarea eficientă ar trebui să fie luate în considerare pentru a se asigura că orice transfer de date este justificat legal și are garanții adecvate în vigoare. Cererea ar trebui să indice în mod clar toate elementele necesare de la partea solicitantă pentru a permite părții destinatare să ia o decizie solidă cu privire la cerere. Aceste detalii ar trebui să includă motivul solicitării, precum și scopul transferului de date.

În cazurile excepționale de transfer internațional de date cu caracter personal între autoritățile de aplicare a legii și organele private dintr-un alt stat, trebuie asigurat un nivel adecvat de protecție care ține cont de natura sensibilă a datelor din domeniul aplicarării legii. În plus, trebuie să se acorde garanții cu privire la utilizarea datelor și la legalitatea transferului de date în țara de primire. Când este posibil, ar trebui să fie disponibilă utilizarea instrumentelor juridice internaționale existente pentru acest tip de transfer de date. De asemenea, trebuie menționat că transferurile internaționale pot apărea în mod excepțional și atunci când autoritățile competente comunică date cu caracter personal pentru interesele specifice ale subiectului de date sau pentru interese legitime prevalente (cum ar fi, de exemplu, în scopuri umanitare).

Așa cum am menționat mai sus, dacă datele trebuie transferate către țări sau organizații care nu participă la Convenția 108 sau la legislația UE privind protecția datelor, ar trebui să se garanteze un nivel adecvat de protecție a datelor (de exemplu, prin garanții standardizate ad hoc sau aprobate de instrumente obligatorii și executorii legale).

În general, în cazul transferurilor internaționale, ar trebui furnizate următoarele garanții: normele de protecție a datelor sunt respectate, în special, principiul proporționalității, păstrarea datelor și calitatea datelor, astfel încât datele să fie corecte, actualizate, relevante și complete . În măsura posibilului, în toate comunicările de date, ar trebui indicate deciziile judiciare, precum și deciziile de nejudecare a urmăririi penale. Este necesar să se stabilească canale sigure de comunicare care să asigure securitatea datelor la cel mai înalt nivel posibil.
În plus, principiul limitării necesității și scopului ar trebui să fie aplicabil în sensul că orice date partajate nu ar trebui utilizate pentru altceva decât scopul pentru care au fost trimise sau primite. Excepțiile de la acest lucru sunt atunci când autoritatea expeditoare, pe baza prevederilor legale, își exprimă acordul pentru utilizarea ulterioară, fiind necesar și vital ca destinatarii să își îndeplinească sarcina.

De asemenea, trebuie să se asigure că există măsuri adecvate pentru a proteja securitatea informațiilor.
Nu în ultimul rând, o importanță deosebită este, de asemenea, garanțiile referitoare la drepturile subiectului de date. Aceste drepturi (la informații, acces etc.) ar trebui să fie protejate și orice restricții ar trebui să fie enunțate în mod clar, în timp ce ar trebui să fie prevăzut un mecanism de remediere, pentru a se asigura că subiectul de date păstrează un drept de a obține compensații și, după caz, compensații, inclusiv posibilitatea subiecților de date de a exercita acțiuni în fața unui organism competent în cazul încălcării drepturilor lor.

10. Responsabilul de protecția datelor (“DPO”)

Desemnarea unui responsabil de protecția datelor nu este doar o măsură prevăzută în lege (RGPD și Directiva (EU) 2016/680 și în legislația RM în care ea a fost transpusă) dar, chiar neavând statut obligatoriu pentru instituțiile publice, se consideră a fi cea mai bună practică în domeniul protecției datelor. DPO poate facilita îndeplinirea de către operatori și persoanele împuternicite a obligațiilor ce le revin în condițiile legii și oferi ajutor subiecților de date în ceea ce privește exercitarea drepturilor acestora. Proiectului de lege cu privire la protecția datelor prevăd condițiile obligatorii privind desemnarea DPO: calitățile profesionale, garanțiile necesare care trebuie puse în aplicare pentru ca DPO să-și poată îndeplini atribuțiile, sarcinile atribuite lui și funcția deținută de acesta în cadrul instituției/organizației în care lucrează. Conform celor menționate mai sus, toate autoritățile și organele publice (indiferent de ceea ce prelucrează) trebuie să desemneze un DPO. Cu toate acestea, o excepție poate fi aplicată în cazul instanțelor de judecată și al altor autorități judiciare independente atunci când acționează în calitatea lor judiciară.

