



REPUBLIKA E SHQIPËRISË  
AKADEMIA E SHKENCAVE  
Kryesia

Rregullore

**Për mbrojtjen, përpunimin, ruajtjen dhe sigurinë e të  
dhënave personale në Akademinë e Shkencave të  
Shqipërisë**

**Kreu I  
Dispozita të përgjithshme**

**Neni 1  
Objekti**

Objekti i kësaj rregulloreje është përcaktimi i procedurave organizative e teknike dhe masave për mbrojtjen e të dhënave personale dhe sigurisë, ruajtjes dhe administrimit të të dhënave personale nga strukturat e Akademisë së Shkencave të Shqipërisë (ASHSH).

**Neni 2  
Baza ligjore**

Mbrojtja e të dhënave personale në ASHSH mbështetet në legjislacionin vendës dhe ndërkombëtar.

1. Aktet kombëtare janë:

- Kushtetuta e Republikës së Shqipërisë, nenet 15-58 të saj;
- Ligji nr. 9887 datë 10.03.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar;
- Ligji nr. 43/2023 *Për qeverisjen elektronike*;
- Urdhrat, udhëzimet dhe vendimet e Komisionerit për Mbrojtjen e të Dhënave Personale;
- Aktet ligjore dhe nënligjore organike për organizimin dhe funksionimin e Akademisë së Shkencave të Shqipërisë.

## 1. Aktet ndërkombëtare janë:

- a. Deklarata Universale e të Drejtave dhe Lirive të Njeriut;
- b. Konventa për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, amenduar nga Protokollin nr. 11, hyrë në fuqi më 1 nëntor 1998;
- c. Direktivat 2002/58/EC dhe 95/46/EC të Këshillit Europian dhe Parlamentit Europian;
- ç. Konventa 108 e Këshillit të Europës *Për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale*, ratifikuar me Ligjin nr. 9288, datë 7.10.2004;
- d. Protokollin shtesë i Konventës së Këshillit të Europës *Për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale, lidhur me autoritetet mbikqyrëse dhe lëvizjen ndërkufitare të të dhënave personale*, ratifikuar me Ligjin nr. 9287, datë 7.10.2004.

### Neni 3 Qëllimi

Kjo rregullore ka për qëllim të përcaktojë parimet e përgjithshme dhe masat organizative e teknike për mbrojtjen, ruajtjen, sigurinë dhe administrimin e të dhënave personale. Ajo zbatohet për të gjitha të dhënat e përpunuara nga ASHSH dhe strukturat pranë saj, në përputhje me ligjin *Për mbrojtjen e të dhënave personale* dhe aktet e cituara në nenin 2 të kësaj rregulloreje.

### Neni 4 Përkufizime

1. Për qëllim të kësaj rregulloreje, termat e mëposhtëm kanë këtë kuptim:
  - a. *Të dhëna personale* janë çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, 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.
  - b. *Subjekt i të dhënave personale* është çdo person fizik, të cilit i përpunohen të dhënat personale.
  - c. *Kontrollues*, për efekt të kësaj rregulloreje është ai që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet e këtë rregullore, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në to.
  - ç. *Përpunues*, për efekt të kësaj rregulloreje është ose janë çdo person fizik ose juridik, autoritet publik ose çdo njësi tjetër, përveç punonjësve të kontrolluesit, që përpunojnë të dhëna për vetë kontrolluesin.
  - d. *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 ose jo.
  - dh. *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 ose ndryshe duke vënë 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.

e. *Pëlqimi i subjekteve të të dhënave* është çdo deklaratë me shkrim, e dhënë shprehimisht me vullnet të plotë e të lirë dhe duke qenë në dijeni të plotë për arsyen pse të dhënat do të përpunohen, lëshuar nga subjekti, duke u shprehur dakord që të përpunohen të dhënat e tij.

ë. *Të dhëna sensitive* është çdo informacion për personin fizik, që ka të bëjë me origjinën e tij racore ose etnike, mendimet politike, anëtarësimin në sindikata, besimin fetar apo filozofik, dënimin penal, si dhe të dhëna për shëndetin dhe jetën seksuale referuar Ligjit nr. 9887, datë 10.3.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar, neni 3, pika 4.

f. *E dhënë gjyqësore* është çdo e dhënë lidhur me vendimet në fushën e gjyqësorëve penale, civile, administrative apo me dokumentimet në regjistrat penalë, civilë, ato të dënimeve administrative etj.

