INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE
INSPECTORATUL DE POLIȚIE JUDEȚEAN ALBA

SERVICIUL CABINET
Operator de date cu caracter personal

Nesecret

Nr. 69948/3/14.05.2018

Ex. unic

EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE LA NIVELUL I.P.J. ALBA

I. Date generale de identificare:

1. *Denumirea operatorului :*
   - **INSPECTORATUL DE POLIȚIE JUDEȚEAN ALBA**

2. *Sediul* operatorului :
   - Alba Iulia, Str. Ion I.C. Bratianu nr. 1B, cod 510118, jud. Alba, tel. 0258-806161, fax: 0258-810683, e-mail: relatiipublice@ab.politiaromana.ro

3. *Persoana anume desemnată la nivelul unității cu responsabilități de coordonare a activităților din domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date:*

Numele și prenumele: Luminita RAC

Funcția/Profesia: comisar de poliție - ofițer specialist I – Compartimentul Schengen și Relații Internaționale, Responsabul protecția datelor cu caracter personal.

Coordonate de contact: Alba Iulia, Piața Ion I.C. Bratianu nr. 1B, cod 510118, jud. Alba, tel. 0258-806161/interior 20123, fax: 0258-810683, e-mail: relatiipublice@ab.politiaromana.ro

II. Scopulrile prelucrării datelor cu caracter personal la nivelul I.P.J. Alba

1. Prevenirea, depistarea, investigarea, verificarea, cercetarea, constatarea, combaterea, reprimarea și urmărirea penală a infracţiunilor sau al executării sancțiunilor penale;
2. Prevenirea, verificare, cercetare, constatare, combatere, sancționare săvârșire contravenții.
3. Protejarea împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și menținerea ordinii publice.
4. Verificarea autenticităţii datelor furnizate de persoana vizată sau în legătură cu persona vizată
5. Introducerea şi actualizarea datelor cu privire la persoanele verificate / cercetate penal pentru săvârşirea unor contraventii / infracţiuni ca Evidenta centralizata a tuturor evenimentelor produse pe raza de competenta si a actiunilor de interes operativ
6. Monitorizarea și securitatea persoanelor, spațiilor și/sau bunurilor private / publice
7. Gestionarea resurselor umane la niveul I.P.J. Alba
8. Gestionarea resurselor economico-financiare și administrative la nivelul I.P.J. Alba
9. Emitere de autorizații și licențe conform competențelor Poliției Române
10. Servicii de consiliere juridică și reprezentare în justiție conform competențelor Poliței Române
11. Prelucrare de imagini video: camere de supraveghere pentru acces în unităţi, body camera / camere video / radare / alte dispozitive de înregistrare video si audio – personalul care desfășoară activități rutiere, ordine publică și investigații, camere portabile, camere de anchetă pentru prevenirea, depistarea, investigarea, verificarea, cercetarea, constatarea, combaterea, reprimarea și urmărirea penală a infracţiunilor sau al executării sancțiunilor penale, precum și pentru prevenirea, verificare, cercetare, constatare, combatere, sancționare săvârșire contravenții.
12. Desfășurarea activităților psihologice la nivelul I.P.J. Alba

III. Descrierea caregoriilor de persoane vizate și a categoriilor de date cu catacter personal

1. Categorii de persoane vizate:

a. Persoane fizice care fac obiectul activităţilor poliţieneşti (legitimare, conducerea la sediul poliţiei, utilizarea forţei sau a mijloacelor din dotare, efectuarea controlului corporal, al bagajului sau al autovehiculului, oprirea vehiculelor, constatarea infracţiunilor sau contravenţiilor, punerea în executare a mandatelor emise de organele judiciare competente)
b. Studenți / Elevi
c. Minori

d. Vizitatori
e. Justițiabili
f. Angajați
g. Personal M.A.I.
h. Membrii familiei persoanei vizate
i. Reprezentanți ai persoanelor juridice
j. Reprezentanți ai instituțiilor publice și / sau private
k. Persoane care au comis fapte penale
l. Persoane sancționate contravențional
m. Persoane cercetate
n. Persoane verificate
o. Persoane în CRAP

2. Categorii de date cu caracter personal prelucrate la nivelul I.P.J. Alba:

a. Numele și prenumele
b. Numele și prenumele membrilor de familie
c. Sexul
d. Porecla/pseudonimul
e. Data și locul nașterii
f. Cetățenia
g. Semnătura
h. Datele din actele de stare civilă
i. Datele din permisiul de conducere / certificatul de înmatriculare
j. Numărul dosarului de pensie
k. Numărul asigurării sociale / asigurării de sănătate
l. Caracteristici fizice / antropometrice
m. Telefon / fax
n. Adresă domiciliu / reședință
o. E-mail
p. Profesie
q. Loc de muncă

r. Formare profesională – diplome – studii
s. Situație familială
t. Situație militară
u. Situație economică și financiară
v. Date privind bunurile deținute
w. Date bancare
x. Obișnuințe, preferințe, comportament
y. Imagine
z. Voce
aa. Date de geolocalizare / date de trafic