Mai exact, în calitate de DPO trebuie numită o persoană care are cunoștințe de specialitate în domeniul legislației cu privire la protecția datelor, cunoștințe în domeniul tehnologiilor informaționale și a securității datelor precum și capacitatea de a îndeplini în mod efectiv sarcinile prevăzute în lege. De aici rezultă că în calitate de DPO poate fi numit nu doar un specialist de drept, dar și un specialist în domeniul tehnologiilor informaționale sau chiar un alt specialist atât timp cât acesta poate dă dovadă de un nivel adecvat de expertiză și competență în raport cu legislația și practicile în domeniul protecției datelor. Mai mult ca atât, nivelul necesar de expertiză trebuie determinat în baza operațiunilor particulare efectuate și protecția necesară pentru tipul de date personale prelucrate de operator și/sau de persoana împuternicită de operator. Prin urmare, în acest caz, DPO datelor trebuie să fie familiarizat și experimentat în ceea ce privește activitatea și, respectiv, prelucrarea datelor în domeniul de aplicare a legii. În cazul unei autorități sau unui organ de stat (cum ar fi poliția de exemplu), DPO trebuie, de asemenea, să aibă cunoștințe solide în ceea ce privește regulile și procedurile administrative ale organizației.

Cu privire la capacitatea sus menționată de a îndeplini sarcinile ce îi revin responsabilului de protecția datelor, aceasta trebuie interpretată atât din perspectiva calităților și cunoștințelor personale, cât și a poziției responsabilului în cadrul organizației. Calitățile personale trebuie să includă, spre exemplu, integritatea și o etică profesională înaltă.

Mai mult ca atât, în funcția de DPO poate fi numit un angajat al autorității competente în domeniul aplicării legii (poliția și altele) – care este operator, sau această funcție poate fi externalizată unui alt prestator de servicii în baza unui contract de prestare a serviciilor. Însă trebuie de menționat că, în cazul în care în această funcție se desemnează un angajat din cadrul instituției, acesta nu trebuie să fie membru executiv al personalului și nu poate să ocupe o funcție de conducere (cum ar fi director executiv, director de operațiuni, director financiar, șef al direcției de comercializare, șef al direcției resurse umane sau șef al direcției tehnologii informaționale), și nici alte poziții mai inferioare în structura organizatorică, dacă asemenea poziții sau roluri implică determinarea scopurilor și mijloacelor de prelucrare. Aceasta se datorează faptului că responsabilul de protecția datelor trebuie să se abțină de la orice sarcini sau atribuții susceptibile care ar genereza un conflict de interese, ceea ce este esențial pentru independența care revine rolului de DPO. În schimb, un conflict de interese poate apărea și în cazul în care un responsabil extern de protecția datelor este, de exemplu, invitat să reprezinte operatorul sau persoana împuternicită de operator în fața instanțelor de judecată în cazurile care implică probleme legate de protecția datelor. Deci, reiese că consilierul juridic al unei entități legale nu trebuie să fie numit în calitate de responsabilul acesteia de protecția datelor, deoarece atribuțiile acestuia în calitate de consilier juridic cel mai probabil vor duce la un conflict de interese în raport cu atribuțiile lui în calitate de DPO. Cu alte cuvinte, consilierul juridic are obligația de a-și apăra clientul indiferent de orice fărădelege sau nereguli din perspectiva protecției datelor, iar DPO are obligația legală de a identifica încălcările de protecție a datelor și a avertiza în privința lor, dar și de a-și documenta recomandarea și opinia. Aceasta denotă că conflictul de interese în asemenea situație este inevitabil.

În ceea ce privește independența DPO, este de accentuat că ea trebuie garantată oricând și este crucială pentru îndeplinirea funcțiilor responsabilului în conformitate cu legislația privind protecția datelor cu caracter personal.. Acest lucru poate fi asigurat prin asumarea de către operatori sau persoanele împuternicite de operatori a angajamentului de a se abține de la emiterea indicațiilor cu privire la exercitarea atribuțiilor responsabilului de protecția datelor precum și prin interzicerea operatorilor de a demite sau penaliza DPO în baza îndeplinirii sarcinilor de către acesta.

De asemenea, un singur responsabil de protecția datelor poate fi desemnat pentru mai multe autorități sau organe competente, ținând cont de structura organizațională și mărimea acestora. Cu toate acestea, este de menționat, de asemenea, că precondiția pentru desemnarea unui singur DPO este capacitatea acestuia de a-și îndeplini sarcinile în mod eficient și de a fi accesibil în raport cu subiecții de date.

DPO trebuie să aibă resurse care i-ar permite să-și îndeplinească sarcinile. Aceasta presupune o susținere activă pentru funcția de DPO din partea conducerii de vârf, alocarea timpului suficient pentru îndeplinirea sarcinilor de către responsabilul de protecția datelor (având în vedere că el poate fi angajat cu normă întreagă sau cu jumătate de normă). Acordarea timpului suficient pentru îndeplinirea sarcinilor responsabilului de protecția datelor este de o importantă majoră. Este o bună practică de a stabili un procentaj de timp alocat pentru îndeplinirea funcțiilor DPO în cazul în care acesta nu este angajat cu normă întreagă.