g. *Qëllimi historik* është qëllimi për studime, hulumtime, kërkime dhe dokumentim të figurave, fakteve dhe rrethanave të së kaluarës. *Qëllimi statistikor* është qëllimi për hulumtime statistikore, prodhim të të dhënave statistikore edhe nëpërmjet sistemit informativ statistikor. *Qëllimi shkencor* është qëllimi për studime dhe hulumtime sistematike, që finalizon zhvillimin e dijeve shkencore në një sektor e drejtim të caktuar. *E drejtë informimi* ka kuptimin sipas përcaktimit në *ligjin për të drejtën e informimit*.

gj. *Sistem audio-video* është sistemi CCTV, që përfshin përdorimin e kamerave, pajisjeve arkivuese dhe pajisjeve të tjera ndihmëse që ruajnë dhe përpunojnë të dhënat.

h. *Sistem arkivimi* është çdo grup i strukturuar i të dhënave personale, të cilat janë të aksesueshme në bazë të kriterëve specifike.

2. Termat e tjerë të përdorur në zbatim të kësaj rregullorje kanë të njëjtin kuptim si në Ligjin nr. 9887 datë 10.3.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar.

#### Neni 5

#### Fusha e zbatimit

Kjo rregullore zbatohet për përpunimin e të dhënave personale plotësisht ose pjesërisht, nëpërmjet mjeteve automatike dhe me mjete të tjera që mbahen në një sistem arkivimi në funksion të studimi shkencor a projekti apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit pranë ASHSH për vlerësimin e evidentimin e punës shkencore.

## Kreu II

## Përpunimi i të dhënave personale

#### Neni 6

#### Mbrojtja e të dhënave personale

Çdo punonjës i njësive a strukturave të SHSH, që merret me përpunimin e të dhënave personale të subjekteve, detyrohet të zbatojë kërkesat e neneve 2 dhe 5 të Ligjit *Për mbrojtjen e të dhënave personale*, i ndryshuar, si më poshtë:

- Përpunimin e të dhënave personale dhe transmetimin e tyre vetëm në përputhje me qëllimin dhe veprimtarinë e ASHSH në cilësinë e kontrolluesit;
- Respektimin e parimit për përpunimin e ligjshëm të të dhënave personale, duke respektuar dhe garantuar të drejtat dhe liritë themelore të njeriut dhe, në veçanti, të drejtën e ruajtjes së jetës private;
- Kryerjen e përpunimit në mënyrë të drejtë dhe të ligjshme;
- Grumbullimin e të dhënave personale për qëllime specifike, të përcaktuara qartë e legjitime dhe *kryerjen e përpunimit të tyre në përputhje me këto qëllime*;
- Të dhënat që do të përpunohen duhet të jenë të mjaftueshme, të lidhen me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim;
- Të dhënat duhet të jenë të sakta nga ana faktike dhe, kur është e nevojshme, të bëhet përditësimi e kryerja e çdo veprimi për të siguruar që të dhënat e pasakta e të parregullta të fshihen apo të ndryshohen;
- Të dhënat duhet të mbahen në atë formë, që të lejojnë identifikimin e subjekteve të të dhënave për një kohë, por jo më tepër sesa është e nevojshme për qëllimin, për të cilin ato janë grumbulluar ose përpunuar më tej.

#### Neni 7

#### Qëllimi i përpunimit

1. Çdo punonjës i strukturave a njësive si dhe grup studiuesish të Akademisë së Shkencave mund t'i përdorë të dhënat personale vetëm për kryerjen e detyrave të parashikuara nga ligji dhe në përputhje me aktet ligjore e nënligjore që rregullojnë mënyrën e përpunimit të të dhënave personale.
2. Qëllimi i përpunimit të të dhënave personale të subjekteve kandidatë për anëtarë të Asamblesë së ASHSH është përmbushja e detyrimeve që rrjedhin nga Ligji nr. 53/2019 *Për Akademinë e Shkencave në Republikën e Shqipërisë*, Statuti e akteve nënligjore përkatëse të dala në dhe për zbatim të këtij ligji.
3. Qëllimi i përpunimit të të dhënave personale të vizitorëve apo punonjësve të medias është identifikimi i tyre në funksion të ruajtjes dhe mbrojtjes së personelit, dokumentacionit etj.
4. Qëllimi i përpunimit të të dhënave personale të personelit në organikë dhe jashtë organike të ASHSH është për efekt të krijimit të marrëdhënies së punës dhe përmbushjes së detyrimeve për administrimin e dosjes personale të punonjësit, në zbatim të Ligjit nr. 53/2019 *Për Akademinë e Shkencave në Republikën e Shqipërisë*, Statutit të ASHSH, vendimeve të Kryesisë dhe Vendimit të Kuvendit nr. 36/2020 *Për miratimin e strukturës, organikës dhe nivelit të pagave për Akademinë e Shkencave në Republikën e Shqipërisë*.
5. Të dhënat për projektet e studimet përpunohen nga vetë studiuesit e tyre.

