

REPUBLIKA E SHQIPËRISË
UNIVERSITETI "ALEKSANDËR MOISIU" Durrës
SENATI AKADEMIK

Nr. 2435 / Prot.
3

Durrës, më 24.10.2025

V E N D I M

Nr. 115, datë 24.10.2025

PËR

"NJË NDRYSHIM NË VENDIMIN E SENATIT AKADEMIK NR. 162, DATË 12.12.2018 "PËR MIRATIMIN E RREGULLORES PËR MBROJTJEN, PËRPUNIMIN, RUAJTJEN DHE SIGURINË E TË DHËNAVE PERSONALE NË UNIVERSITETIN "ALEKSANDËR MOISIU", Durrës"

Bazuar në ligjin, Nr. 80/2015, "Për Arsimin e Lartë dhe Kërkimin Shkencor në Institucionet e Arsimit të Lartë në Republikën e Shqipërisë"; në ligjit Nr. 124 / 2024 "Për mbrojtjen e të dhënave personale"; në Statutit të UAMD-së, neni 15; në Rregullores së UAMD-së; në vendimin e Senatit Akademik Nr. 162, datë 12.12.2018 "Për miratimin e Rregullores për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në Universitetin "Aleksandër Moisiu" Durrës"; referuar shkresës Nr. 2167 prot., datë 25.09.2025 të Drejtorisë së Burimeve Njerëzore dhe Dokumentacionit, si dhe të shkresës 2167/1 prot., datë 16.10.2025 të Drejtorisë Juridike, në mbledhjen e datës 24.10.2025, Senati Akademik,

V E N D O S I:

1. Miratimin e një ndryshimi në Vendimin e Senatit Akademik nr. 162, datë 12.12.2018 "Për miratimin e rregullores për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të dhënave personale në Universitetin "Aleksandër Moisiu", Durrës", sipas materialit bashkëlidhur.
2. Për zbatimin e këtij vendimi ngarkohen:
 - Administratori
 - Zv. Rektorët
 - Drejtuesit e Njësive Kryesore
 - Drejtorët e Drejtorive
 - Drejtoria e Teknologjisë së Informacionit për publikim
3. Ky vendim hyn në fuqi menjëherë.

K R Y E T A R

Prof. Dr. Shkëlqim Fortuzi





REPUBLIKA E SHQIPËRISË
UNIVERSITETI "ALEKSANDËR MOISIU" Durrës

**RREGULLORE
PËR MBROJTJEN PËRPUNIMIN RUAJTJEN DHE SIGURINË E TË DHËNAVE
PERSONALE NË UAMD**

Miraturar me Vendimin Nr 115 datë 24 / 10 / 2025 të Senatit Akademik të Universitetit
"Aleksandër Moisiu" Durrës

**KREU 1
DISPOZITA TË PËRGJITHSHME**

Neni 1

Objekti

Objekti i kësaj Rregullore është përcaktimi i procedurave organizative e teknike, masave për mbrojtjen e të dhënave personale dhe sigurisë, ruajtjes dhe administrimit të të dhënave personale nga strukturat e Universitetit "Aleksandër Moisiu" Durrës (UAMD)

Neni 2

Baza ligjore

Kjo rregullore mbështetet në Kushtetutën e Republikës së Shqipërisë, ligjin nr 80/2015 "Për arsimin e lartë dhe kërkimin shkencor në Institucionet e Arsimit të Lartë në Republikën e Shqipërisë" në ligjin nr.124/2024 "Për mbrojtjen e të dhënave personale" i ndryshuar, urdhërat, udhëzimet dhe vendimet e Komisionerit për mbrojtjen e të dhënave personale si dhe në Statutin dhe Rregulloren e Universitetit "Aleksandër Moisiu" Durrës.

Neni 3

Qëllimi

Kjo rregullore ka për qëllim të përcaktojë parimet e përgjithshme dhe masat organizative dhe teknike për mbrojtjen, ruajtjen, sigurinë dhe administrimin e të dhënave personale. Ajo zbatohet për të gjitha të dhënat e përpunuara nga UAMD, në përputhje me ligjin për mbrojtjen e të dhënave personale.

Përpunimi i të dhënave personale duhet të bëhet në përputhje me Kushtetutën, ligjin për mbrojtjen e të dhënave personale, statutin dhe Rregulloren e UAMD si dhe me misionin e UAMD-së si institucion i arsimit të lartë që vepron konform ligjit nr. 80/2015 "Për arsimin e lartë dhe kërkimin shkencor në institucionet e arsimit të lartë në Republikën e Shqipërisë". Përpunimi i të dhënave personale në UAMD ka në themel respektimin e të drejtave dhe të lirive themelore të njeriut.

Neni 4

Fusha e zbatimit

Kjo rregullore zbatohet për përpunimin e të dhënave personale pjesërisht ose tërësisht, në formë shkresore dhe/ ose elektronike nëpërmjet mjeteve automatike dhe me mjete të tjera që mbahen në një sistem arkivimi në UAMD dhe strukturat përbërëse të saj në përputhje me legjislacionin në fuqi për mbrojtjen e të dhënave personale.

