REPUBLIKA E SHQIPËRISË
PROKURORIA E PËRGJITHSHME

URDHËR

Nr. 122, Datë 10.04. 2013

"PËR MIRATIMIN E RREGULLORES "PËR MBROJTJEN, PËRPUNIMIN, RUAJTJEN DHE SIGURINË E TË DHËNAVE PERSONALE NË PROKURORI"

Në mbështetje të nenit 8 pika 2 gërma "gj" i ligjit nr. 8737, datë 12.02.2001, "Për organizimin dhe funksionimin e Prokurorisë në Republikën e Shqipërisë", (të ndryshuar):

URDHËROJ:

1. Miratimin e rregullores "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në prokurori"
2. Për ndjekjen dhe zbatimin e këtij urdhri, ngarkohet Drejtoria e Inspektimit dhe Burimeve Njerëzore dhe Drejtoria e Teknologjisë së Informacionit në Prokurorinë e Përgjithshme.
3. Ky urdhër hyn në fuqi menjëherë.

PROKURORI I PËRGJITHSHËM

ADRIATIK LLALLA

PP.15
Urdhëri 122 dt 10.04.2018

REPUBLIKA E SHQIPËRISË
PROKURORIA E PËRGJITHSHME

R R E G U L L O R E

"PËR MBROJTJEN, PËRPUNIMIN, RUAJTJEN DHE SIGURINË E TË DHËNAVE PERSONALE NË PROKURORI"

HYRJE

Në mbështjetje të neneve 15 deri 58 të Kushtetutës së Republikës së Shqipërisë, Deklaratës Universale të të drejtave dhe lirive të njeriut, Konventës për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, Direktivat 2002/58/EC dhe 95/46/EC të Këshillit Evropian dhe Parlamentit Evropian, Konventës 108 të Këshillit të Europës "Për mbrojtjen e individëve nga Përpunimi Automatik i të Dhënave Personale" dhe protokollit të saj shtesë, Kodit të Procedurës Penale të Republikës së Shqipërisë, nenit 8 pika "gj" të ligjit nr. 8737, datë 12.02.2001 "Për organizimin dhe funksionimin e Prokurorisë në Republikën e Shqipërisë" (i ndryshuar), ligjit nr. 9887, datë 10.03.2008, "Për Mbrojtjen e të Dhënave Personale", (i ndryshuar), vendimet dhe udhëzimet e Komisionerit për Mbrojtjen e të Dhënave Personale, hartohet kjo rregullore për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në prokurori.

Kjo rregullore përbën një akt normativ të Prokurorit të Përgjithshëm, i detyrueshëm për të gjithë prokurorët, oficerët e Policisë Gjyqësore dhe punonjësit e administratës së Prokurorisë.

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

1. Objekti i kësaj rregulloreje është përcaktimi i procedurave organizative e teknike, masave për mbrojtjen e të dhënave personale dhe sigurisë, ruajtjes dhe administrimit të të dhënave personale nga organi i Prokurorisë.

Neni 2
Qëllimi

1. Kjo rregullore ka për qëllim të sigurojë që përpunimi i të dhënave personale të subjekteve, që kryhet nga prokuroria në kuadër të veprimtarisë së saj, të jetë në përputhje me parimet dhe standartet e vendosura në aktet kombëtare dhe ndërkombëtare në fuqi, në fushën e mbrojtjes së të dhënave personale.

Neni 3
Fusha e zbatimit

1. Kjo rregullore zbatohet për përpunimin plotësisht ose pjesërisht të të dhënave personale që mbahen në një sistem arkivimi apo që kanë për qëllim të formojnë pjesë të një sistemi arkivimi në organin e prokurorisë, i kryer nëpërmjet mjeteve automatike, manuale apo mjete të tjera, në përputhje me "Ligjin për mbrojtjen e të dhënave personale".
2. Kjo rregullore zbatohet përsa nuk bie në kundërshtim me Kodin e Procedurës Penale të Republikës së Shqipërisë.

