PRELUCRAREA DATELOR BIOMETRICE

OPERATOR	Responsabil cu protecţia datelor personale
DIRECŢIA GENERALĂ DE PAŞAPOARTE Instituţie publică în cadrul Ministerul de Interne Sediul: str. Nicolae Iorga nr. 27, sector 1, Bucureşti	Str. Nicolae Iorga nr. 27, sector 1, Bucureşti Email:protecţiadatelor.dgp@mai.gov.ro

La depunerea cererii pentru eliberarea paşapoartelor simple electronice la serviciul public comunitar pentru eliberarea şi evidenţa paşapoartelor simple, solicitantului i **se preiau impresiunile digitale şi imaginea facială**, aşa cum este prevăzut în Legea 248/2007 privind regimul liberei circulaţii a cetăţenilor români în străinătate, cu modificarile si completarile ulterioare şi Hotărârea Guvernului nr. 94/2006 pentru aprobarea Normelor metodologice de aplicare a Legii. Regula generală este de preluare a amprentelor plane ale arătătorului stâng şi arătătorului drept. În situaţia în care amprentele degetelor arătătoare stâng şi drept nu au calitate corespunzătoare şi/sau prezintă leziuni, se înregistrează amprentele plane de bună calitate ale degetelor mijlocii, inelarelor sau degetelor mari.

Aveţi dreptul de acces la datele stocate în cipul din paşaportul electronic, astfel că în momentul ridicării documentului puteţi solicita vizualizarea acestor date, în condiţii de securitate şi confidenţialitate.

Sunt preluate în vederea înregistrării numai două impresiuni digitale care sunt salvate în baza de date şi ulterior inscripţionate în mediul electronic de stocare – respectiv în cip (conform prevederilor Regulamentului (CE) 2252/2004 şi Documentului ICAO 9303 Partea I, anexa G).

Regula generală este de preluare a amprentelor plane ale arătătorului stâng şi arătătorului drept. În cazul în care amprentele degetelor arătătoare stâng şi drept nu au calitate corespunzătoare şi/sau prezintă leziuni este necesar să se înregistreze amprentele plane de bună calitate a degetelor mijlocii, inelarelor sau mari. Formatul standardului de stocare NIST (CBEFF – cadru comun pentru formatele de schimb de date biometrice) menţionează degetul de la care s-a prelevat amprenta, pentru a putea fi verificat degetul corect.)

Mediul de stocare electronic conţine următoarele categorii de date:

- **imaginea facială** în conformitate cu normele ICAO. ,,Imaginea facială conform formatului de schimb al datelor biometrice, înregistrată în grupul de date 2 (al structurii datelor logice) este derivată de la fotografia de paşaport utilizată pentru a crea imaginea imprimată pe pagina ce conţine datele din paşaport cu citire optică şi va fi codificată conform formatului de tip 2 (imaginea facială completă) sau formatul de tip 3 (imagine token) stabilite în ultima versiune a normei ISO 19794-5". Imaginea facială este stocată ca fişier de imagine comprimat.
- Cele **două amprente** prelevate în format de stocare NIST.
- Conform structurii datelor logice ICAO, **datele alfanumerice ale zonei de lectură optică (MRZ)** a documentului şi datele numerice de securizare ale documentului (PKI) sunt stocate în cip împreună cu identificatori biometrici (imaginea facială şi cele două amprente).

Impresiunile digitale şi imaginea facială colectate în scopurile prevazute la art. 4 alin. (3) din *Regulamentul (CE)2252/2004 al Consiliului din 13 decembrie 2004 privind standardele pentru elementele de securitate şi elementele biometrice integrate în paşapoarte şi în documente de călătorie emise de statele membr, cu completările ulterioare,* se includ în mediul de stocare electronică a paşaportului simplu electronic şi se stochează în baza de date a Sistemului naţional informatic de evidenţă a pasapoartelor simple şi în bazele de date de producţie gestionate potrivit art. 4 lit. c) din Hotararea Guvernului nr. 1319/2008 privind organizarea si functionarea Centrului National Unic de Personalizare a Pasapoartelor Electronice.