Neni 5 Përkufizime

Në kuptim të kësaj rregulloreje, termat e mëposhtëm kanë kuptimin si vijon:

1. **“Të dhëna personale”** janë çdo informacion që lidhet me një person fizik të identifikuar ose të identifikueshëm (“subjekti i të dhënave”). Një person fizik konsiderohet i identifikueshëm nëse mund të identifikohet drejtpërdrejt ose tërthorazi, në veçanti me anë të një identifikuesi, si emri, numri i identifikimit, të dhënat e vendndodhjes, identifikuesi në internet ose një ose më shumë elemente të veçanta të identitetit fizik, fiziologjik, gjenetik, mendor, ekonomik, kulturor ose social të atij personi.
2. **“Përpunim”** është çdo veprim ose grup veprimesh të kryera me të dhënat personale, me ose pa mjete automatike, si mbledhja, regjistrimi, organizimi, strukturimi, ruajtja, përshtatja ose ndryshimi, rikuperimi, konsultimi, përdorimi, zbulimi me transmetim, shpërndarje ose çdo formë tjetër vëniesh në dispozicion, përafrimi ose kombinimi, kufizimi, fshirja ose shkatërrimi.
3. **“Kufizim i përpunimit”** është shënimi i të dhënave personale të ruajtura me qëllim kufizimin e përpunimit të tyre në të ardhmen.
4. **“Përpunim automatik”** është çdo përpunim i të dhënave personale që realizohet në tërësi ose pjesërisht me mjete automatike.
5. **“Përpunim joautomatik”** është çdo përpunim i të dhënave personale që nuk realizohet me mjete automatike.
6. **“Profilizim”** është çdo formë përpunimi automatik të të dhënave personale që konsiston në përdorimin e këtyre të dhënave për të vlerësuar aspekte personale që lidhen me një person fizik, në veçanti për të analizuar ose parashikuar aspekte që kanë të bëjnë me performancën në punë, gjendjen ekonomike, shëndetin, preferencat personale, interesat, besueshmërinë, sjelljen, vendndodhjen ose lëvizjet e atij personi.
7. **“Pseudonimizim”** është përpunimi i të dhënave personale në një mënyrë që ato nuk mund t’i atribuohen më një subjekti të caktuar pa përdorur informacione shtesë, të cilat mbahen të ndara dhe i nënshtrohen masave teknike dhe organizative për të garantuar që të dhënat personale nuk i atribuohen një personi fizik të identifikuar ose të identifikueshëm.
8. **“Kontrollues”** është personi fizik ose juridik, autoriteti publik, institucioni ose organi tjetër (për efekt të kësaj rregulloreje është UAMD nëpërmjet punonjësve të tij) që, vetëm ose së bashku me të tjerë, përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale.
9. **“Përpunues”** është personi fizik ose juridik, autoriteti publik, institucioni ose organi tjetër tjetër (për efekt të kësaj rregulloreje është UAMD nëpërmjet punonjësve të tij) që përpunon të dhëna personale në emër të kontrolluesit.
10. **“Marrës”** është personi fizik ose juridik, autoriteti publik, institucioni ose organi tjetër, të cilit i zbulohen të dhënat personale, pavarësisht nëse është ose jo palë e tretë.
11. **“Subjekt i të dhënave”** është çdo person fizik të dhënat personale të të cilit përpunohen.
12. **“Pëlqim”** është çdo deklaratë ose veprim i qartë, specifik, i informuar dhe i lirë i vullnetit të subjektit të të dhënave, me të cilin ai jep pranimin për përpunimin e të dhënave personale që e prekin.
13. **“Kategoritë e veçanta të të dhënave personale”** përfshijnë të dhënat që zbulojnë origjinën racore ose etnike, opinionet politike, besimet fetare ose filozofike, anëtarësimin në sindikata, si dhe përfshijnë të dhënat gjenetike, biometrike, shëndetësore, dhe ato që lidhen me jetën seksuale ose orientimin seksual të një personi fizik.
14. **“Cenim i të dhënave personale”** është çdo shkelje e sigurisë që çon në shkatërrimin, humbjen, ndryshimin, zbulimin ose aksesimin e paautorizuar të të dhënave personale, të

transmetuara, ruajtura ose përpunuar në ndonjë mënyrë tjetër.

15. **“Komisioneri”** është Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, autoriteti i pavarur përgjegjës për monitorimin e zbatimit të legjislacionit për mbrojtjen e të dhënave personale.
16. **“Të dhëna penale”** janë të dhënat personale në lidhje me dënimet penale, veprat penale dhe masat e sigurimit të lidhura me to;
17. **“Të dhëna të anonimizuara”** janë të dhëna, të cilat kanë qenë fillimisht të dhëna personale, por janë përpunuar në mënyrë të tillë që nuk është më e mundur që një person fizik ose juridik t’ia atribuojë këto të dhëna një personi fizik të identifikuar ose të identifikueshëm
18. Termat e tjerë që nuk përcaktohen në këtë rregullore kanë kuptimin që u jepet në Ligjin nr. 124/2024.