O altă bună practică este determinarea timpului necesar pentru îndeplinirea funcțiilor, nivelului de prioritate adecvat atribuțiilor responsabilului de protecția datelor precum și elaborarea unui plan de lucru de către responsabilul de protecția datelor (sau organizația). Mai mult ca atât, trebuie asigurată susținerea adecvată în ceea ce privește resurse financiare, infrastructură (încăperi, instalații, echipamente) și, după caz, personal (de exemplu, poate fi creată o direcție de protecție a datelor, în care se angajează responsabilul de protecția datelor care va fi ajutat de personalul angajat în aceeași direcție). Trebuie făcută o comunicare oficială cu privire la desemnarea unui DPO întregului personal și asigurat accesul la alte servicii din cadrul organizației pentru ca DPO să poată beneficia de susținere, contribuție și informare esențială din partea celorlalte servicii. În acest sens, DPO trebuie să fie invitat să participe la toate ședințele conducerii de vârf și de nivel mediu, el trebuie informat prompt cu privire la problemele legate de protecția datelor sau operațiunile care pot avea drept rezultat efecte care implică protecția datelor, trebuie consultat în asemenea cazuri și avizului acestuia trebuie să i se acorde pondere corespunzătoare. În cele din urmă, trebuie să fie prevăzută formarea continuă a DPO.

Trebuie de menționat că informația de contact a DPO trebuie publicată într-o formă vizibilă, clară și ușor accesibilă și trebuie plasată pe site-ul oficial și la sediul operatorului/persoanei împuternicite de operator, astfel încât să permită publicului, adică subiecților de date să ia legătură cu acesta, dacă apare necesitatea. Această informație de contact poate include adresa poștală, numărul de telefon de serviciu, adresa poștei electronice de serviciu sau un formular special de adresare către DPO. Numele responsabilului de protecția datelor nu este necesar, dar poate fi furnizat, dacă să consideră a fi util.

Sarcinile DPO includ cel puțin obligația de a monitoriza conformitatea cu legislația în domeniul protecției datelor (inclusiv efectuarea controalelor, sensibilizarea opiniei publice și instruirea personalului). În acest scop, DPO poate colecta informații pentru identificarea operațiunilor de prelucrare, analiza și controla conformitatea activităților de prelucrare, informa, oferi sfaturi și recomandări operatorului sau persoanei împuternicite de operator, ajuta operatorul și/sau persoana împuternicită de operator în ceea ce privește evaluarea impactului asupra protecției datelor (DPIA), în special prin explicarea necesității de a efectua această evaluare și de a coopera cu autoritatea de supraveghere. Mai mult, DPO poate fi însărcinat cu evidența activităților de prelucrare, care în mod oficial constituie una din obligațiile operatorului. Având în vedere că înregistrările trebuie considerate drept unul din instrumentele care permit responsabilului de protecția datelor să-și îndeplinească sarcina de monitorizare a conformității, informare și îndrumare a operatorului sau persoanei împuternicite de operator, ele pot fi considerate drept un mijloc care-i facilitează lucrul. Responsabilii de protecția datelor, de asemenea, pot îndruma operatorul și/sau persoana împuternicită de operator în cazuri de incidente de securitate și pot ajuta la îndeplinirea procedurii de notificare a încălcării securității datelor. În cele din urmă, în toate atribuțiile sale DPO trebuie să adopte o abordare bazată pe risc, ceea ce înseamnă că el trebuie să-și organizeze activitățile în ordine de prioritate și să-și concentreze eforturile asupra problemelor ce prezintă riscuri mai ridicate la adresa securității datelor.

În concluzie, trebuie de accentuat că responsabilii de protecția datelor au obligația de a păstra secretul sau confidențialitatea cu privire la îndeplinirea sarcinilor sale, însă această obligație de păstrare a secretului/confidențialității prevăzută pentru DPO nu interzice acestuia să contacteze și să consulte autoritatea de supraveghere.

De asemenea, este de menționat că rolul responsabilului de protecția datelor este în primul rând unul consultativ, ceea ce însemnă că chiar dacă opinia și aportul acestuia trebuie luate în considerare cu atenție și respectate, el personal nu poate fi tras la răspundere pentru o eventuală neconformitate cu cerințele privind protecția datelor în raport cu activitățile de prelucrare ale operatorului și/sau persoanei împuternicite de operator. Operatorul sau persoana împuternicită de operator trebuie să asigure și, conform principiului de responsabilitate, să fie în stare să demonstreze că prelucrarea are loc în conformitate cu legea privind protecția datelor cu caracter personal. Conformitatea cu prevederile legislației este în primul rând responsabilitatea operatorului sau a persoanei împuternicite de operator.

Ținând cont de cele enunțate mai sus, desemnarea unui responsabil calificat de protecția datelor trebuie să constituie o prioritate în domeniul aplicării legii.