UDHËZIM I PËRBASHKËT
Nr. 93, datë 5.5.2026

PËR TRANSMETIMIN E TË DHËNAVE TË UDHËTIMIT NË RASTET E MOSFUNKSIONIMIT TË SISTEMIT KRYESOR TË PËRPUNIMIT TË INFORMACIONIT TË UDHËTIMIT

Në mbështetje të pikës 4, të nenit 102 të Kushtetutës dhe të nenit 5, pika 9, të ligjit nr. 38/2025, "Për përpunimin e informacionit të udhëtimit në Republikën e Shqipërisë", ministri i Punëve të Brendshme dhe Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale,

UDHËZOJNË:

1. QËLLIMI

Qëllimi i këtij udhëzimi është:

a) Të përcaktojë rregullat, procedurat dhe masat e standardizuara për transmetimin, marrjen, përpunimin dhe ruajtjen e të dhënave të udhëtimit nga transportuesit ajrorë, tokësorë dhe detarë drejt Sektorit të Inteligjencës së Udhëtimit (SIU), në rastet kur sistemi kryesor i transmetimit të të dhënave të udhëtimit nuk funksionon, duke garantuar vazhdimësinë e përpunimit të të dhënave, nivel të përshtatshëm mbrojtjeje dhe përdorim të kontrolluar të aplikacionit alternativ;

b) Të sigurojë funksionimin e pandërprerë, të sigurt dhe të kontrolluar të procesit të shkëmbimit të të dhënave të udhëtimit, edhe në rastet kur sistemi kryesor pëson mangësi ose avari teknike;

c) Të garantojë që SIU-ja të ketë akses në kohë dhe në mënyrë të strukturuar tek të dhënat e udhëtimit, për qëllime të parandalimit, zbulimit, analizimit dhe profilizimit të rreziqeve të sigurisë që lidhen me krimin e organizuar, terrorizmin, migracionin e paligjshëm dhe veprimtari të tjera penale në fushën e kompetencave ligjore të Policisë së Shtetit;

d) Të harmonizojë proceset e transmetimit të të dhënave nga transportuesit me kërkesat teknike dhe operacionale të sistemit të ngritur pranë SIU-ve, duke garantuar cilësinë, integritetin, disponueshmërinë dhe konfidencialitetin e të dhënave të administruara;

e) Të sigurojë që çdo përpunim i të dhënave nga SIU-të të kryhet në përputhje me parimet themelore të ligjshmërisë, transparencës, minimizimit, proporcionalitetit, kufizimit të ruajtjes dhe përgjegjshmërisë sipas Rregullores për Mbrojtjen e të dhënave të Bashkimit Evropian (GDPR) dhe të ligjit nr. 124/2024, "Për mbrojtjen e të dhënave personale";

f) Të përcaktojë detyrime të qarta për transportuesit dhe për strukturat përgjegjëse të SIU-të, lidhur me përdorimin e aplikacionit alternativ, regjistrimin, auditimin, transferimin dhe fshirjen e të dhënave të grumbulluara gjatë periudhës së mosfunksionimit të sistemit kryesor;

g) Të krijojë një bazë të qartë operacionale dhe ligjore, që i mundëson SIU-së të ndërtojë analiza inteligjence, profile rreziku, sinjalizime operacionale, si dhe të rrisë efikasitetin në bashkëpunimin ndërinstitucional dhe ndërkombëtar.

2. FUSHA E ZBATIMIT

2.1 Në rast shfaqjeje të një problemi apo mangësie teknike të sistemit, të tilla si probleme teknike të infrastrukturës përkatëse dhe linjës së transmetimit, transportuesit ajrorë, ujorë dhe tokësorë, në kuadër të përmbushjes së detyrimeve ligjore të tyre, do të dërgojnë të dhënat e udhëtimit, sipas formatit të përcaktuar, në përputhje me nevojat e sistemit të ngritur, në një aplikacion alternativ për përpunimin e të dhënave të udhëtimit.