KREU II **PËRPUNIMI I TË DHËNAVE PERSONALE**

Neni 6 **Parimet për përpunimin e të dhënave personale**

Përpunimi i të dhënave personale në UAMD bëhet duke respektuar parimet e përcaktuara në ligjin nr. 124/2024, si më poshtë:

1. Parimi i ligjshmërisë, drejtësisë dhe transparencës – përpunimi kryhet në mënyrë të ligjshme, të drejtë dhe transparente kundrejt subjektit të të dhënave.
2. Parimi i përpunimit në përputhje me qëllimin – të dhënat mblidhen për një qëllim specifik dhe të ligjshëm, të përcaktuar qartë në momentin e mbledhjes, dhe nuk përpunohen më tej për qëllime të papërputhshme me atë fillestar.
3. Parimi i minimizimit të të dhënave – të dhënat janë të përshtatshme, të nevojshme dhe të kufizuara në raport me qëllimin e përpunimit.
4. Parimi i saktësisë – të dhënat janë të sakta dhe të përditësuara kur është e nevojshme; merren masa për korrigjimin ose fshirjen e të dhënave të pasakta.
5. Parimi i kufizimit të ruajtjes – të dhënat ruhen vetëm për periudhën që është e nevojshme për qëllimin për të cilin përpunohen.
6. Parimi i integritetit dhe konfidencialitetit – garantohet siguria e të dhënave, duke i mbrojtur nga përpunimi i paautorizuar ose i paligjshëm dhe nga humbja apo dëmtimi aksidental.
7. Parimi i përgjegjshmërisë – UAMD, në cilësinë e kontrolluesit, është përgjegjës dhe duhet të jetë në gjendje të provojë përputhshmërinë me parimet e mësipërme.

Neni 7 **Qëllimi i përpunimit**

Çdo punonjës i UAMD-së ka të drejtën e përpunimit të të dhënave personale vetëm për kryerjen e detyrave të parashikuara nga ligji dhe në përputhje me aktet ligjore e nënligjore që rregullojnë mënyrën e përpunimi të të dhënave personale.

Neni 8 **Kriteret për përpunimin e të dhënave personale**

Përpunimi i të dhënave personale në UAMD kryhet vetëm nëse përmbushet të paktën një nga kriteret e mëposhtme:

- a) Subjekti i të dhënave ka dhënë pëlqimin për përpunimin e të dhënave personale për një ose më shumë qëllime specifike;

- b) Përpunimi është i nevojshëm për përmbushjen e një kontrate ku subjekti i të dhënave është palë ose për marrjen e hapave që i paraprijnë lidhjes së kontratës;
- c) Përpunimi është i nevojshëm për përmbushjen e një detyrimi ligjor të UAMD-së si kontrollues;
- ç) Përpunimi është i nevojshëm për mbrojtjen e interesave jetikë të subjektit të të dhënave ose të një personi tjetër fizik;
- d) Përpunimi është i domosdoshëm për përmbushjen nga UAMD e një detyre ligjore me interes publik ose për ushtrimin e funksioneve, detyrave ose kompetencave publike të përcaktuara me ligj;
- dh) Përpunimi është i domosdoshëm për përmbushjen e interesave të ligjshme të UAMD-së ose të një pale të tretë, me përjashtim të rasteve kur të drejtat dhe liritë themelore të subjektit të të dhënave kanë përparësi.
- e) Kur përpunimi bazohet në interesin legjitim, duhet bërë një balancim i qartë mes interesit të UAMD dhe të drejtave të individit.

Kur përpunimi bazohet në shkronjat “c” dhe “d”, ai duhet të jetë i përcaktuar qartë në një dispozitë ligjore dhe proporcional me qëllimin publik që synohet.

Neni 9

Përpunimi i kategorive të veçanta të të dhënave personale (të dhëna sensitive)

1. Përpunimi i kategorive të veçanta të të dhënave personale është i ndaluar, përveç rasteve kur zbatohen masat e përshtatshme për mbrojtjen e të drejtave themelore dhe interesave të subjekteve të të dhënave dhe kur përmbushet të paktën një nga kriteret e mëposhtme:
 - a) Subjekti i të dhënave ka dhënë shprehimisht pëlqimin për përpunimin e një ose disa kategorive të veçanta të të dhënave personale, për qëllime të përcaktuara;
 - b) Përpunimi është i nevojshëm për përmbushjen e një detyrimi ose të drejte specifike të kontrolluesit ose subjektit të të dhënave në fushën e punësimit, sigurimeve shoqërore apo mbrojtjes sociale, në përputhje me legjislacionin në fuqi;
 - c) Përpunimi është i nevojshëm për mbrojtjen e interesave jetikë të subjektit të të dhënave ose të një personi tjetër fizik;
 - d) Përpunimi lidhet me të dhëna të bëra haptazi publike nga subjekti i të dhënave;
 - e) Përpunimi është i nevojshëm për paraqitjen e një kërke, ushtrimin ose mbrojtjen e një të drejte përpara gjykatës ose autoriteteve publike;
 - f) Përpunimi është i nevojshëm për arsye të një interesi publik thelbësor, bazuar në legjislacionin në fuqi;
 - g) Përpunimi është i nevojshëm për qëllime arkivimi për interes publik, kërkime shkencore ose historike, apo qëllime statistikore, në përputhje me ligjin.
2. UAMD nuk përpunon kategori të veçanta të të dhënave personale nëse nuk përmbushet një nga kushtet e mësipërme dhe nëse nuk zbatohen masa të përshtatshme mbrojtëse.