#### Neni 8

## Kriteret e përpunimit të të dhënave personale

1. Punonjësit e çdo strukture të Akademisë së Shkencave të Shqipërisë që përpunojnë të dhëna personale të subjekteve, bazohen në kriteret e përcaktuara në nenin 6 të Ligjit *Për mbrojtjen e të dhënave personale*.
2. Të dhënat personale përpunohen vetëm:
  - Nëse subjekti i të dhënave personale ka shprehur pëlqimin
  - Për të mbrojtur interesat jetikë të subjektit të të dhënave;
  - Për përmbushjen e një detyrimi ligjor të kontrolluesit;
  - Për kryerjen e një detyre ligjore me interes publik a ushtrimin e një kompetence të kontrolluesit a të një pale të tretë, së cilës i janë përhapur të dhënat;
  - Për ndjekjen e interesave legjitime të ASHSH ose të një pale të tretë, së cilës i janë përhapur të dhënat, përveç kur këta interesa mbizotërojnë mbi interesat për mbrojtjen e të drejtave dhe të lirive themelore të subjektit të të dhënave.
3. Si raste përjashtimore të mbrojtjes së të dhënave personale parashikohen:
  - Për subjektet kandidatë për anëtarë të Asamblesë ASHSH, këto të drejta e liri janë të kufizuara sipas nenit 7 të Statutit të ASHSH;
  - Për rastet e informacionit për personat publikë zyrtarë ose punonjës të administratës publike, janë të kufizuara sipas nenit 4, pika 4, germa “b” e Ligjit nr. 9887 datë 10.3.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar.

### Neni 9

#### Përpunimi i të dhënave sensitive

1. Përpunimi i të dhënave sensitive nga çdo punonjës kryhet në përputhje me kriteret e përcaktuara në nenin 7 të Ligjit *Për mbrojtjen e të dhënave personale*, i ndryshuar.
2. Çdo punonjës i strukturave të ASHSH që në veprimtarinë e tij referuar rregullores së brendshme dhe akteve ligjore për organizimin e brendshëm përpunojnë të dhëna sensitive të cilat sigurohen gjatë dhe për shkak të ushtrimit të veprimtarisë duhet të nënshkruajnë deklaratën e konfidencialitetit sipas modelit bashkëlidhur rregullores.

### Neni 10

#### Transferimi ndërkombëtar i të dhënave

1. Në rast të kryerjes së transferimit ndërkombëtar të të dhënave personale punonjësi i ASHSH zbaton parashikimet e nenit 8 dhe 9 të Ligjit *Për mbrojtjen e të dhënave personale*, i ndryshuar e aktet nënligjore të dala në zbatim të tij.
2. Të dhënat dhe informacionet, mund t’u komunikohen institucioneve homologe të shteteve të tjera në bazë të marrëveshjes së bashkëpunimit, me kusht që në shtetin kërkues këto të dhëna dhe informacione të trajtohen dhe të ruhen, në përputhje me legjislacionin për mbrojtjen e të dhënave.
3. Të dhënat dhe informacionet e përmendura në paragrafin e mësipërm trajtohen vetëm nga autoritetet përkatëse të shtetit marrës.

4. Transferimi i të dhënave të cilat janë “shumë sekrete” realizohet nëpërmjet linjave të komunikimit elektronik të mbrojtura kriptologjikisht e cila përdoret nga njësia/të përgjegjëse për mbrojtjen e të dhënave. Kjo nënkupton që procedurat dhe masat e mbrojtjes kriptologjike për transferimin e të dhënave përcaktohen nga ASH.

## Kreu III Të drejtat e subjektit të të dhënave

### Neni 11

#### Zbatimi i të drejtave të subjekteve të të dhënave personale

1. Përhapja ose komunikimi i të dhënave personale kryhet në përputhje me qëllimin për të cilin janë grumbulluar këto të dhëna.
2. Çdo person ka të drejtë që të njihet me të dhënat personale të përpunuara nëpërmjet një kërkesë me shkrim.
3. Çdo institucion që përpunon të dhëna personale është i detyruar që në bazë të Ligjit nr. 9887 datë 10.3.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar si dhe të zbatojë këto të drejta të subjekteve të të dhënave personale:
  - a. Të drejtën për akses;
  - b. Të drejtën për të kërkuar korrigjimin ose fshirjen;
  - c. Vendimmarrjen automatike;
  - d. Të drejtën për të kundërshtuar;
  - e. Të drejtën për tu ankuar;
  - ë. Të drejtën për kompensimin e demit.
4. Kërkesa duhet të përmbajë të dhëna të mjaftueshme për të vërtetuar identitetin e kërkuarit. Kontrolluesi, brenda 30 ditëve nga data e marrjes së kërkesës, informon subjektin e të dhënave ose i shpjegon atij arsyet e mosdhënies së informacionit.