Neni 4
Përkufizime

1. Për qëllim të kësaj Rregulloreje, termat e mëposhtëm kanë këtë kuptim:

a) "Kontrollues" për efekt të kësaj rregulloreje është Prokurori i Përgjithshëm ose personat e autorizuar prej tij, të cilët, përcaktojnë qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore në fuqi, dhe përgjigjen për përmbushjen e detyrimeve të përcaktuara në këtë ligj;
b) "Përpunues" për efekt të kësaj rregulloreje janë, prokurorët, oficerët e Policisë Gjyqësore dhe/ose punonjës të tjerë të prokurorisë të cilët nën drejtimin e prokurorit përgjegjës janë të ngarkuar me detyrën e përpunimit të të dhënave nga kontrolluesi dhe në emër të tij;
c) "Subjekt i të dhënave personale" për efekt të kësaj rregulloreje është, çdo person fizik të cilit i përpunohen të dhënat personale;
d) "Sistem arkivimi" është çdo grup i strukturuar i të dhënave personale, të cilat janë të aksesueshme në bazë të kritereve specifike, të centralizuara, të decentralizuara ose të shpërndara në një bazë, funksionale ose gjeografike;
e) "Përpunim i të dhënave personale" është çdo veprim ose grup veprimesh, të cilat janë kryer mbi të dhënat personale, me mjete automatike ose jo, të tilla si mbledhja, regjistrimi, organizimi, ruajtja, përshtatja ose ndryshimi, rikthimi, konsultimi, shfrytëzimi, transmetimi, shpërndarja/ vënia në dispozicion, shtrirja ose kombinimi, fotografimi, pasqyrimi, hedhja, plotësimi, seleksionimi, bllokimi, asgjësimi ose shkatërrimi, edhe në qoftë se nuk janë të regjistruara në një bankë të dhënash.
f) "Marrës" është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër të cilit i janë dhënë të dhënat e një palë të tretë. Autoritetet, të cilat mund të marrin të dhëna në kuadrin e një hetimi të veçantë, nuk konsiderohen si marrës;
g) "Transferim ndërkombëtar" është dhënia e të dhënave personale marrësve në shtetet e huaja;
h) "Incident në të dhënat personale" do të thotë një shkelje e sigurisë që çon në shkatërrimin aksidental apo të paligjshëm, humbje, ndryshim, zbulim i paautorizuar, apo qasje në të dhënat personale të transmetuara, të ruajtura ose të përpunuara.

2. Termat e tjerë të përdorur në këtë rregullore do të kenë të njëjtin kuptim si në ligjin nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale", (i ndryshuar).

KREU II
PARIMET DHE KRITERET E PËRPUNIMIT TË TË DHËNAVE PERSONALE

Neni 5
Mbrojtja e të dhënave personale

1. Përpunuesi, që ka për detyrë përpunimin e të dhënave personale të subjekteve, është i detyruar:
   a) Të respektojë parimin e përpunimit të drejtë dhe të ligjshëm të të dhënave personale, duke garantuar mbrojtjen e të drejtave dhe lirive themelore të njeriut dhe, në veçanti, të drejtën e ruajtjes së jetës private;
   b) Të garantojë se të dhënat personale janë mbledhur vetëm për qëllim të veprimtarive të parandalimit, hetimit të veprave penale dhe ndjekjes së autorëve të tyre, dhe do të përpunohen në përputhje me veprimtarinë e saj;
   c) Të respektojë parimin e propocionalitetit, në mënyrë që të dhënat që do të përpunohen të jenë në atë masë sa nevojitet për të përmbushur qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;
   d) Të garantojë saktësinë e të dhënave dhe t'i përditësojë për të siguruar që të dhënat e pasakta e të parregullta të fshihen apo të ndryshohen;

e) Të sigurojë që të dhënat duhet të mbahen në atë formë, që të lejojnë identifikimin e subjekteve të të dhënave për aq kohë, sa është e nevojshme për qëllimin për të cilin ato janë grumbulluar ose përpunuar dhe jo më tepër.

Neni 6
Kriteret e përpunimit të të dhënave personale dhe të dhënave sensitive

1. Përpunuesi, që ka për detyrë përpunimin e të dhënave personale të subjekteve, në kuadër të veprimtarisë së prokurorisë, kryen përpunimin e çdo informacioni në lidhje me një person fizik, të identifikuar ose të identifikueshëm, drejtëpërdrejt ose tërthorazi, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social, duke respektuar parimet e vendosura në nenin 5 të kësaj rregulloreje.
2. Përpunuesi kryen përpunimin e të dhënave sensitive, që zbulojnë origjinën racore ose etnike, mendimet politike, anëtarësinë në sindikata, besimin fetar apo filozofik, dënimet penale, si dhe shëndetin dhe jetën seksuale, vetëm në rastet e mëposhtme:
   a) Subjekti i të dhënave ka dhënë pëlqimin, që mund të revokohet në çdo çast dhe e bën të paligjshëm përpunimin e mëtejshëm të të dhënave;
   b) Është në interesin jetik të subjektit të të dhënave ose të një personi tjetër dhe subjekti i të dhënave është fizikisht ose mendërisht i paaftë për të dhënë pëlqimin e vet;
   c) Autorizohet nga kontrolluesi për një interes të rëndësishëm publik, nën masa të përshtatshme mbrojtëse;
   ç) Lidhet me të dhëna, që janë bërë haptazi publike nga subjekti i të dhënave ose është i nevojshëm për ushtrimin apo mbrojtjen e një të drejte ligjore;
   d) Të dhënat përpunohen për qëllime historike, shkencore ose statistikore, nën masa të përshtatshme mbrojtëse.
3. Përpunimi i të dhënave sensitive lejohet kur është i nevojshëm për përmbushjen e detyrimit ligjor dhe të drejtave specifike të kontrolluesit në fushën e punësimit.