Neni 10

Transferimi ndërkombëtar i të dhënave personale

1. Transferimi ndërkombëtar i të dhënave personale nga UAMD kryhet vetëm në përputhje me ligjin nr. 124/2024, aktet nënligjore të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale dhe klauzolat standarde të mbrojtjes së të dhënave, kur është e aplikueshme.
2. Transferimi lejohet vetëm nëse:
 - o Shteti marrës siguron nivel të përshtatshëm mbrojtjeje, sipas vlerësimit të Komisionerit; ose
 - o UAMD merr masa të përshtatshme mbrojtëse dhe i garanton subjektit të të dhënave të drejta të zbatueshme dhe mjete juridike efektive.

3. Cdo transferim ndërkombëtar i të dhënave nga UAMD miratohet paraprakisht nga Rektori dhe njoftohet ose miratohet nga Komisioneri, në përputhje me legjislacionin në fuqi.
4. Gjatë transferimit merren masa teknike dhe organizative për të parandaluar aksesin e paautorizuar, përvetësimin ose dëmtimin e të dhënave personale.

Neni 11

Përpunimi i të dhënave personale me sistem video survejimi

1. UAMD përpunon të dhënat personale në formën e imazheve dhe tingujve të regjistruar nga sistemet e video survejimit (CCTV), vetëm për qëllime të përcaktuara, legjitime dhe të qarta, në përputhje me parimet e nenit 6 të Ligjit nr. 124/2024.
2. Qëllimi kryesor i përdorimit të sistemit të video survejimit është siguria fizike e personave dhe mbrojtja e pronës së institucionit.
3. Sistemet e video survejimit vendosen vetëm në zona të përcaktuara qartë dhe të nevojshme (hyrje, korridore, shkallë, ambiente të përbashkëta), duke shmangur çdo regjistrim në zona si, tualete, dhoma zhveshje apo në zyra administrative.
4. Pozicionimi i kamerave bëhet në mënyrë të tillë që të minimizohet ndërhyrja në jetën private të individëve dhe të mos regjistrohen imazhe jashtë ambienteve të autorizuara.
5. Në çdo ambient të survejuar vendosen njoftime të dukshme dhe të qarta, në përputhje me udhëzimet e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, që informojnë për ekzistencën e sistemit të survejimit.
6. Përpunimi i të dhënave përmes sistemit të video survejimit bazohet në kriteret e nenit 7 të Ligjit 124/2024, duke respektuar proporcionalitetin dhe domosdoshmërinë e masës.

Neni 12

Përpunimi i të dhënave personale që nuk kërkon identifikimin e subjektit

- Kur qëllimet për të cilat UAMD përpunon të dhëna personale nuk kërkojnë ose nuk më lejojnë identifikimin e subjektit të të dhënave, institucioni nuk është i detyruar të mbajë, marrë ose përpunojë informacione shtesë vetëm për të identifikuar subjektin, me qëllim respektimin e detyrimeve që rrjedhin nga ligji për mbrojtjen e të dhënave personale.
- Nëse subjekti i të dhënave ofron informacione shtesë që e bëjnë të mundur identifikimin, të drejtat dhe detyrimet ligjore të UAMD zbatohen në përputhje me ligjin.
- UAMD merr masa të arsyeshme për të siguruar që përpunimi i këtij lloji të të dhënave të jetë në përputhje me parimet e ligjshmërisë, proporcionalitetit dhe minimizimit të të dhënave, dhe të mos çojë në identifikim të paautorizuar.

Neni 13

Detyrimet për përpunimin e të dhënave të marra nga sistemet e video survejimit

Sistemi i video survejimit nuk duhet të cenojë jetën private të individëve përtej asaj që është domosdoshmërisht e nevojshme për qëllimin e vendosjes.

