ROMÂNIA
AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld. Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poștal 010336, București, Tel: +40 31 805 9211, Fax: +40 31 805 9602, www.dataprotection.ro, e-mail: anspdcp@dataprotection.ro

6b-8/283
26 05 11

Stimată Doamnă Secretar,

Vă supunem atenției următoarele aspecte legate de întrebarea formulată de domnul deputat Mihai-Adrian Țiu, având ca obiect *legalitatea pontării angajaților folosind datele biometrice și sancțiunile prevăzute de lege pentru această prelucrare,* adresată Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, prin adresa Camerei Deputaților – Cabinet Secretar nr. 6b-8/230 din 20.05.2026, înregistrată la instituția noastră sub nr. 16837 din 25.05.2026.

Art. 4 pct. 14 din Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE ("GDPR") definește **datele biometrice** ca fiind "date cu caracter personal care **rezultă în urma unor tehnici de prelucrare specifice** referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice".

În acest context, precizăm că în documentul intitulat **"Avizul 4/2007 privind conceptul de date cu caracter personal"**, Grupul de Lucru Art. 29 (în prezent Comitetul European pentru Protecția Datelor) precizează următoarele: "Aceste date [datele biometrice] pot fi definite ca proprietăți biologice, caracteristici fiziologice, trăsături vitale sau acțiuni repetate, atât trăsăturile cât și/sau acțiunile fiind caracteristice persoanei și fiind măsurabile, chiar dacă modelele utilizate în practică pentru măsurarea din punct de vedere tehnic a acestora implică un anumit grad de probabilitate. Exemple tipice ale unor asemenea date biometrice sunt amprentele digitale, modelele retinei, structura feței, vocile, precum și geometria mâinii, modelele sangvine sau chiar unele aptitudini înrădăcinate sau alte trăsături comportamentale (precum semnătura de mână, felul de a se mișca, în special felul de a merge sau de a vorbi etc.)".

Corelat cu cele de mai sus, în documentul intitulat **"Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice"**, Grupul de Lucru Art. 29 menționează că "există două categorii principale de tehnici biometrice", unele dintre acestea referindu-se la "tehnici bazate pe caracteristici fizice și fiziologice, care măsoară caracteristicile fizice și fiziologice ale unei persoane și care includ: verificarea amprentelor digitale, analiza imaginii degetului, recunoașterea irisului, analiza retinei, recunoașterea facială, modelul conturului mâinii, recunoașterea formei urechilor, detectarea mirosului corporal, recunoașterea vocală, analiza tiparului ADN, analiza porilor sudoripari etc."

În ceea ce privește prelucrarea **datelor biometrice**, precizăm că aceasta face parte din categoria datelor cu caracter sensibil și este supusă condițiilor **art. 9** din GDPR.

Astfel, conform art. 9 alin. (2) lit. a) din GDPR, datele cu caracter sensibil pot fi prelucrate dacă persoana vizată și-a dat **consimțământul explicit** pentru prelucrarea acestor date pentru unul sau mai multe scopuri specifice.

De asemenea, dispozițiile art. 9 alin. (2) lit. b) din GDPR, precizează că datele cu caracter sensibil pot fi prelucrate dacă aceasta este necesară în scopul îndeplinirii obligațiilor și al

exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate.

Aceste prevederi se coroborează cu cele de la art. 5 din GDPR unde se regăsesc principiile de prelucrare a datelor, printre care și cel referitor la legalitatea prelucrării. Astfel, datele cu caracter personal trebuie să fie "prelucrate în mod **legal**, echitabil și transparent față de persoana vizată ("legalitate, echitate și transparență")".

În ceea ce privește consimțământul persoanei vizate, art. 4 pct. 11 din GDPR precizează că acesta înseamnă orice manifestare de voință liberă, specifică, informată și **lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă**, printr-o declarație sau **printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.**

De asemenea, **art. 7** din același regulament prevede condițiile de obținere a consimțământului, inclusiv sub aspectul demonstrării, de către operator, a obținerii acestuia.