După personalizarea pasaportului simplu electronic şi transmiterea acestuia la autoritatea competentă să îl elibereze, datele biometrice stocate în bazele de date de producţie se şterg prin procedura automată.

Impresiunile digitale stocate în baza de date a Sistemului naţional informatic de evidenţă a paşapoartelor simple se şterg prin procedură automată imediat după ridicarea pasaportului simplu electronic în conditiile art. 14 sau, dacă nu a fost ridicat în astfel de condiţii, cel târziu la împlinirea unui termen de 3 luni de la data programată pentru eliberarea acestuia. Impresiunile digitale nu fac obiectul unei stocări centralizate şi nu sunt destinate dezvăluirii către terţi.

Imaginea facială este stocată în baza de date a Sistemului naţional informatic de evidenţă a pasapoartelor simple ca fişier de imagine comprimat. Termenul de stocare este permanent iar scopul stocării imaginii faciale este verificarea identităţii persoanei în asocierea „persoană – date" (în vederea înlăturării încercărilor de obţinere a documentelor de calătorie prin fals de identitate).

Stocarea amprentelor până la momentul eliberării paşaportului către cetăţean este necesară pentru ca în cazul în care se constată, în momentul eliberării paşaportului, neconcordanţe între datele tipărite pe acesta şi datele reale ale solictantului (erori de operare la nume, prenume, data naşterii etc), paşaportul să poată fi produs din nou, cu corecţiile

necesare, fără a mai fi nevoie de depunerea unei noi cereri şi înregistrarea amprentelor.

Aceste măsuri sunt menite să combată mai eficient frauda şi falsificarea documentelor. În plus, datele sunt securizate şi suportul de stocare are o capacitate suficientă pentru a garanta integritatea, autenticitatea şi confidenţialitatea datelor conform **politicii de securitate** adoptată la nivelul instituţiei.

Potrivit prevederilor Regulamentului Consiliul Uniunii Europene nr. 2252/1312.2004 şi a Deciziei COM (2009)7476, la nivelul Direcţiei Generale de Paşapoarte a fost constituit Punctul Unic de Contact (S.P.O.C.). SPOC face parte din infrastructura privind cheile publice de decriptare a informaţiei incluse pe cip-ul aferent documentelor de călătorie din UE (cunoscută sub denumirea PKI, cu rolul de a asigura integritatea şi autenticitatea datelor incluse in cip).

Pentru protecţia vieţii private, la nivel UE s-a decis ca, dintre toate categoriile de date incluse pe cip, autorităţile competente din Statele Membre să aibă acces, respectiv să poată citi amprentele digitale dintr-un document de călătorie electronic, doar cu autorizaţia prealabilă, suplimentară, a statului care a emis documentul (procedură denumită EAC – Extended Acces Control).

*Operaţiunea de citire a datelor privind amprentele de pe cip, include o serie de teste, respectiv: **1**. BAC (Basic Access Control), care a fost suplimentat cu PACE (Password Authenticated Connection Establishment) – permiţând deschiderea conţinutului cip-ului şi verificarea autenticităţii datelor **2**. autentificarea pasivă, care permite verificarea corespondenţei dintre date şi semnăturile asociate, pentru a verifica sursa datelor **3**. **EAC (Controlul Extins al Accesului** – prin care cip-ul "testează"cititorul. EAC include atât testul de autentificare a cipului, respectiv că a fost emis de emitentul corect şi autentificarea terminalului, respectiv că cititorul este autorizat să acceseze aceste date.*

Respectarea drepturilor fundamentale ale persoanelor vizate şi protecţia datelor cu caracter personal prelucrate de către Direcţia Generală de Paşapoarte, sunt obiective majore, a căror îndeplinire, prin asigurarea şi aplicarea unor garanţii eficiente, a fost permanent monitorizată de conducerea instituţiei noastre, conştienţi fiind de importanţa, complexitatea şi implicaţiile acestui domeniu.