1. Sistemi i video survejimit nuk duhet të cenojë jetën private të individëve përtej asaj që është domosdoshmërisht e nevojshme për qëllimin e vendosjes.
2. Përpunimi i të dhënave të marra nga sistemi i video survejimit lejohet vetëm për një interes të rëndësishëm publik.
3. Instalimi i sistemit të video survejimit është rreptësisht i ndaluar në ambientet që përdoren ekskluzivisht në tualete, dhoma zhveshje, apo në zyra administrative.
4. Të dhënat e regjistruara përpunohen dhe ruhen vetëm për qëllimet për të cilat janë mbledhur dhe

- nuk përdoren për qëllime të tjera, përveç rasteve kur ekziston një bazë ligjore specifike.
5. Periudha e ruajtjes së regjistrimeve është maksimumi 60 ditë, përveç rasteve kur të dhënat kërkojnë nga organet ligj zbatuese për hetime, në përputhje me ligjin.
 6. Çdo akses ose përdorim i të dhënave të video survejimit dokumentohet dhe monitorohet nga personat përgjegjës të caktuar nga UAMD.
 7. UAMD merr masa teknike dhe organizative për të garantuar sigurinë dhe integritetin e të dhënave të video survejimit dhe për të parandaluar aksesin e paautorizuar.

Neni 14

Masat e marra për sigurinë e të dhënave dhe mbrojtjen e sistemeve të video survejimit

1. UAMD merr masa organizative dhe teknike të përshtatshme për të siguruar sistemet e video survejimit, regjistrimet dhe pajisjet, në mënyrë që të mbrohen nga:
 - o akses i paautorizuar ose aksidental;
 - o ndryshimi, shkatërrimi ose humbja e paautorizuar;
 - o përpunimi i paligjshëm.
2. Këto masa përfshijnë:
 - o ruajtjen e regjistrimeve në ambiente të sigurta;
 - o kufizimin e aksesit vetëm për personat e autorizuar;
 - o regjistrimin e çdo aksesimi;
 - o përdorimin e fjalëkalimeve dhe kontrolleve të aksesit për sistemet elektronike;
 - o mirëmbajtjen periodike të pajisjeve për të siguruar funksionimin korrekt dhe të sigurt.
3. Personeli/studentët mund të kenë akses në regjistrime vetëm nëse kjo është e domosdoshme për përmbushjen e detyrave të tyre, në përputhje me parimin e proporcionalitetit.

Neni 15

Të drejtat e subjektit të të dhënave të marra nga sistemet e video survejimit

1. Subjektet e të dhënave (personeli/studentët) kanë të drejtë të informohen në mënyrë të qartë dhe të dukshme për ekzistencën e sistemit të video survejimit, përmes njoftimeve të vendosura në mënyrë të dukshme në ambientet e survejuara.
2. Subjektet e të dhënave kanë të drejtë të:
 - o kërkojnë akses në regjistrimet që i përkasin atyre;
 - o kundërshtojnë përpunimin në rast se cenohen të drejtat dhe liritë e tyre;
 - o kërkojnë fshirjen e të dhënave në rast se përpunimi është i paligjshëm.
3. Kërkesat për ushtrimin e këtyre të drejtave trajtohen nga struktura përgjegjëse e UAMD brenda afateve të përcaktuara nga ligji, dhe në bashkëpunim me Komisionerin kur është e nevojshme.
4. Ushtrimi i këtyre të drejtave nuk duhet të cenojë të drejtat dhe interesat legjitime të palëve të tjera apo hetimet ligjore në zhvillim.

Neni 16

Detyrimi i ruajtjes së konfidencialitetit të të dhënave të marra nga sistemet e video survejimit

1. Punonjësit, përpunuesit dhe personat e autorizuar që marrin dijeni për të dhënat personale të përfuara nga sistemet e video survejimit, janë të detyrueshëm të ruajnë konfidencialitetin dhe besueshmërinë e këtyre të dhënave, edhe pas përfundimit të marrëdhënies së punës ose përfundimit të funksioneve të tyre.
2. Të dhënat e video survejimit nuk mund të përhapen, publikohen ose shpërndahen përveç rasteve kur parashikohet me ligj ose me vendim të organeve kompetente.
3. Shkelja e detyrimit të konfidencialitetit përbën shkelje disiplinore dhe administrative, dhe ndëshkohet sipas legjislacionit në fuqi.

KREU III TË DREJTAT E SUBJEKTIT TË TË DHËNAVE

Neni 17

Zbatimi i të drejtave të subjekteve të të dhënave personale

1. UAMD garanton respektimin e të drejtave të subjekteve të të dhënave personale në përputhje me ligjin, duke siguruar ushtrimin e këtyre të drejtave në mënyrë efektive dhe të qartë.
2. Subjektet e të dhënave kanë të drejtë të:
 - o informohen në lidhje me përpunimin e të dhënave të tyre;
 - o marrin akses në të dhënat personale që i përkasin;
 - o kërkojnë korrigjimin e të dhënave të pasakta;
 - o kërkojnë fshirjen e të dhënave personale ("e drejta për t'u harruar") në përputhje me nenin 17 të ligjit;
 - o kërkojnë kufizimin e përpunimit;
 - o kundërshtojnë përpunimin për arsye që lidhen me situatën e tyre të veçantë;
 - o marrin të dhënat në një format të strukturuar (portabiliteti i të dhënave), nëse është e aplikueshme.
3. Kërkesat trajtohen nga strukturat përgjegjëse të UAMD brenda 30 ditëve nga marrja e kërkesës, me mundësi shtyrjeje në raste të veçanta, sipas nenit 18 të ligjit.
4. UAMD ka të drejtë të kërkojë verifikimin e identitetit të subjektit para dhënies së informacionit.