3. Categorii de date cu caracter personal special prelucrate la nivelul I.P.J. Alba:

a. CNP – codul numeric personal
b. Seria și numărul actului de identitate / pașaportului
c. Date privind starea de sănătate
d. Date genetice
e. Date biometrice
f. Date privind săvârșirea de infracțiuni
g. Date privind condamnări penale / măsuri de siguranță
h. Date privind sancțiuni disciplinare / administrative
i. Date privind sancțiuni contravenționale
j. Date privind cazierul judiciar

IV. Categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale

a. Persoana vizată
b. Reprezentanții legali ai persoanei vizate
c. Personal M.A.I.
d. Autorități publice sau locale de aplicare a legii
e. Servicii sociale și de sănătate
f. Instituții de învățământ și educație

g. Societăți bancare
h. Birouri de credit
i. Agenții de colectare a debitelor / recuperare a creanțelor
j. Societăți de asigurare și reasigurare
k. Organizații profesionale
l. Asociații și fundații
m. Mass-media
n. Angajatorul / potențialul angajator al persoanei vizate
o. destinatarii din țări terțe sau organizații internaționale: ***statele aparținând spațiului Schengen - SIS, INTEROPL, EUROPOL etc – strict prin IGPR – CCPI și / sau punctele de contact.***

V. ***Categoriile de activități de prelucraredesfășurate în numele operatorului, la nivelul IPJ Alba:***

a. Introducerea de noi date,
b. Ştergerea unor date existente în baza de date,
c. Actualizarea datelor stocate
d. Interogarea bazei de date pentru regăsirea anumitor informaţii, selectate după un criteriu ales.
e. Colectarea,
f. Înregistrarea,
g. Organizarea,
h. Stocarea,
i. Păstrarea,
j. Adaptarea ori modificarea,
k. Extragerea,
l. Consultarea,
m. Utilizarea,
n. Dezvăluirea către terți prin transmitere,
o. Diseminare,
p. Alăturarea ori combinarea,
q. Blocarea,
r. Distrugerea datelor cu caracter personal.

VI. <u>Dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizatiei internationale respective, și dacă este cazul, documentația care dovedește existența unor garanții adecvate</u>

<u>Nu este cazul.</u>

VII. <u>Acolo unde este posibil, termenele limită preconizate pentru ștergerea diferitelor categorii de date:</u>

a. Pentru evidențele letrice – conform nomenclatoarelor în vigoare
b. Pentru imaginile video – la 30 de zile
c. Pentru restul datelor: la incetarea scopului pentru care au fost prelucrate.

VIII. <u>Descrierea generală a măsurilor tehnice și organizatorice de securitate:</u>

a. Măsurile cuprinse în Planul anual de cerințe minime de securitate aprobat la nivelul I.P.J. Alba

Nr. crt.	OBIECTIV	ACTIUNE
1.	**Identificarea şi autentificarea utilizatorului**	***- identificarea utilizatorului prin introducerea unei parole*** – *Identificarea se poate face prin mai multe metode*, cum ar fi: • introducerea codului de identificare de la tastatură (un şir de caractere) • folosirea unei cartele cu cod de bare • folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice. *Fiecare utilizator are propriul său cod de identificare.* Niciodată mai mulţi utilizatori nu trebuie să aibă acelaşi cod de identificare. Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate şi distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate şi distruse se stabileşte de operator.

Nr. crt.	OBIECTIV	ACTIUNE
		- autentificarea utilizatorului prin introducerea unei parole. *Orice cont de utilizator este însoţit de o modalitate de autentificare*. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană etc. Parolele sunt şiruri de caractere. Cu cât şirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afişate în clar pe monitor. Parolele trebuie schimbate periodic în funcţie de politicile de securitate ale entităţii (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizaţi de operator. Operatorul trebuie să solicite realizarea unui sistem informaţional care să refuse automat accesul unui utilizator după 5 introduceri greşite ale parolei. Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare trebuie să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa opera-torului. Fiecare entitate va stabili o procedură proprie de administrare şi gestionare a conturilor de utilizator. Operatorii autorizează anumiţi utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare, dacă utilizatorul acestora şi-a dat demisia ori a fost concediat, şi-a încheiat contractul, a fost transferat la alt serviciu şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.) ***- întocmirea unei liste, aprobate de conducerea entităţii, care sa cuprinda persoanele care au acces la bazele de date cu caracter personal efectuate manual .*** ***- stabilirea de măsuri pentru revocarea codului de autentificare al unui utilizator.*** Trebuie să fie efectuată *obligatoriu* în cazul în care acesta este transferat la un alt serviciu şi nu condiţionat de noile sarcini de serviciu
2.	**Tipul de acces**	***- stabilirea tipurilor de acces*** *după funcţionalitate* cum ar fi: administrare, introducere, prelucrare, salvare etc.