Neni 7
Transferimi ndërkombëtar i të dhënave

1. Transferimi ndërkombëtar i të dhënave personale kryhet, me marrës, nga shtete me një nivel të mjaftueshëm të mbrojtjes së të dhënave personale. Shtetet, që kanë nivel të mjaftueshëm të mbrojtjes së të dhënave, përcaktohen në vendimin e Këshillit të Ministrave nr. 934 datë 02.09.2009 "Për përcaktimin e shteteve, me nivel të mjaftueshëm të mbrojtjes së të dhënave personale" dhe vendimit nr. 3 datë 20.11.2012 të Komisionerit për Mbrojtjen e të Dhënave Personale.
2. Transferimi ndërkombëtar i të dhënave personale me një shtet, që nuk gëzon statusin e shtetit që ofron nivel të mjaftueshëm të mbrojtjes, mund të bëhet nëse:
   a) Autorizohet nga akte ndërkombëtare, të ratifikuara nga Republika e Shqipërisë dhe që janë të zbatueshme në mënyrë të drejtpërdrejtë;
   b) Subjekti i të dhënave ka dhënë pëlqimin për transferimin ndërkombëtar të tyre;
   c) Është i nevojshëm për mbrojtjen e interesave jetësorë të subjektit të të dhënave;
   d) Është i nevojshëm apo përbën një kërkesë ligjore për një interes të rëndësishëm publik ose për ushtrimin dhe mbrojtjen e një të drejte ligjore;
   e) Është bërë nga një regjistër, i cili është i hapur për këshillime dhe siguron informacion për publikun në përgjithësi.
3. Në raste të tjera të domosdoshmërisë së transferimit ndërkombëtar të të dhënave personale me një shtet, që nuk ka nivel të mjaftueshëm të mbrojtjes së të dhënave, kur nuk janë

kushtet e parashikuara në pikën 2 të këtij neni, Kontrolluesi, përpara transferimit të të dhënave, bën kërkesë për autorizim te Komisioneri për Mbrojtjen e të Dhënave Personale, duke garantuar respektimin e interesave për ruajtjen e sekretit të subjektit të të dhënave jashtë Republikës së Shqipërisë.

4. Transferimi ndërkombëtar i të dhënave personale te institucionet ndërkombëtare, bëhet duke zbatuar përsa është e mundur parashikimet e pikës 2 të këtij neni.

KREU III
TË DREJTAT E SUBJEKTIT TË TË DHËNAVE

Neni 8
Zbatimi i të drejtave të subjekteve të të dhënave personale

1. Kontrolluesi i garanton subjektit të cilit i janë përpunuar të dhënat, këto të drejta:
   a) Të drejtën për akses, që përfshin, njohjen e subjektit me qëllimin e mbledhjes së të dhënave, kategorinë e të dhënave që janë mbledhur dhe/ose do të mblidhen, kategorinë e subjekteve që do t'i zbulohen këto të dhëna;
   b) Të drejtën për të kërkuar korrigjimin ose fshirjen;
2. Çdo person, të dhënat e të cilit janë përpunuar ose po përpunohen nga organi i prokurorisë, ka të drejtë që të njihet me to, duke ju drejtuar, kontrolluesit vet ose nëpërmjet përfaqësuesit ligjor. Kërkesa bëhet me shkrim dhe duhet të përmbajë të dhëna të mjaftueshme për të vërtetuar identitetin e kërkuesit. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit.
3. E drejta për akses kufizohet në rastet kur njohja me këto të dhëna pengon ose paragjykon hetimin dhe ndjekjen penale, cënon informacionin që përbën sekret hetimor, informacionin që përbën "sekret shtetëror", sigurinë ose rendin publik, parandalimin e krimit, dhe mbrojtjen e të drejtave dhe lirive të të tjerëve.
4. Në rastet kur subjekti i të dhënave ka kundërshtuar të dhënat e tij personale, prokurori kufizon përdorimin e tyre deri në verifikimin e pretendimeve të subjektit. Të dhënat personale do të korrigjohen ose fshihen në rastet kur është e mundur, në të kundërt, dokumentit që pasqyron të dhënat personale të gabuara, duhet t'i bashkëlidhet një deklaratë korrigjuese e të dhënave.

KREU IV
SIGURIA E TË DHËNAVE PERSONALE

Neni 9
Masat për sigurinë e të dhënave

1. Prokuroritë marrin masa organizative dhe teknike të përshtatshme për të mbrojtur të dhënat personale nga shkatërrime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, si dhe nga çdo formë e paligjshme përpunimi.
2. Në mënyrë të veçantë marrin këto masa sigurie:
   a) Përcaktojnë funksionet e çdo zyre dhe operatori përgjegjës për përdorimin e të dhënave;