### Neni 12

#### Kërkesa për informacion

1. Kërkesën për informacion mund ta bëjë:
  - a. Vetë personi ;
  - b. Përfaqësuesi ligjor i pajisur me autorizimin përkatës;
  - c. Persona të tjerë të cilët megjithëse nuk kanë interes të drejtpërdrejtë, provojnë se kanë një interes të ligjshëm për të marrë dijeni në lidhje me këto të dhëna dhe që përputhet me qëllimin e grumbullimit të këtyre të dhënave;
  - ç. Prindi ose kujdestari kur:
    - Fëmija nuk ka zotësi të plotë për të vepruar

• Prindi është duke vepruar në interes të fëmijës.

Përgjigja në çdo rast dërgohet në adresën e kërkuar nga vetë kërkuesi.

## Kreu IV

### Siguria e të dhënave personale

#### Neni 13

#### Masat për sigurinë e të dhënave

ASHSH dhe njësitë e kërkim studimit apo qendrat e ngritura pranë saj, 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, veçanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë tjetër e paligjshme përpunimi.

1. Mbrojtja e të dhënave personale realizohet me marrjen e masave organizative, që janë:

a. Kryetari përcakton strukturat dhe/ose personat përgjegjës për mbledhjen e përpunimin e të dhënave personale si dhe funksionet e tyre, përveç rasteve kur kjo shprehet në ligj, ku si rregull nëpunësi i caktuar është koordinatori për të drejtën e informimit, i cili krahas detyrës së tij funksionale ushtron dhe këtë përgjegjësi.

b. Personi/at përgjegjës për sigurinë e të dhënave personale në institucion udhëzon/jnë 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;

c. Punonjësi i informacionit në ASHSH (apo punonjësit e tjerë në mungesë të punonjësit të informacionit) dhe personat e autorizuar ndalojnë hyrjen e personave të paautorizuar në mjediset e kontrolluesit ose përpunuesit të të dhënave.

ç. Aksesit në të dhënat dhe programet, bëhet vetëm nga personat e autorizuar, ndalojnë hyrjen në mjetet e arkivimit dhe përdorimin e tyre nga persona të paautorizuar;

d. Vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetëm me autorizim të ASHSH dhe çdo mjet sigurohet me masa parandaluese ndaj vënies së autorizuar në punë;

dh. Sa herë që punonjësit e ASHSH largohen nga vendi i tyre i punës, ata duhet të mbyllin kompjuterat e tyre, printerat, dollapët, kasafortat dhe zyrën, në të cilat janë ruajtur të dhënat personale dhe nuk duhet të lënë të dhëna të pambrojtura në tavolinë në prani të personave të cilët nuk janë të punësuar nga ana e ASHSH apo të nxjerrin jashtë zyrës, në kompjutera, laptop, flesh apo pajisje të tjera që përmbajnë të dhëna personale;

e. Të dhënat të mbrohen duke verifikuar identitetin e përdoruesit dhe duke i lejuar akses vetëm individëve të autorizuar.

ë. Punonjësit 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 ASHSH;

f. Ndalohet njohja ose çdo përpunim i të dhënave të regjistruara në dosje për një qëllim të ndryshëm nga e drejta për të hedhur të dhëna. Përfshihet nga ky rregull rasti kur të dhënat përdoren për parandalimin ose ndjekjen e një veprë penale.

g. Punonjësit ruajnë dokumentacionin e të dhënave për aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar.

gj. Niveli i sigurisë duhet të jetë i përshtatshëm me natyrën e përpunimit të të dhënave personale.

h. Respektojnë aktet e tjera ligjore dhe nënligjore që përcaktojnë se si duhet të përdoren të dhënat personale.

2. Personi i autorizuar për përpunimin e të dhënave të sistemit audio-video dhe të sigurisë teknike do të jetë përgjegjësi për IT-në në institucion. Ai humbet të drejtën e aksesimit që lidhet me detyrën e mëparshme nëse ndryshon vendin e punës ose largohet nga puna.