Nr. crt.	OBIECTIV	ACTIUNE
		după acţiuni aplicate asupra datelor cu caracter personal cum ar fi: scriere, citire, ştergere ***- stabilirea procedurilor privind tipurile de acces.*** ***- stabilirea modalităţilor stricte prin care se vor distruge datele cu caracter personal.*** Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câţiva utilizatori.
3.	**Colectarea datelor**	***- desemnarea utilizatorilor autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional.*** ***- luarea de măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data şi ora modificării.*** ***- luarea măsuri pentru ca sistemul informaţional să menţină datele şterse sau modificate.***
4.	**Execuţia copiilor de siguranţă**	***- stabilirea intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal.*** ***- stabilirea programelor folosite pentru prelucrările automatizate.*** ***- numirea utilizatorilor care execută copiile de siguranţă.*** ***- stabilirea camerelor in care se stochează copiile de siguranţă, în fişete metalice cu sigiliu aplicat.*** ***- luarea de măsuri ca accesul la copiile de siguranţă să fie monitorizat.***

Nr. crt.	OBIECTIV	ACTIUNE
5.	**Computerele şi terminalele de acces**	***- luarea de măsuri, astfel încât computerele şi alte terminale de acces să fie instalate în încăperi cu acces restricţionat.*** Dacă nu pot fi asigurate aceste condiţii, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice. ***- luarea de măsuri, astfel încât dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat.*** Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate. ***- luarea de măsuri astfel încât terminalele de acces folosite în relaţia cu publicul, pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de public şi după o perioadă scurtă, stabilită de operator, în care nu se acţionează asupra lor, acestea trebuie ascunse.***
6.	**Fişierele de acces**	***- luarea de măsuri astfel încât orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fişier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator. Informaţiile înregistrate în fişierul de acces sau în registru vor fi:*** • codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale); • numele fişierului accesat (fişei); • numărul înregistrărilor efectuate;

Nr. crt.	OBIECTIV	ACTIUNE
		• tipul de acces; • codul operaţiei executate sau programul folosit; • data accesului (an, lună, zi); • timpul (ora, minutul, secunda). ***- luarea de măsuri, pentru prelucrările automate, astfel încât aceste informaţii vor fi stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator.*** ***- luarea de măsuri pentru ca orice încercare de acces neautorizat să fie, de asemenea, înregistrată.*** ***- luarea de măsuri pentru ca operatorul să păstreze, obligatoriu fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.*** ***- luarea de măsuri astfel încât fişierele de acces să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente.***
7.	**Sistemele de telecomunicaţii**	***- luarea de măsuri pentru efectuarea periodică a controlului autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.*** ***- luarea de măsuri pentru conceperea sistemului de telecomunicaţii astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde.*** Dacă sistemul de

Nr. crt.	OBIECTIV	ACTIUNE
		telecomunicaţii nu poate fi astfel securizat, *operatorul este obligat* să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal. Prin sistemele de telecomunicaţii se vor transmite numai datele cu caracter personal strict necesare.
8.	**Instruirea personalului**	- ***informarea utilizatorilor cu privire la prevederile legislației în vigoare privind prelucrarea datelor cu caracter personal, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii utilizatorului.*** Utilizatorii care au acces la date cu caracter personal vor fi instruiţi de către operator asupra confidenţialităţii acestora şi vor fi avertizaţi prin mesaje care vor apărea pe monitoare în timpul activităţii. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă. - ***prelucrarea***, ***ori de cate ori se impune,*** cu fiecare lucrător care are acces la baze / date cu caracter personal, a ***legislației în vigoare, (***ordine, dispozitii, adrese și proceduri), cu privire la protecția datelor cu caracter personal, în vederea prevenirii și evitării incidentelor pe aceasta linie. - ***semnarea,*** de către fiecare lucrător care are acces la date cu caracter personal, a ***Declarației anexate***, conform Instrucţiunilor MAI nr. 27/2010 privind măsurile de natură tehnică pentru protectia datelor cu caracter personal.
9.	**Folosirea computerelor**	- ***interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;*** - ***informarea utilizatorilor în privinţa pericolului privind viruşii informatici;*** - ***implementarea unor sisteme automate de devirusare şi de securitate a sistemelor***