b) Futja, kopjimi, leximi, modifikimi, heqja fshirja e të dhënave personale bëhet nga përpunuesi dhe punonjësi i mirëmbajtjes së sistemit apo pajisjeve të telekomunikacionit në prani të përpunuesit;
c) Regjistrojnë dhe dokumentojnë modifikimet, korrigjimet, fshirjet, transmetimet, përditësimet, etj.
d) Aksesi në të dhënat dhe programet, bëhet vetëm nga përpunuesi dhe punonjësi i mirëmbajtjes së sistemit apo pajisjeve të telekomunikacionit në prani të përpunuesit, dhe merren masa për të identifikuar çdo hyrje në mjetet e arkivimit;
e) Udhëzojnë operatorët, pa përjashtim, për detyrimet që kanë, në përputhje me ligjin për mbrojtjen e të dhënave personale dhe rregulloret e brendshme për mbrojtjen e të dhënave, përfshirë edhe rregulloret për sigurinë e të dhënave;
f) Ndalojnë hyrjen e personave të paautorizuar në mjediset e kontrolluesit ose përpunuesit të të dhënave;
g) Vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetëm me autorizim të kontrolluesit, dhe çdo mjet sigurohet me masa parandaluese ndaj vënies së paautorizuar në punë;
h) Sigurojnë që kur largohen nga vendi i tyre i punës, punonjësit të mbyllin kompjuterat e tyre, dollapët, kasafortat dhe zyrën, në të cilat janë ruajtur të dhënat personale;
i) Sigurojnë që të mos largohen nga mjediset e punës kur ka të dhëna të pambrojtura në tavolinë, dhe janë të pranishëm persona të paautorizuar;
j) Nuk mbajnë në monitor të dhëna personale, kur është i pranishëm një person i pautorizuar;
k) Nuk lejojnë persona të paautorizuar të ndërhyrjnë në pajisjet elektronike/komputerike të institucionit;
l) Nuk nxjerrin jashtë zyrës, në asnjë rast, kompjutera, laptop, flesh apo pajisje të tjera që përmbajnë të dhëna personale dhe nuk duhet ti lënë ato në vende të pasigurta, pa u siguruar për fshirjen apo shkatërrimin e të dhënave;
m) Udhëzimet për përdorimin e kompjuterit, duhet të ruhen në mënyrë të tillë që ato të mos jenë të aksesueshme nga persona të pa autorizuar;
n) Kryejnë vazhdimisht procedurën e hyrjes dhe daljes duke përdorur fjalëkalime personale në fillim dhe në mbarim të aksesit të tyre në të dhënat e mbrojtura, të ruajtura në bazat e të dhënave të prokurorisë;
o) Në dokumente që përmbajnë të dhëna të mbrojtura, duhet të sigurojnë shkatërrimin e materialeve ndihmëse, (p.sh. shkresa, skica) të përdorura ose të prodhuara për krijimin e dokumentit, kur kjo është e mundur;
p) Të dhënat e dokumentuara nuk përdoren për qëllime të tjera, që nuk janë në përputhje me qëllimin e grumbullimit;
q) Ruajnë dokumentacionin e të dhënave për aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar dhe në përputhje me legjislacionin në fuqi;
r) Niveli i sigurisë duhet të jetë i përshtatshëm me natyrën e përpunimit të të dhënave personale;
s) Të respektojnë aktet ligjore dhe nënligjore që përcaktojnë mënyrën e përdorimit të të dhënave personale, e në veçanti rregullat e përcaktuara në Udhëzimin nr.24 datë 27.12.2012 "Për detyrimet e kontrolluesve përpara se të përpunojnë të dhënat personale" dhe udhëzimin nr. 21, datë 24/09/ 2012 "Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga kontrolluesit e mëdhenj"(i ndryshuar), të Komisionerit për Mbrojtjen e të Dhënave Personale.[1]

[1] Aktet nënligjore të Komisionerit për Mbrojtjen e të Dhënave Personale gjenden të publikuara në faqen e internetit: http://ëëë.kmdp.al/

Neni 10
Menaxhimi i incidenteve në të dhënat personale

1. Përpunuesi/punonjësi i prokurorisë është i detyruar që në rast se ndodhet para një incidenti të kryer nga vet ai ose të zbuluar prej tij, të njoftojë menjëherë eprorin e tij dhe të mbaj procesverbal ku evidenton datën dhe orën kur ka ndodhur apo është zbuluar incidenti, llojin e incidentit, efektet e incidentit, personin që ka marrë njoftim për të si dhe çdo rrethanë tjetër që e vlerëson të dobishme.
2. Në rast se është i nevojshëm rikuperimi i të dhënave, kontrolluesi urdhëron personat kompetent për kryerjen e veprimeve për rikuperimin e të dhënave personale.

Neni 11
Mbrojtja e ambjenteve

1. Ambientet në të cilat do të përpunohen të dhënat personale duhet të mbrohen nga masa organizative, fizike dhe teknike që të parandalojnë aksesin e personave të paautorizuar në mjediset dhe aparaturat me të cilat do të përpunohen të dhënat personale.
2. Zbatimi i masave të sigurimit duhet të bëhet në përputhje me nivelin e sigurisë së të dhënave dhe informacionit të administruar, si dhe treguesit e nivelit të rrezikut që mund të vijë nga ekspozimi i paautorizuar i informacionit të ruajtur.
3. Në ambientet ku përpunohen të dhëna personale zbatohen këto masa sigurie:
   a) Ndalohet hyrja e personave të paautorizuar;
   b) Personat që futen në këto ambjete duhet të pajisen me autorizimin përkatës nga kontrolluesi;
   c) Ambientet e hyrjes, survejohen me kamera gjatë 24 orëve;
   d) Veç masave dhe sistemeve të tjera të mbrojtjes, vendosen pajisje dhe sisteme të sigurimit elektronik (sisteme sinjalizimi, telekamera, etj);
   e) Ambientet pajisen me dollap hekuri, të sigurta për mbrojtjen e dosjeve nga dëmtimi i tyre, me kasaforta e brava automatike me çelësa dhe drynë të veçantë nga ata të përdorimit të zakonshëm dhe vulosen me dyllë ose plastelinë;
   f) Dyert duhet të jenë të blinduara dhe dritaret të përforcohen me shufra hekuri;
   g) Sigurohet mbikëqyrje e vazhdueshme, ditën dhe natën me roje fizike.