2.2 Udhëzimi zbatohet plotësisht në rastet kur transportuesit apo SIU-të hasin:

a) avari teknike;

b) mungesë të lidhjes së sistemit kryesor të përpunimit të informacionit të udhëtimit;

c) dështime të përkohshme të infrastrukturës teknologjike.

Në këto raste përdoret aplikacioni alternativ, duke respektuar të gjitha kërkesat e privatësisë dhe sigurisë.

3. APLIKACIONI ALTERNATIV

Aplikacioni alternativ për përpunimin e të dhënave të udhëtimit është një mjet rezervë (*fallback system*) i vënë në dispozicion nga SIU-ja, i destinuar të përdoret vetëm në rastet kur sistemi kryesor elektronik i transmetimit dhe përpunimit të të dhënave të udhëtimit nuk është operacional për shkak të një defekti, avarie teknike, mungese lidhjeje ose situate tjetër të papritur teknologjike.

Aplikacioni alternativ garanton vazhdimësinë e përpunimit të të dhënave dhe parandalon vonesat në analizën e rrezikut, duke siguruar që funksionet e sigurisë kombëtare dhe kontrollit kufitar të mos ndërpriten.

3.1 Qëllimi i aplikacionit alternativ

Aplikacioni alternativ, synon:

a) të mundësojë transmetimin e pandërprerë të të dhënave të udhëtimit dhe të dhënave të tjera të udhëtimit drejt SIU-së;

b) të sigurojë redundancë operative në rast dështimi të sistemit primar;

c) të garantojë që SIU-ja të ketë akses në kohë reale në të dhënat kritike për analizën e rrezikut;

d) të mbajë standardet e privatësisë dhe mbrojtjes së të dhënave në nivel të barabartë me sistemin kryesor.

3.2 Aktivizimi i aplikacionit alternativ

Aplikacioni alternativ përdoret vetëm në rastet, kur:

a) transportuesi nuk mund të transmetojë të dhëna në sistemin kryesor për shkak të defekteve teknike;

b) sistemi kryesor i SIU-së ka ndërprerje, ngadalësim serioz ose avari;

c) infrastruktura e komunikimit është e pamundur ose e pasigurt;

d) ka mangësi të përkohshme të serverëve të Policisë së Shtetit.

SIU-ja njofton transportuesit kur sistemi primar ka kaluar në gjendjen “jo operacionale”.

3.3 Procedurat e transmetimit në aplikacionin alternativ

Transportuesit janë të detyruar që:

a) të transmetojnë ndërmjet mjeteve rezervë të autorizuara nga SIU-ja (aplikacion *web*, API alternative, format të siguruar *fallback*);

b) të dërgojnë të dhënat në të njëjtin nivel cilësie dhe saktësie si në sistemin kryesor;

c) të përditësojnë të dhënat e udhëtimit sipas afateve ligjore edhe gjatë funksionimit të aplikacionit alternativ (48–24 orë, 180 minuta, 60 minuta, pas imbarkimit).

3.4 Administrimi i të dhënave në aplikacionin alternativ nga SIU-ja

SIU-ja kryen këto veprime:

a) regjistrimin e çdo transmetimi të kryer në aplikacionin alternativ;

b) verifikimin e saktësisë së të dhënave të dërguara;

c) krahasimin e tyre me strukturat e të dhënave të sistemit kryesor;

d) monitorimin e performancës teknike të aplikacionit rezervë;

e) garantimin e aksesit të kufizuar dhe të gjurmueshëm nga personeli i SIU-së.

f) verifikon automatikisht çdo të dhënë të marrë për integritet, plotësi dhe përputhshmëri.

3.5 Transferimi i të dhënave në sistemin kryesor

Sapo sistemi kryesor rikthehet në funksion:

a) të dhënat e regjistruara në aplikacionin alternativ transferohen automatikisht në sistemin primar;

b) SIU-ja verifikon përputhshmërinë dhe integritetin e të dhënave;

c) dokumentohet çdo hap i procesit të transferimit.

Ky proces garantohet nga strukturat e teknologjisë së informacionit të Drejtorisë së Përgjithshme të Policisë së Shtetit.