Neni 18

Kërkesë për informacion

1. Çdo subjekt i të dhënave ka të drejtë të paraqesë një kërkesë për të marrë informacion në lidhje me përpunimin e të dhënave të tij personale nga UAMD.
2. Kërkesa mund të bëhet nga:
 - o vetë personi;
 - o përfaqësuesi ligjor i pajisur me autorizim;
 - o persona të tjerë që vërtetojnë interes të ligjshëm, në përputhje me ligjin.
3. UAMD jep përgjigje brenda 30 ditëve, në formë të shkruar ose elektronike, në gjuhë të qartë dhe të kuptueshme.
4. Nëse kërkesa nuk mund të plotësohet, UAMD informon kërkuesin për arsyet dhe të drejtën për të paraqitur ankesë te Komisioneri.

KREU IV NJOFTIMI

Neni 19

Përgjegjësia për të njoftuar

1. UAMD ka detyrimin të njoftojë Komisionerin dhe subjektet e të dhënave për çdo cenim të sigurisë së të dhënave personale që mund të shkaktojë rrezik për të drejtat dhe liritë e individëve.
2. Njoftimi bëhet pa vonesë të panevojshme, dhe në çdo rast brenda 72 orëve nga momenti i njohjes me cenimin, sipas nenit 29 të ligjit.
3. Njoftimi përmban natyrën e cenimit, kategoritë e të dhënave të prekura, pasojat e mundshme dhe masat e marra.



Personi i kontaktit i autorizuar nga Rektori është përgjegjës për përgatitjen dhe dërgimin e njoftimit.

KREU V SIGURIA E TË DHËNAVE PERSONALE

Neni 20

Masat për sigurinë e të dhënave personale

- UAMD, në cilësinë e kontrolluesit, zbaton masa teknike dhe organizative të përshtatshme për të garantuar një nivel sigurie në përpunimin e të dhënave personale, në përputhje me natyrën, qëllimet, kontekstin dhe rreziqet e përpunimit.
- Masat e sigurisë synojnë të mbrojnë të dhënat personale nga:
 - a) përpunimi i paautorizuar ose i paligjshëm;
 - b) qasja e paautorizuar;
 - c) shkatërrimi, humbja, ndryshimi ose dëmtimi aksidental;
 - ç) çdo formë tjetër cenimi të konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave.
- Masat përfshijnë, ndër të tjera:
 - a) përdorimin e mjeteve të përshtatshme të kontrollit të aksesit fizik dhe elektronik;
 - b) enkriptimin dhe anonimizimin kur është e përshtatshme;
 - c) mekanizma të vazhdueshëm monitorimi dhe auditimi të sigurisë;
 - ç) procedura të qarta për kopje rezervë dhe rikuperim pas incidenteve;
 - d) trajnimin e stafit dhe përcaktimin e qartë të përgjegjësive për sigurinë e të dhënave.
- Masat teknike dhe organizative rishikohen dhe përditësohen periodikisht, sidomos në rast ndryshimesh të kontekstit të përpunimit ose të rreziqeve të reja.
- Çdo incident që cenon të dhënat personale trajtohet sipas procedurave të veçanta për njoftimin dhe menaxhimin e shkeljeve, në përputhje me legjislacionin në fuqi.

Neni 21

Masat e sigurisë për ruajtjen nga zjarri

UAMD zbaton masa për mbrojtjen nga zjarri të pajisjeve dhe ambienteve ku ruhen të dhëna personale, përfshirë ndalimin e përdorimit të materialeve ndezëse, kabllave provizore, përdorimin e sistemeve të alarmit dhe respektimin e rregullave të sigurisë fizike të përcaktuara në legjislacionin përkatës.

Neni 22

Mbrojtja e ambienteve

1. Ambientet ku përpunohen të dhëna personale mbrohen me masa fizike, teknike dhe organizative për të parandaluar aksesin e paautorizuar.
2. Ndalohej hyrja e personave të paautorizuar; çdo hyrje lejohet vetëm me autorizim nga Rektori.
3. Ambientet survejohen dhe mbrohen fizikisht me roje gjatë 24 orëve.
4. Përdoren kasaforta dhe brava të sigurta për ruajtjen e dokumenteve.
5. Kryhet kontroll periodik për të parandaluar përdorimin e pajisjeve të paautorizuara të regjistrimit.



Neni 23 **Personat e autorizuar për akses**

Vetëm personat e autorizuar nga Rektori ose strukturat përgjegjëse të UAMD kanë të drejtë të qëndrojnë në ambientet ku përpunohen të dhëna personale.