Neni 12
Hyrja e autorizuar

1. Në ambjentet ku përpunohen të dhëna të mbrojtura (personale) lejohet të qëndrojnë:
   a) Punonjësit e Prokurorisë, vetëm nëse ata janë të punësuar në këtë ambient ose nëse prania e tyre është thelbësore për kryerjen e detyrave të punës;
   b) Personeli i mirëmbajtjes së sistemit apo pajisjeve të telekomunikacionit lejohet të futen në këto ambiente i shoqëruar nga personi i caktuar nga kontrolluesi vetëm kur kërkohet nga titullari i drejtorisë/njësisë.

Neni 13
Detyrat e Drejtorisë së Teknologjisë

1. Drejtoria e Teknologjisë së Informacionit duhet të ketë një backup të të gjitha të dhënave dhe softëare-ve që mbahen ose ruhen në serverin qëndror. Backup-i duhet të mbahet në një vend të sigurt jashtë godinës në të cilën gjendet serveri qendror. Drejtoria e Teknologjisë së Informacionit mban një backup të të dhënave dhe të sistemit të vendosur në kompjuterin dytësor.

Neni 14
Mbrojtja e pajisjeve elektronike

1. Pajisjet elektronike për përpunimin e të dhënave dhe informacioneve në organin e prokurorisë përdoren vetëm për kryerjen e detyrave të përcaktuara. Këto pajisje përdoren vetëm nga punonjës të prokurorisë të trajnuar më parë për përdorimin e tyre.
2. Trajnimi i personelit që merret me përpunimin e të dhënave bëhet nga Drejtoria e Teknologjisë së Informacionit.
3. Për çdo gabim apo defekt në sistemet/databaset e prokurorisë njoftohet administratori i sistemit, i cili mbi bazën e kërkesës bën rregullimin përkatës.

Neni 15
Mbrojtja e softëare

1. Programet për trajtimin e të dhënave dhe informacioneve të blera apo të dhuruara nga donatorë të ndryshëm menaxhohen nga Drejtoria e Teknologjisë së Informacionit.
2. Kur një program i destinuar për trajtimin e të dhënave të prokurorisë është krijuar me iniciativën e një punonjësi të prokurorisë i cili nuk është i përfshirë në zhvillimin e organizimit dhe të planifikimit të programeve, para se të përdoret, programi duhet të jetë miratuar me akt të shkruar nga Drejtoria e Teknologjisë së Informacionit. Pas miratimit Drejtoria e Teknologjisë së Informacionit organizon instalimin e tij në pajisjet elektronike.
3. Për secilin program Drejtoria e Teknologjisë së Informacionit mund të përcaktojë:
   a) Kush mund ta fshijë, kopjojë ose ta ndryshojë atë;
   b) Ku duhet të ruhet kopja e programit dhe cili është përgjegjës për mbajtjen e tij të përditësuar.

Neni 16
Blerja e programeve

1. Çdo program që do të blihet nga Prokuroria e Përgjithshme duhet të pajiset me liçencë për instalimin e tij në prokuroritë e rretheve gjyqësore.

Neni 17
Fjalëkalimet

1. Shumë nga aplikimet dhe sistemet kompjuterike janë të mbrojtura me fjalëkalime. Për arsye sigurie, këto fjalëkalime duhet të ndryshohen çdo 6 muaj.
2. Fjalëkalimet, të mbyllura në zarf dorëzohen për ruajtje në zyrën e protokollit të institucionit.

Neni 18
Monitorimi dhe regjistrimi i aksesit për të dhënat personale

1. Hyrja tek të dhënat dhe informacionet u nënshtrohet normave të veçanta të sigurisë për ruajtjen e paprekshmërisë dhe përditësimin e tyre. Sistemi duhet të ndërtohet në mënyrë të tillë që të vërtetojë identitetin e përdoruesit. Kjo kërkon që serveri qëndror të njohë çdo operator terminalist dhe çdo përdorues nëpërmjet programeve të veçanta. Ky sistem mundëson identifikimin e vazhdueshëm të përdoruesit në çdo kohë, në një terminal të caktuar, vendin e punës ose pajisje të tjera për periudhën për të cilën të dhënat specifike janë ruajtur.
2. Përdoruesit duhet të njihen me llojin e të dhënave në regjistrimet e përditshme dhe kohën e

ruajtjes së këtyre regjistrimeve.

