



PRELUCRAREA DATELOR BIOMETRICE

OPERATOR Responsabil cu protecția datelor
personale
SERVICIUL PUBLIC COMUNITAR PENTRU
ELIBERAREA ȘI EVIDENȚA
PAȘAPOARTELOR SIMPLE IAȘI
Sediul: Bld. Primăverii nr. 36, Iași Bld. Primăverii nr. 36, Iași
Email: pasapoarte@prefecturaiasi.ro

La depunerea cererii pentru eliberarea pașapoartelor simple electronice la serviciul public comunitar pentru eliberarea și evidența pașapoartelor simple, solicitantului i se preiau impresiunile digitale și imaginea facială, așa cum este prevăzut în Legea 248/2007 privind regimul liberei circulații a cetățenilor români în străinătate, cu modificările și completările ulterioare și [Hotărârea Guvernului nr. 94/2006](#) pentru aprobarea Normelor metodologice de aplicare a Legii. Regula generală este de preluare a amprentelor plane ale arătătorului stâng și arătătorului drept. În situația în care amprentele degetelor arătătoare stâng și drept nu au calitate corespunzătoare și/sau prezintă leziuni, se înregistrează amprentele plane de bună calitate ale degetelor mijlocii, inelarelor sau degetelor mari.

Aveți dreptul de acces la datele stocate în cipul din pașaportul electronic, astfel că în momentul ridicării documentului puteți solicita vizualizarea acestor date, în condiții de securitate și confidențialitate.

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

Regula generală este de preluare a amprentelor plane ale arătătorului stâng și arătătorului drept. În cazul în care amprentele degetelor arătătoare stâng și drept nu au calitate corespunzătoare și/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) menționează degetul de la care s-a prelevat amprenta, pentru a putea fi verificat degetul corect.)



Mediul de stocare electronic conține 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 pașaport utilizată pentru a crea imaginea imprimată pe pagina ce conține datele din pașaport cu citire optică și 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 fișier 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 și datele numerice de securizare ale documentului (PKI) sunt stocate în cip împreună cu identificatori biometrici (imaginea facială și cele două amprente).

Impresiunile digitale și 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 și elementele biometrice integrate în pașapoarte și în documente de călătorie emise de statele membr, cu completările ulterioare*, se includ în mediul de stocare electronică a pașaportului simplu electronic și se stochează în baza de date a Sistemului național informatic de evidență a pasapoartelor simple și în bazele de date de producție gestionate potrivit art. 4 lit. c) din Hotărârea Guvernului nr. 1319/2008 privind organizarea și functionarea Centrului National Unic de Personalizare a Pasapoartelor Electronice.

După personalizarea pașaportului simplu electronic și transmiterea acestuia la autoritatea competentă să îl elibereze, datele biometrice stocate în bazele de date de producție se șterg prin procedura automată.

Impresiunile digitale stocate în baza de date a Sistemului național informatic de evidență a pașapoartelor simple se șterg prin procedură automată imediat după ridicarea pașaportului simplu electronic în condițiile art. 14 sau, dacă nu a fost ridicat în astfel de condiții, cel târziu la împlinirea unui termen de 3 luni de la data programată pentru eliberarea acestuia. Impresiunile digitale nu fac obiectul unei stocări centralizate și nu sunt destinate dezvăluirii către terți.

Imaginea facială este stocată în baza de date a Sistemului național informatic de evidență a pasapoartelor simple ca fișier de imagine comprimat. Termenul de stocare este permanent iar scopul stocării imaginii faciale este verificarea identității persoanei în asocierea „persoană - date” (în vederea înlăturării încercărilor de obținere a documentelor de călătorie prin fals de identitate).

Stocarea amprentelor până la momentul eliberării pașaportului către cetățean este necesară pentru ca în cazul în care se constată, în momentul eliberării pașaportului, neconcordanțe între datele tipărite pe acesta și datele reale ale solicitantului (erori de operare la nume, prenume, data nașterii etc), pașaportul să poată fi produs din nou, cu corecțiile



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

Aceste măsuri sunt menite să combată mai eficient fraudă și falsificarea documentelor. În plus, datele sunt securizate și suportul de stocare are o capacitate suficientă pentru a garanta integritatea, autenticitatea și confidențialitatea datelor conform politicii de securitate adoptată la nivelul instituției.

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

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

Operațiunea 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) - permițând deschiderea conținutului cip-ului și verificarea autenticității datelor 2. autentificarea pasivă, care permite verificarea corespondenței dintre date și 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 și autentificarea terminalului, respectiv că cititorul este autorizat să acceseze aceste date.

Respectarea drepturilor fundamentale ale persoanelor vizate și protecția datelor cu caracter personal prelucrate de către Direcția Generală de Pașapoarte, sunt obiective majore, a căror îndeplinire, prin asigurarea și aplicarea unor garanții eficiente, a fost permanent monitorizată de conducerea instituției noastre, conștienți fiind de importanța, complexitatea și implicațiile acestui domeniu.