Neni 24 **Baza e të dhënave të studentëve**

Përpunimi dhe transmetimi i të dhënave të studentëve bëhet në përputhje me ligjin për arsimin e lartë dhe Ligjin 124/2024, duke respektuar parimet e sigurisë, proporcionalitetit dhe kufizimit të ruajtjes. UAMD siguron mbrojtjen teknike dhe ligjore të këtyre të dhënave gjatë çdo faze të përpunimit.

Neni 25 **Mbrojtja e të dhënave personale të studentëve/punonjësve**

UAMD garanton që çdo qasje, përdorim ose shpërndarje e të dhënave të studentëve/punonjësve të bëhet vetëm në përputhje me qëllimin ligjor dhe me pëlqimin ose bazën ligjore të përshtatshme, në përputhje me nenet 7, 12 dhe 17 të Ligjit 124/2024.

Neni 26 **Mbrojtja e pajisjeve elektronike**

Pajisjet elektronike që përdoren për përpunimin e të dhënave personale janë në pronësi të UAMD dhe përdoren vetëm për qëllime institucionale.

Përdorimi i tyre nga personeli dhe studentët bëhet në përputhje me rregullat e sigurisë dhe me autorizim nga strukturat përkatëse.

UAMD merr masa teknike dhe organizative për mbrojtjen e pajisjeve nga akseset e paautorizuara, në përputhje me ligjin 124/2024.

Neni 27 **Programet kompjuterike (softëare)**

Instalimi, përdorimi ose heqja e programeve kompjuterike që përpunojnë të dhëna personale bëhet vetëm me autorizim të posaçëm të strukturave përgjegjëse të UAMD.

Çdo program duhet të jetë i licencuar dhe i sigurt.

Nuk lejohet përdorimi i programeve të paautorizuara ose "pirate".

Neni 28 **Monitorimi i sistemeve**

UAMD monitoron akseset dhe përdorimin e sistemeve që përpunojnë të dhëna personale, për të parandaluar aksesin e paautorizuar dhe përdorimin e papërshtatshëm.

Regjistrat e aksesit ruhen për periudhën e përcaktuar dhe mund të përdoren vetëm për qëllime sigurie ose hetimi të shkeljeve.

Neni 29 **Monitorimi dhe regjistrimi i aksesit për të dhënat personale**



Hyrja tek të dhënat dhe informacionet u nënshtrohet normave të veçanta të sigurisë për ruajtjen e paprekshmërisë dhe për azhurnimin e tyre. Sistemi është i ndërtuar në mënyrë të tillë që vërteton identitetin e përdoruesit. 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.

Regjistrimet e përditshme administrohen nga njësi organizative të administratës së përgjithshme të institucionit, përgjegjës për mbrojtjen e të dhënave, që përcakton përmbajtjen e të dhënave të regjistrimeve ditore dhe kohën e ruajtjes së të dhënave personale. Periudha e ruajtjes së regjistrimit të të dhënës ose informacionit është e barabartë me periudhën e ruajtjes së dokumentit shkresor që përmban këtë të dhënë ose informacion. Me kalimin e këtij afati këto të dhëna arkivohen ose asgjësohen. 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 vetijake.

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.

Neni 30

Drejtoria e Teknologjisë së Informacionit

DTI në UAMD merr masa organizative dhe teknike të administrimit dhe të garantimit të sigurisë së bazës të të dhënave të studentëve/ punonjësve, si dhe të dhëna të tjera nga dëmtime/ shkatërtime të paligjshme, aksidentale, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë e paligjshme përpunimi.

Drejtoria e Teknologjisë së Informacionit duhet të ketë një kopje dhe një dublikatë të të gjitha të dhënave dhe softëare që mbahen ose ruhen në kompjuterin qendror. Kopja dublikatë duhet të mbahet në një vend të sigurt jashtë godinës në të cilën gjendet kompjuteri qendror. DTI mban një kopje të të dhënave dhe të sistemit të vendosur në kompjuterin dytësor.

Një kopje dublikatë duhet të mbahet në një vend ose ambient të ndryshëm nga godina në të cilën ndodhet DTI. Numri dhe forma e kopjeve shtesë e dokumenteve, mjeteve të tjera të komunikimit në të cilën ato ruhen përcaktohet nga njësia përkatëse për çdo dokument.

Neni 31

Dublikata e programeve

Dublikata e programeve me të dhëna që përdoren në rastin e fatkeqsive natyrore ose në raste të gjëndjes së jashtëzakonshme ose gjëndje lufte duhet të ruhen në vende ose ambiente që ndodhen jashtë zyrës kryesore të njësisë organizative përkatëse të UAMD-së. Mënyra e krijimit, shumëfishimit dhe ruajtjes së këtyre dublikatave përcaktohet në mënyrë të veçantë për çdo dokument, në përputhje me rregullat e ruajtjes dhe garantimit të tyre, të vendosura nga njësia organizative përkatëse dhe me rregullat e zbatueshme në rastin e fatkeqsive natyrore.