3. Regjistrimet e përditëshme administrohen nga zyra përgjegjëse për mbrojtjen e të dhënave, që përcakton përmbajtjen e të dhënave të regjistrimeve ditore dhe kohën e ruajtjes së të dhënave personale.
4. Njohja dhe regjistrimi i operatorëve terminalistë dhe i përdoruesve kryhet me përdorimin e fjalëkalimeve për hyrjen në bankën e të dhënave. Fjalëkalimet cilësohen sekrete dhe janë vetjake.
5. Hyrja në të dhënat dhe informacionet lejohet ose pengohet me programe të veçanta elektronike. Kontrolli dhe dokumentimi i aksesit në të dhëna dhe informacione realizohet nga personat përgjegjës për mbrojtjen e të dhënave.

KREU V
DISPOZITA TË FUNDIT

Neni 19
Konfidencialiteti

1. Çdo punonjës i prokurorisë që përpunon të dhëna apo vihet në dijeni me të dhënat e përpunuara nuk mund t'i bëjë të njohur përmbajtjen e këtyre të dhënave personave të tjerë. Ai detyrohet të ruajë konfidencialitetin dhe besueshmërinë edhe pas përfundimit të funksionit.
2. Çdo person që vepron nën autoritetin e kontrolluesit, nuk duhet t'i përpunojë të dhënat personale, tek të cilat ka akses, pa autorizimin e kontrolluesit, përveçse kur detyrohet me ligj.
3. Punonjësi i prokurorisë që në ushtrim të detyrave të tij merr dijeni mbi informacione konfidenciale, nënshkruan marrëveshjen tip sipas **Aneksit 1** bashkëlidhur kësaj rregulloreje, që i bashkëlidhet kontratës së tij të punës ose aktit të emërimit.
4. Pas përfundimit të kontratës së punës apo transferimit të një punonjësi, burimet njerëzore duhet të njoftojnë strukturat përkatëse të teknologjisë së informacionit për marrjen e masave teknike mbrojtëse.

Neni 20
Lëshimi i kopjeve, ekstrakteve dhe vërtetimeve

1. Punonjësi i prokurorisë, në përputhje me dispozitat e Kodit të Procedures Penale, i lëshon kopje, ekstrakte ose vërtetime të akteve të veçanta që përmbajnë të dhëna personale, vetëm subjektit të të dhënave personale ose personit të autorizuar prej tij. Në çdo rast tjetër kur kërkuesi vërteton një interes të ligjshëm për t'u pajisuar me kopje, ekstrakte ose vërtetime të akteve të veçanta që përmbajnë të dhëna personale të një personi tjetër, punonjësi duhet të bëj të padallueshme në mënyrë mekanike, të dhënat personale në dokumentin që do t'i jepet kërkuesit.
2. Vërtetimet e prokurorisë për ndjekje penale, i lëshohen vetëm subjektit për të cilin jepet vërtetimi ose personit të autorizuar prej tij.

Neni 21
Administrimi i Dokumenteve "Sekret Shtetëror"

1. Aktet, dokumentacioni dhe çdo informacion që përmbajnë të dhëna personale dhe klasifikohen "sekret shtetëror" administrohen sipas ligjit nr. 8457, datë 11.02.1999 "Për informacionin e klasifikuar "Sekret Shtetëror", të ndryshuar, akteve nënligjore të dala në zbatim të tij dhe Vendimit të Këshillit të Ministrave nr. 312 datë 16.03.2011, "Për miratimin e rregullores për punën me informacionin e klasifikuar "Sekret Shtetëror".

Neni 22
Arkivimi

1. Dokumentet manuale, që përmbajnë të dhëna personale që sipas akteve ligjore e nënligjore në fuqi duhet të ruhen, arkivohen sipas kritereve të përcaktuar në rregulloren "Për normat tekniko-profesionale metodologjike të shërbimit arkivor në Republikën e Shqipërisë", dalë në zbatim të ligjit nr. 9154, datë 6.11.2003 "Për arkivat".

Neni 23
Mbajtja e të dhënave personale në sistemet elektronike

1. Të dhënat personale që mbahen në sistemet elektronike, në rast se nuk ka një detyrim ligjor për ruajtjen e tyre, duhet të fshihen, ose të bëhen anonime, në momentin që ato nuk janë më të nevojshme për qëllimin për të cilin janë mbledhur në mënyrë të ligjshme nga ana e prokurorisë.
2. Kontrolluesi çdo tre vjet, vendos për domosdoshmërinë e mbajtjes së të dhënave personale ose fshirjen e tyre, pas vlerësimit të kryer nga përgjegjësit e zyrave që administrojnë këto të dhëna.
3. Kjo vendimarrje duhet të dokumentohet në sistem dhe të përfshijë arsyet për marrjen e një vendimi të tillë.

Neni 24
Detyrimi për bashkëpunim

1. Prokuroria do të bashkëpunojë me Komisionerin për Mbrojtjen e të Dhënave Personale, për zbatimin e kësaj rregulloreje dhe akteve ligjore e nënligjore në fuqi në fushën e mbrojtjes së të dhënave personale, si dhe për t'i siguruar atij të gjithë informacionin që kërkon për përmbushjen e detyrave të tij funksionale.

