

**Către: INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE**  
**Subiect: Solicitare de clarificări licitație deschisă CN1014432**

Nr. ieșire: 181/05.09.2019

## **Solicitare de clarificări**

Referitor la procedura de licitație deschisă, înregistrată în SICAP sub nr. CN1014432, având ca obiect furnizarea unei **Soluții informatică pentru recunoaștere facială + training**, în cadrul proiectului „Dezvoltarea sistemului de identificare și recunoaștere facială (NBIS) și interconectarea acestuia cu autoritățile de aplicare a legii din UE prin intermediul sTESTA”, organizată de INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE, **în vederea identificării unei soluții tehnice care să corespundă cerințelor caietului de sarcini dar care să asigure în același timp o funcționalitate reală și eficientă a sistemului, implicit prin respectarea legislației incidente aplicabile la nivel european sau național, vă rugăm să ne clarificați următoarele aspecte:**

**Premisă:** În vederea implementării sistemului de recunoaștere facială, autoritatea contractantă avea obligația realizării unei evaluări a impactului prelucrării de date (DPIA), în conformitate cu [Decizia](#) Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal, dar și conform Art. 32 din [Legea nr. 363/2018](#).

**Solicitare 1:** Autoritatea contractantă a realizat o DPIA privind implementarea unei soluții de recunoaștere facială?

**Solicitare 2:** În cazul în care a fost realizată o DPIA, va rugăm să ne prezentați concluziile acesteia.

**Premisă:** Conform dispozițiilor art. 10 din [Legea nr. 363](#) din 28 decembrie 2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, **prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice se poate realiza numai dacă sunt strict necesare 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.

Mai mult, art. 11 din Legea nr. 363/2018 prevede că:

- 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 prevăzute la 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.”

**Solicitare 3:** Vă rugăm să ne comunicați, în mod explicit, care sunt **garanții adecvate pentru drepturile și libertățile persoanei vizate pe care Autoarea Contractantă le-a luat în calcul atunci când a proiectat cerințele sistemului de recunoaștere facială**, pentru a asigura viabilitatea sistemului, în conformitate cu dispozițiile art. 10 din Legea nr. 363/2018.

**Solicitare 4:** Vă rugăm să ne indicați **dispozițiile legale exprese** care reglementează prelucrările de date asociate sistemului de recunoaștere ce face obiectul prezentei achiziții, conform cerințelor art. 11(1) din Legea nr. 363/2018.

**Solicitare 5:** Vă rugăm să ne prezentați care sunt **măsurile corespunzătoare** care vor fi instituite pentru protejarea drepturilor, a libertăților și a intereselor legitime ale persoanei vizate, obligatorii conform art. 11(2) din Legea nr. 363/2018.

**Solicitare 6:** Vă rugăm să ne indicați în mod explicit care sunt „**pericolele iminente**” (art. 10 din Legea nr. 363/2018) pentru care se va utiliza sistemul, având în vedere că la art. 2.2 din în caietul de sarcini sunt prezentate mai multe activități ale IGPR în care va fi folosit sistemul de recunoaștere facială, însă nu toate se încadrează, în accepțiunea noastră în categoria de „pericol iminent cel puțin asupra vieții, integrității corporale sau sănătății”.

Implementarea unei tehnologii în domeniul recunoașterii faciale va permite Poliției Române să includă această metodă ca măsură în combaterea și elucidarea cazurilor asociate furtului de identitate sau documentelor pierdute ori furate, precum și identificarea suspectilor care comit sau intenționează să comită fapte de natură penală (terorism, infracțiuni cu violență etc.).

*extras din caietul de sarcini, art. 2.2, pag 2*

**Premisă:** Art. 12 (1) din Legea nr. 363/2018 prevede că „Operatorii sunt obligați să instituie **măsurile organizatorice, tehnice și de procedură** pentru a furniza persoanei vizate informațiile necesare potrivit prevederilor art. 13 și art. 16-21 și pentru a asigura transmiterea unui răspuns în legătură cu prelucrările desfășurate în condițiile prevăzute la art. 11 sau în legătură cu notificarea persoanelor vizate în cazul apariției unui incident de securitate, în condițiile prevederilor art. 39”.

**Solicitare 7:** Care sunt cerințe ale Autorității contractante cu privire la funcționalitățile sistemului de recunoaștere facială care vor asigura respectarea prevederilor art. 13 și art. 16-21 din Legea nr. 363/2018?

**Premisă:** Conform dispozițiilor art. 25 al [Regulamentului General privind Protecția Datelor](#) (Regulamentul UE 679/2016) prin care se instituie obligativitatea asigurării protecției datelor începând cu momentul conceperii (“privacy by design”) și pe toata durata de viață a sistemului (“privacy by default”), considerand caracterul controversat al sistemelor de recunoaștere facială la nivel mondial, în momentul stabilirii mijloacelor de prelucrare Operatorul are obligația de a aplica măsuri tehnice și organizatorice adecvate și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

**Solicitare 8:** Vă rugăm sa ne comunicați care sunt solicitările punctuale ale Autorității contractante privind securitatea sistemului de recunoaștere facială, prin care se va asigura respectarea obligației privind asigurarea protecției datelor începând cu momentul conceperii (“privacy by design”) și pe toata durata de viață a sistemului ce face obiectul achiziției, în special în ceea ce privește prelucrarea datelor biometrice (protocoale, certificări, autorizații, etc.).

**Premisă:** Conform dispozițiilor art. 33 din Legea nr. 363/2018, operatorul sau persoana împuternicită de către operator este obligat să consulte autoritatea de supraveghere înainte de prelucrarea datelor cu caracter personal care fac parte dintr-un sistem nou atunci când 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 sau când tipul de prelucrare, în special în cazul în care se utilizează noi tehnologii, mecanisme sau proceduri, implică un risc ridicat la adresa drepturilor și libertăților persoanelor vizate. Mai mult, conform art. 49 interoperabilizarea sistemelor de evidență a datelor cu caracter personal sunt posibile numai cu consultarea prealabilă a autorității de supraveghere.

**Solicitare 9:** Va rugăm să ne comunicați dacă autoritatea contractantă a consultat Autoritatea Națională de Supraveghere ([ANSPDPC](#)) înainte de proiectarea sistemului de monitorizare facială care face obiectul prezentei proceduri.

**Solicitare 10:** În cazul în care Autoritatea de Supraveghere a fost consultată, vă rugăm sa ne puneți la dispoziție punctul de vedere al acesteia cu privire la implementarea sistemului de recunoaștere facială.

Vă rugăm sa ne prezentați punctul dumneavoastră de vedere cu privire la aspectele menționate mai sus.

Vă mulțumim!