3.6 Fshirja e të dhënave nga aplikacioni alternativ

Pasi të dhënat janë transferuar me sukses:

a) ato fshihen menjëherë nga aplikacioni alternativ;

b) fshirja regjistrohet dhe dokumentohet në *log*-et e auditimit;

c) SIU-ja siguron që asnjë kopje e të dhënave të mos mbetet në sistemin rezervë.

Kjo procedurë është e detyrueshme për të përmbushur parimin e minimizimit, kufizimit të ruajtjes dhe integritetit, sipas GDPR-së dhe ligjit nr. 124/2024.

3.7 Masat e sigurisë në aplikacionin alternativ

Aplikacioni alternativ është i ndërtuar mbi të njëjtat standarde sigurie si sistemi kryesor:

a) enkriptim në transmetim dhe ruajtje (TLS 1.2+/AES-256);

b) kontroll aksesesh me autentikim shumëfaktorësh;

c) logim të detajuar të çdo veprimi;

d) auditim periodik të funksionalitetit dhe sigurisë;

e) izolim të mjedisit rezervë nga sistemet e tjera të PSH-së (*network segmentation*).

4. MBROJTJA E TË DHËNAVE

Sektori i Inteligjencës së Udhëtimit (SIU), transportuesit dhe strukturat teknike të Policisë së Shtetit janë të detyruara të sigurojnë mbrojtjen e të dhënave personale të udhëtarëve gjatë të gjithë ciklit të përpunimit të tyre, në përputhje me parimet e privatësisë dhe kërkesat ligjore në fuqi.

Mbrojtja e të dhënave bazohet në katër elemente themelore: konfidencialiteti, integriteti, disponueshmëria dhe akses i kufizuar.

4.1 Konfidencialiteti i të dhënave

Të dhënat API/PNR dhe të dhënat e tjera të udhëtimit trajtohen vetëm nga personeli i autorizuar, brenda roleve të përcaktuara qartë.

Personeli merr qasje vetëm në të dhënat që i nevojiten për të kryer detyrat funksionale.

Ndalohen rreptësisht:

a) shpërndarja e të dhënave tek persona të paautorizuar;

b) kopjimi, ruajtja ose transferimi i të dhënave në pajisje të paautorizuara;

c) përdorimi i të dhënave për qëllime personale.

Çdo shkelje e konfidencialitetit përbën shkelje administrative dhe penale, sipas ligjeve në fuqi.

4.2 Integriteti i të dhënave

Të dhënat ruhen dhe përpunohen në mënyrë të tillë që të jenë të plota, të sakta dhe të pandryshuara në mënyrë të paautorizuar. Çdo ndryshim, korrigjim ose rifreskim i të dhënave regjistrohet automatikisht në *log*-et e sistemit.

SIU-ja kryen verifikime periodike të integritetit për:

a) parandalimin e manipulimit;

b) identifikimin e anomalive;

c) përputhshmërinë e të dhënave midis sistemit kryesor dhe aplikacionit alternativ.

4.3 Akses i kufizuar dhe i kontrolluar

Aksesi ndaj sistemeve të SIU-ve bëhet vetëm me kredenciale të personalizuara dhe autentikim shumëfaktorësh (MFA). Parimi i qasje minimale (*least privilege*) zbatohet për çdo rol dhe funksion.

Çdo qasje regjistrohet në mënyrë të plotë në *log*-et e auditimit, duke përfshirë:

a) identitetin e përdoruesit;

b) datën dhe orën;

c) të dhënat e aksesit;

d) veprimet e kryera.

Qasja në qendrën fizike të të dhënave lejohet vetëm për personel me autorizim të posaçëm.

4.4 Disponueshmëria dhe vazhdimësia e shërbimit

Sistemet e përpunimit të informacionit të udhëtimit kanë mekanizma sigurie që garantojnë funksionimin e pandërprerë të shërbimit (*High Availability*). Në rast ndërprerjesh, aktivizohet aplikacioni alternativ, i cili siguron vazhdimësinë e procesit.

Rezervat (*backups*) kryhen rregullisht dhe testohen periodikisht për rikuperim.