Neni 25
Mbikëqyrja e masave dhe procedurave mbrojtëse

1. Mbikëqyrja e implementimit të rregullave për mbrojtjen e të dhënave personale për respektimin e normave të sigurisë, për mbrojtjen e të dhënave të automatizuara kundër prishjes së tyre aksidentale ose të paautorizuar, si dhe kundër hyrjes, ndryshimit dhe përhapjes së paautorizuar të tyre realizohet nga drejtuesi i prokurorisë dhe punonjësi i Drejtorisë së Teknologjisë së Informacionit.

Neni 26
Masat ndëshkuese

1. Shkelja e detyrimeve të përcaktuar në këtë rregullore për mbrojtjen e të dhënave personale kur nuk përbën vepër penale ose kundravajtje administrative në përputhje me ligjet në fuqi, përbën shkak për fillimin e procedimit disiplinor ndaj punonjësit të prokurorisë.

Neni 27
Kontrolli i rregullores

1. Çdo dy vjet nga hyrja në fuqi e kësaj rregulloreje, një prokuror që ushtron funksionet pranë Prokurorisë së Përgjithshme dhe një përfaqësues nga Drejtoria e Teknologjisë së Informacionit në Prokurorinë e Përgjithshme, ushtrojnë kontroll në të gjithë sistemin e prokurorisë për zbatimin e detyrimeve të kësaj rregulloreje.
2. Prokurori i Përgjithshëm dhe Komisioneri për Mbrojtjen e të Dhënave Personale, pasi njihen me përfundimet dhe rekomandimet e grupit të kontrollit, japin udhëzimet e nevojshme për përpunuesit.

Neni 28
Hyrja në fuqi

1. Kjo rregullore hyn në fuqi menjëherë.

PROKURORI I PËRGJITHSHËM

ADRIATIK LLALLA

ANEKS 1

DEKLARATË KONFIDENCIALITETI

Une _____si punonjës i Prokurorisë të _____, kam dijeni të plotë që për shkak të detyrës do të kem akses në informacione/arkiva të cilat janë të konsideruara si konfidenciale.

Unë pranoj me përgjegjësinë time të plotë të respektoj konfidencialitetin në lidhje me informacionet/arkivat në të cilat kam akses, si dhe të ndjek procedurat e punës në mënyrë të tillë që të mbroj privatësinë dhe të veproj në mënyrë profesionale, në përputhje me rregulloren "Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në prokurori" dhe "Marrëveshjen e Konfidencialitetit dhe Politikën e Sigurisë".

Marr përgjegjësinë e plotë që në qoftë se konstatohet qe kam vepruar në kundërshtim me udhëzimet në lidhje me informacionet konfidenciale apo në rast të mosruajtjes së privatësisë, ndaj meje të merren masa të menjëhershme. Unë e kuptoj këtë veprim si një nevojë për të mbajtur standarte të larta profesionale në zyrë dhe në Prokurorinë e _____.

_____ **Nënshkrimi i të punësuarit**

_____ **Nënshkrimi i eprorit**

Data __/___/_____

Marrëveshja e Konfidencialitetit dhe Politika e Sigurisë

Prokuroria e _____ kërkon që siguria dhe konfidencialiteti i të dhënave dhe informacionit të kenë rëndësi maksimale. Qëllimi i kësaj politike është të sigurojë që informacioni konfidencial, i çfarëdolloj formati qoftë, të mos dalë nga prokuroria pa aprovimin e qartë të Drejtuesit të Prokurorisë. Për këto arsye, u kërkon të gjithë përdoruesve të të dhënave dhe informacioneve, të ndjekin procedurën e mëposhtme:

Politikë për Konfidencialitetin e të Dhënave

Çdo garantim aksesi individual në të dhëna dhe informacione në dosjet fizike përbën një pozicion besueshmërie dhe duhet të garantojë siguri dhe konfidencialitet për informacionin që ai/ajo përdor. Përdoruesve të të dhënave dhe informacioneve të Prokurorisë, u kërkohet të veprojnë në përputhje me legjislacionin Shqiptar dhe politikat e Institucionit. Të gjithë përdoruesit e të dhënave dhe informacionit duhet të lexojnë dhe kuptojnë se si zbatohen rregulloret dhe politikat në funksionet e tyre të punës. Të gjithë përdoruesit të cilët kanë akses në sistemet informatike apo arkivat fizike, duhet të pranojnë të lexojnë dhe të respektojnë politikat dhe udhëzimet e Prokurorisë.