Neni 32

Humbja ose zhdukja e dokumenteve

Në rast humbjeje ose zhdukjeje të një dokumenti që përmban të dhëna personale, personi përgjegjës njofton menjëherë strukturat kompetente dhe ndërmerren masa për identifikimin e rrethanave dhe parandalimin e pasojave, duke respektuar detyrimin për njoftimin e cënimit të të dhënave.

KREU VI



SANKSIONE ADMINISTRATIVE DHE ANKIMET NDAJ TYRE

Neni 33 Shkeljet dhe përgjegjësitë

1. Çdo shkelje e dispozitave të kësaj rregulloreje dhe të ligjit për mbrojtjen e të dhënave personale sjell përgjegjësi disiplinore, administrative dhe/ose penale, në përputhje me legjislacionin në fuqi.
2. Punonjësit dhe personat e autorizuar janë individualisht përgjegjës për çdo përpunim të të dhënave personale në kundërshtim me ligjin.
3. Masat disiplinore dhe administrative vendosen në përputhje me Kodin e Punës dhe aktet e brendshme të UAMD.
4. Shkeljet e rënda i referohen menjëherë Komisionerit për veprime të mëtejshme.

Neni 34 Trajtimi i ankesave

1. Subjektet e të dhënave kanë të drejtë të paraqesin ankesa në lidhje me mënyrën e përpunimit të të dhënave të tyre personale nga UAMD.
2. Ankesat paraqiten me shkrim në adresë të personit përgjegjës ose në adresën zyrtare të UAMD dhe regjistrohen në regjistrin përkatës.
3. Personi përgjegjës shqyrton ankesën dhe jep përgjigje të arsyetuara brenda 30 ditëve, në përputhje me ligjin.
4. Subjektet e të dhënave mund t'i drejtohen Komisionerit nëse nuk janë të kënaqur me përgjigjen e UAMD ose nëse nuk kanë marrë përgjigje në afat.
5. UAMD bashkëpunon me Komisionerin për zgjidhjen e rasteve të ankesave në mënyrë efikase dhe transparente.

Neni 35 Mjetet juridike gjyqësore të subjekteve të të dhënave

- Çdo subjekt i të dhënave personale ka të drejtë të paraqesë padi në gjykatë nëse vlerëson se të drejtat e tij të garantuara nga legjislacioni për mbrojtjen e të dhënave personale janë shkelur si rezultat i përpunimit të të dhënave nga UAMD, në cilësinë e kontrolluesit ose përpunuesit.
2. Subjekti i të dhënave ka gjithashtu të drejtë të paraqesë padi kundër vendimeve ose mosveprimeve të Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, në përputhje me nenin 92 të Ligjit nr. 124/2024.
 3. Padia mund të ngrihet pranë gjykatave shqiptare; në vendin ku subjekti i të dhënave ka vendbanimin ose selinë; ose në vendin ku ndodhet selia e UAMD-së si kontrollues/përpunues.
 4. Ushtrimi i mjeteve juridike gjyqësore është i pavarur nga e drejta e subjektit për të paraqitur ankesë pranë Komisionerit, sipas nenit 86 të Ligjit nr. 124/2024.

KREU VII DISPOZITA TË FUNDIT

Neni 36 Informimi dhe ndërgjegjësimi

1. UAMD ndërmerr masa të vazhdueshme për informimin dhe ndërgjegjësimin e personelit, studentëve dhe palëve të treta mbi rregullat për mbrojtjen e të dhënave personale dhe detyrimet që rrjedhin nga ligji.



Në faqen zyrtare të internetit të UAMD publikohen politika të qarta dhe të kuptueshme për mbrojtjen e të dhënave personale dhe mënyrën e ushtrimit të të drejtave nga subjektet e të dhënave.

Neni 37

Bashkëpunimi dhe konsultimi me Komisionerin

1. UAMD dhe personi përgjegjës bashkëpunojnë në mënyrë aktive me Komisionerin për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale gjatë çdo inspektimi, kontrolli apo kërkesë për informacion.
2. Të gjitha strukturat e UAMD janë të detyruara t'i vënë në dispozicion Komisionerit dokumentacionin dhe informacionin e kërkuar, në përputhje me afatet ligjore.
3. Komisioneri ka të drejtë të kryejë inspektime në ambientet e UAMD-së për të verifikuar respektimin e legjislacionit dhe të kësaj rregulloreje.

Neni 38

Hyrja në fuqi

Kjo rregullore hyn në fuqi pas miratimit nga Senati Akademik dhe njoftimit zyrtar në faqen e internetit të UAMD.

1. Me hyrjen në fuqi të kësaj rregulloreje, çdo dispozitë e mëparshme e brendshme që bie ndesh me të, shfuqizohet.
2. Çdo ndryshim i ardhshëm i ligjit për mbrojtjen e të dhënave personale do të reflektohet në këtë rregullore.