4.5 Mbrojtja ndaj aksesit të paautorizuar dhe sulmeve kibernetike

SIU-ja dhe transportuesit zbatojnë masa për:

a) *firewalls* dhe IDS/IPS të avancuara;

b) enkriptim të plotë të trafikut të të dhënave;

c) kontroll të integritetit të sistemeve;

d) detektim dhe sinjalizim të menjëhershëm të tentativave të aksesit të paautorizuar;

e) vlerësime të rregullta të cenueshmërisë dhe testime të penetrimit.

4.6 Përdorimi i parimit "*Privacy by Design & by Default*"

Të gjitha procedurat dhe sistemet:

a) ndërtohen duke integruar mbrojtjen e të dhënave që në fazën e projektimit;

b) përdorin konfigurime të paracaktuara të sigurta;

c) minimizojnë të dhënat që përpunohen;

d) sigurojnë konfigurim të qartë të të drejtave të aksesit.

4.7 Menaxhimi i incidenteve të sigurisë së të dhënave

Në rast incidenti me ndikim tek të dhënat personale:

a) SIU-ja kryen vlerësimin e menjëhershëm të incidentit;

b) DPO-ja njoftohet menjëherë;

c) në incidentet që përbëjnë rrezik për subjektet, njoftohet Komisioneri sipas afateve të ligjit;

d) përgatitet raporti i incidentit dhe masat e ndërmarra (*post-incident report*);

e) zbatohen masa parandaluese për të shmangur përsëritjen.

4.8 Detyrimi për dokumentim dhe auditim

SIU-ja mban dokumentacion të përditësuar, për:

a) masat e sigurisë të zbatuara;

b) procedurat e përpunimit të të dhënave;

c) *log*-et e auditimit;

d) evidencat e qasjes dhe veprimeve të personelit.

Komisioneri, në cilësinë e autoritetit mbikëqyrës, ka të drejtën të kontrollojë zbatimin e këtyre masave.

5. VLERËSIMI I PASOJAVE NË PRIVATËSI (DPIA)

5.1 DPIA-ja është një proces i detyrueshëm dhe thelbësor për SIU-në në rastet kur përpunimi i të dhënave të udhëtimit ose të dhënave të tjera të udhëtimit paraqet rrezik të lartë për të drejtat dhe liritë e individëve, në kuptim të ligjit nr. 124/2024 dhe GDPR (neni 35).

5.2 Monitorimi dhe përditësimi i DPIA-së

SIU-ja duhet të:

a) përditësojë DPIA-në çdo herë që ndryshon sistemi, teknologjia, procedura ose rritet volumi i të dhënave;

b) rishikojë DPIA-në të paktën një herë në vit;

c) dokumentojë çdo ndryshim dhe matje të re të rrezikut;

d) sigurojë që proceset e reja API/PNR të mos nisin pa një DPIA të përditësuar.

5.3 Evidencat dhe dokumentimi

SIU-ja mban:

a) DPIA-të e kryera;

b) raportet e analizës së rrezikut;

c) matricat e rrezikut;

d) masat e zbatuara;

e) rekomandimet e DPO-së;

f) komunikimet me Komisionerin;

g) evidencat e auditimeve lidhur me DPIA-në.

6. SANKSIONET

Çdo person që përdor të dhënat dhe informacionet e bazës së të dhënave të udhëtimit të aplikacionit alternativ dhe nuk i fshin të dhënat sapo të jetë përmbushur qëllimi i mbledhjes së tyre, ndëshkohet me masa administrative dhe disiplinore sipas akteve normative në fuqi.

7. DISPOZITA PËRFUNDIMTARE

1. Udhëzimi i përbashkët nr. 464, datë 10.12.2020, "Për transmetimin e të dhënave të pasagjerit te Njësia e Informacionit të Pasagjerit", shfuqizohet.

Ky udhëzim hyn në fuqi pas botimit në Fletoren Zyrtare.

MINISTËR I PUNËVE TË BRENDSHME
Besfort Lamallari

KOMISIONERI PËR TË DREJTËN E
INFORMIMIT DHE MBROJTJEN E
TË DHËNAVE PERSONALE
Besnik Dervishi