Çdo individi me akses të autorizuar në sistemet informatike, regjistra apo dosje, i është dhënë akses të përdorë të dhënat apo dosjet e Prokurorisë, vetëm në funksion të punës së saj dhe nuk duhet t`a përhapë këtë informacion jashtë saj me përjashtim të rasteve të aprovuara nga titullari. Individi duhet:

- Të aksesojë të dhëna për të realizuar përgjegjësitë e punës përkatëse (tij/saj);
- Të mos kërkojë favore personale apo të lejojnë të tjerët të përfitojnë personalisht nga çdo e dhënë që ka mbërritur tek ata nëpërmjet detyrave të punës;
- Të mos kryejë apo lejojë përdorim të paautorizuar të çdo informacioni në sistemet e informacionit apo arkivat e Prokurorisë;
- Të mos shtojë, ndryshojë apo fshijë të dhëna në sistemet e informacionit apo arkiva jashtë qëllimit të përgjegjësive të punës së tyre;
- Të mos përfshijë apo mundësojë të përfshijë në ndonjë regjistrim apo raport një të dhënë false apo të papërshtatshme;
- Të mos alternojë apo fshijë (apo mundësojë të tjerëve), raporte apo informacione të sistemit;
- Të mos përhapë të dhëna të Prokurorisë përveç sa kërkohet për të përmbushur përgjegjësitë e punës;

Është përgjegjësi individuale raportimi i menjëhershëm tek eprori direkt për çdo dhunim të kësaj politike apo ndonjë veprim tjetër i cili dhunon Konfidencialitetin e të dhënave.

Masa sigurie dhe procedura

Të gjithë përdoruesit e sistemeve të informacionit të Prokurorisë janë të pajisur me një llogari dhe fjalëkalim personal për të aksesuar të dhënat personale me qëllim realizimin e përgjegjësive të detyrave të punës. Përdoruesve të sistemeve të informacionit të Prokurorisë u kërkohet të ndjekin procedurat e mëposhtme:

i. Të gjitha veprimtaritë, të realizuara nga llogaria dhe fjalëkalimi e një përdoruesi, janë përgjegjësi e personit të cilit i përket llogaria dhe fjalëkalimi. Llogaria dhe fjalëkalimi duhet të mbeten konfidenciale dhe nuk duhen shpërndarë tek të tjerë persona;

ii. Përdorimi i fjalëkalimit të dikujt tjetër është dhunim i kësaj politike, pavarësisht nga mënyra se si është siguruar;

iii. Fjalëkalimi juaj siguron akses në informacione të cilat janë garantuar specifikisht për ju. Bëni kujdes të mos e shkruani në letër apo t'ia jepni dikujt tjetër;

iv. Është përgjegjësia juaj ndryshimi i menjëhershëm i fjalëkalimit nëse vini re se dikush tjetër e ka marrë atë;

v. Është e ndaluar të shohësh apo aksesosh informacione shtesë (në çfarëdolloj formati) nëse nuk jeni të autorizuar t`a bëni një veprim të tillë. Çdo akses i realizuar pa autorizim konsiderohet si "akses i paautorizuar";

vi. Për të parandaluar përdorimin e paautorizuar, përdoruesi duhet të mbyllë të gjitha aplikacionet të cilat janë sensitive nga natyra. Një alternativë është vendosja e fjalëkalimit të kompjuterit të punës.

vii. Fjalëkalimet duhet të ndryshohen periodikisht dhe/ose nëse ka ndonjë arsye për të besuar se ato janë kompromentuar apo zbuluar pa dashje;

viii. Pas përfundimit të kontratës apo transferimit të një punonjësi, burimet njerëzore duhet të njoftojnë strukturat përkatëse të teknologjisë së informacionit për marrjen e masave teknike përkatëse;

Unë e kuptoj që jam përgjegjës për çdo ndryshim të bërë duke përdorur llogarinë dhe fjalëkalimin tim ID. Pranoj se nuk do t`a përhap llogarinë dhe fjalëkalimin tim me asnjë individ tjetër dhe do të njoftoj menjëherë sektorin e burimeve njerëzore nëse besoj se fjalëkalimi im është kompromentuar.

Unë e kuptoj që aksesi im në të dhënat dhe sistemet e informacionit të Prokurorisë ka vetëm qëllimin e përmbushjes së detyrave dhe përgjegjësive të mia dhe se informcioni konfidencial nuk do të transmetohet jashtë Prokurorië. Thyerja e konfidencialitetit, duke përfshirë ndihmën ose bashkëpunimin me persona të tjerë për të dhunuar ndonjë pjesë të kësaj politike mund të sjellë sanksione, ndjekje civile apo penale si dhe masa disiplinore si, pezullim apo heqje të akseseve dhe largim nga detyra.

U njoha me Marrëveshjen e Konfidencialitetit dhe Politikën e Sigurisë

(Nënshkrimi i Punonjësit)

REPUBLIKA E SHQIPËRISË
PROKURORIA E PËRGJITHSHME

Nr 310/2 Prot

Tiranë më, 10. 04.2013

Lënda: Për caktimin e Personit të Kontaktit për Mbrojtjen e të Dhënave

Drejtuar: KOMISIONERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Znj. FLORA ÇABEJ (POGAÇE)

TIRANË

Znj. Komisionere!

Në vijim të komunikimit, konfirmojmë se Person Kontakti për Mbrojtjen e të Dhënave në Prokurori, do të jetë z.Arben Dollapaj, Drejtor i Drejtorisë së Inspektimit dhe Burimeve Njërzore në Prokurorinë e Përgjithshme.

Duke ju falenderuar për bashkëpunimin,

PROKUROR I PËRGJITHSHËM

ADRIATIK LLALLA