În același timp, referitor la valabilitatea consimțământului angajaților, precizăm că, în Ghidul nr. 05/2020 privind consimțământul în temeiul Regulamentului (UE) **2016/679,** emis de Comitetul European pentru Protecția Datelor, se menționează faptul că "Un dezechilibru de putere apare, de asemenea, în contextul relațiilor de muncă. Având în vedere dependența care rezultă din relația dintre angajator și angajat, este puțin probabil ca persoana vizată să poată refuza să-și acorde consimțământul față de angajatorul său pentru prelucrarea datelor fără a se confrunta cu temerea sau cu riscul real de consecințe negative ca urmare a unui refuz. Este puțin probabil ca un angajat să poată răspunde în mod liber la o cerere de consimțământ din partea angajatorului său. (...) Având în vedere dezechilibrul de putere dintre un angajator și membrii personalului său, **angajații își pot da consimțământul în mod liber numai în circumstanțe excepționale,** și anume atunci când nu va exista nicio consecință negativă, indiferent dacă aceștia consimt sau nu."

Pe de altă parte, sub aspectul **proporționalității** prelucrării preconizate **de date biometrice ale angajaților în scopul accesului și pontajului, reiterăm că art. 5 din GDPR stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor.** În ceea ce privește principiul proporționalității, acesta stabilește că datele sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor") și prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").

Astfel, în ceea ce privește **proporționalitatea** instituirii unei asemenea măsuri, Grupul de Lucru precizează, în documentul **"Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice"**, anterior menționat, faptul că: "Utilizarea biometriei ridică problema proporționalității fiecărei categorii de date prelucrate în lumina scopului în care sunt prelucrate acestea. Având în vedere faptul că datele biometrice pot fi utilizate numai dacă sunt adecvate, relevante și neexcesive, trebuie să se evalueze cu exactitate necesitatea și proporționalitatea datelor prelucrate și să se analizeze dacă scopul urmărit ar putea fi atins într-un mod mai puțin intruziv."

În acest context, subliniem că potrivit principiului responsabilității, **operatorul trebuie să demonstreze că prelucrarea se efectuează în conformitate cu GDPR.**

În ceea ce privește responsabilitatea operatorului, **art. 24** din GDPR prevede că "Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare **măsuri tehnice și organizatorice adecvate** pentru a garanta și **a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu**

prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar."

Precizăm că potrivit principiului responsabilității, operatorul trebuie să **demonstreze** că prelucrarea se efectuează în conformitate cu GDPR, iar atunci când măsurile luate sunt proporționale în raport cu operațiunile de prelucrare, acestea includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

De asemenea, operatorul trebuie să asigure, în conformitate cu **art. 25** din GDPR, protecția datelor începând cu momentul conceperii și în mod implicit (principiile privacy by design și privacy by default).

În același timp, menționăm că, pentru sectorul privat, regimul sancționator aplicabil este prevăzut de art. 83 din GDPR.

În contextul celor menționate și al necesității asigurării unei protecții eficiente a dreptului la viață privată și la protecția datelor personale, raportat la principiul proporționalității prelucrărilor, instituția noastră a sancționat în mai multe rânduri prelucrarea de către operatori a datelor biometrice ale angajaților proprii considerând aceasta ca fiind excesivă raportat la scopul urmărit, respectiv acces și pontaj. (a se vedea, printre altele și comunicatul de presa din 2 iunie 2016, accesibil la adresa https://www.dataprotection.ro/?page=sanctiuni_mai&lang=ro).

De altfel, **această abordare a fost confirmată în mai multe rânduri și de hotărârile pronunțate de instanțele de judecată.**

Față de cele de mai sus, precizăm că, în lipsa unui act normativ de nivelul legii care să prevadă garanții adecvate pentru protecția datelor personale, având în vedere natura sensibilă a datelor care necesită protecție, raportat la principiul proporționalității instituit de art. 5 din GDPR, la condițiile de obținere a consimțământului prevăzute de art. 7 din același regulament, la prevederile art. 9 GDPR, precum și aplicabilitatea acestora în relația angajat-angajator, rezultă că nu este legitimă, necesară și proporțională prelucrarea datelor menționate prin raportare la scopul declarat (pontaj angajați), fiind necesară alegerea unei alte soluții mai puțin intruzive pentru atingerea respectivului scop, care nu implică prelucrarea datelor biometrice ale persoanelor vizate – angajați.

Cu deosebită considerație,

Ancuța Gianina OPRE,

PREȘEDINTE

Doamnei Oana MURARIU, Secretar al Camerei Deputaților
Parlamentul României