Nr. crt.	OBIECTIV	ACTIUNE
		informatice; ***- dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afişate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.***
10.	**Imprimarea datelor**	***- luarea de măsuri astfel încât scoaterea la imprimantă a datelor cu caracter personal să se realizeze numai de utilizatori autorizaţi pentru această operaţiune de către operator.*** ***- aprobarea de proceduri interne specifice privind folosirea şi distrugerea acestor materiale.*** Fiecare entitate îşi va aproba propriul sistem de securitate, ţinând seama de aceste cerinţe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcţie de importanţa datelor cu caracter personal prelucrate, îşi va impune măsuri de securitate suplimentare, conform planului propriu.
11.	**Instrucțiuni MAI nr. 27/2010**	***Prelucrarea*** cu toți lucrătorii din subordine, pe bază de proces verbal și semnătură, a ***Instrucțiunilor M.A.I. nr. 27/2010***
12.	**Fișe de Post**	***Completarea fișelor postului*** cu atribuții pe linia prelucrării datelor cu caracter personal
13.	**Declarații**	Verificarea completării de către personalul din subordine a ***Declarației pe proprie răspundere*** privind confidențialitatea datelor cu caracter personal.
14.	**Registru**	***Înființarea unui registru de verificări***[1] (letric sau electronic) pentru fiecare stație de lucru în care vor fi consemnate următoarele (cap de tabel): - CNP-ul interogat, - Data interogării, - Grad, nume prenume persoana care solicită interogarea

[1] Acolo unde se impune – ori de cate ori nu se poate completa campul ”MOTIVUL VERIFICARII”

Nr. crt.	OBIECTIV	ACTIUNE
		- Unitatea din care face parte persoana care solicita interogarea - Unitatea prin intermediul căreia se solicita interogarea - Motivul efectuării interogării, - Observații ***Nu se va proceda la efectuarea interogării în bazele de date decât dacă au fost completate datele în registru SAU aplicație.***
15.	**Evidență useri**	Întocmirea unei ***liste cu toți lucrătorii din subordine*** cu specificarea bazelor de date la care aceștia au acces.
16.	**Informarea imediată a responsabilului cu privire la modificarile de personal**	***Informarea imediată a responsabilului pe protecția datelor***, cu privire una din situațiile menționate în art. 10 si 11 din I.M.A.I. 27/2010, pentru a fi luate măsurile care se impun: *ART. 10* *"Extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal se dispune de operator atunci când utilizatorul se află în una dintre următoarele situaţii:* *a) la modificarea raporturilor de muncă;* *b) la modificarea atribuţiilor privind prelucrarea datelor cu caracter personal, prevăzute în fişa postului.* *ART. 11* *(1) Dreptul de acces al utilizatorului la sistemul de evidenţă a datelor cu caracter personal se suspendă pe perioada în care acesta se află în una dintre următoarele situaţii:* *a) urmează un curs sau o specializare cu scoatere din program, pentru o perioadă mai mare de 3 luni;* *b) se află în concediu fără plată, concediu medical, concediu pentru creşterea sau îngrijirea copilului minor, pentru o perioadă mai mare de 3 luni;* *c) se află în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;* *d) pe perioada cercetării administrative, în situaţia în care faţă de utilizator se efectuează*

Nr. crt.	OBIECTIV	ACTIUNE
		cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispoziţiilor legale. *e) alte cazuri prevăzute de lege.* *(2) La propunerea responsabilului/structurii responsabile cu protecţia datelor cu caracter personal, conducătorul operatorului dispune revocarea contului unic de către administratorul aplicaţiei atunci când utilizatorul se află în una dintre următoarele situaţii:* *a) la încetarea raporturilor de muncă/de serviciu;* *b) a intervenit o modificare a raporturilor de muncă/de serviciu, iar noile atribuţii nu impun accesul la date cu caracter personal."*
17.	**Gestionare solicitari pe linia PDCP**	***Respectarea Dispoziției șefului inspectoratului nr. 1/03.01.2018*** privind gestionarea solicitărilor persoanei vizate, respectiv: "Toate categoriile de șefi (servicii, birouri, compartimente, poliții municipale și orășenești, secții de poliție rurală, posturi de poliție) vor remite (redirecționa) solicitările primite în baza legislației privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, spre competentă soluționare responsabilului nominalizat la nivelul Inspectoratului de Poliţie Judeţean Alba".

RESPONSABIL PROTECȚIA DATELOR CU CARACTER PERSONAL
Comisar de poliţie
RAC LUMINITA