3. Mbrojtja e të dhënave personale realizohet përveç të tjerave, edhe me marrjen e masave të sigurisë teknike, si më poshtë:

a. Nëpërmjet instalimit dhe përditësimit automatik të sistemeve të operimit të software-ve kompjuterikë dhe konfigurimin e të gjitha pajisjeve që gjenden në Server Room të Akademisë së Shkencave (Linux, Microsoft Windows Server, etc.), të sistemit antivirus dhe sistemit të dyfishtë firewall, i cili menaxhohet nëpërmjet sistemit të serverëve dhe pajisjeve network

b. Lejimin e aksesit të stafit vetëm në ato materiale që i duhen për të kryer detyrën.

c. Përdorimin e fjalëkalimeve.

ç. Specifikimin e procedurave të rikrijimit të sistemit (backup), në rast dëmtimi.

d. Ngritja e shërbimeve të centralizuara të menaxhimit të pajisjeve kompjuterike të lidhura në rrjetin LAN/WAN të ASHSH (Active Directory, File Server, DHCP-Server, Print-Server, WSUS etj.)

dh. Në rastin e njërive a projekteve që bazohen në të dhëna personale, përpunimi i tyre është pjesë e veçantë e projektit. Mbrojtja e këtyre të dhënave garantohet sipas legjislacionit në fuqi.

#### Neni 14 Mbrojtja e ambienteve

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 aparatat 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 ambiente duhet të pajisen me autorizimin përkatës;

c. Kryhet kontroll, për të parandaluar vendosjen apo përdorimin e mjeteve të përgjimit, regjistrimit a të filmimit.

ç. Ambientet e hyrjes, survejohen me kamera gjatë 24 orëve.

d. Personeli i mirëmbajtjes së sitemit apo pajisjeve të telekomunikacionit lejohet të futet në këto ambiente i shoqëruar nga personi i caktuar nga titullari vetëm kur kërkohet nga titullari ose eprori direkt.

dh. Çdo masë tjetër e përcaktuar në rregulloret e brendshme administrative të institucionit.

#### Neni 15

Në ambientet ku përpunohen të dhëna të mbrojtura (personale) lejohet të qëndrojnë:

1. Punonjësit e ASHSH nëse ata janë të punësuar në këtë ambient ose nëse prania e tyre është thelbësore për kryerjen e detyrave të punës.

2. Personeli i mirëmbajtjes së sistemit apo pajisjeve të telekomunikacionit lejohet të futet në këto ambiente i shoqëruar nga personi i caktuar nga titullari vetëm kur kërkohet nga titullari ose eprori direkt.

#### Neni 16

##### Njësia e teknologjisë së informacionit

1. Njësia e teknologjisë së informacionit (ose specialisti i ngarkuar për këtë detyrë në mungesë të një njësie të mirëfilltë apo të përcaktuar në organigramën e institucionit) duhet të zbatojë legjislacionin në fuqi për mbrojtjen e të dhënave personale, konfidencialitetit dhe komunikimit.

2. Njësia e teknologjisë së informacionit të ketë një kopje dhe një dublikatë të të gjitha të dhënave dhe software që mbahen ose ruhen në kompjuterin qëndror. Kopja dublikatë duhet të mbahet në një vend të sigurt të godinës.

#### Neni 17

Të drejtat dhe detyrimet e punonjësve të njësisë së teknologjisë së informacionit (ose specialist në mungesë të një strukture të tillë)

1. Punonjësi i njësisë së IT në ushtrimin e detyrës së tij/saj duhet të:

- a. Zbatojë legjislacionin në fuqi për mbrojtjen e të dhënave personale, konfidencialitetit të komunikimit, lirinë dhe të drejtat e njeriut.
  - b. Sigurojë burimet për përdorimin e pajisjeve elektronike dhe sistemeve elektronike me qëllim që të ndihmojë punonjësit për përmbushjen e detyrave të tyre.
  - c. Sigurojë që konfigurimi i të gjitha pajisjeve të sigurisë është një e dhënë konfidenciale vetëm për personelin teknik. I njëjti rregull vlen edhe kur staf teknik është i jashtëm.
  - d. Sigurojë që për çdo kompjuter të lidhur në internet aplikohet firewall dhe kontrollet e sigurisë së aksesit të konfigurohen në mënyrë të tillë që *asnjë aplikacion i brendshëm të mos hapë porta alternative komunikimi me internetin.*
  - dh. Ndërmarrë këshillime, që mund të përfshijnë trajnime intensive rreth rregullores dhe përdorimit të pajisjeve;
  - f. Vendosë opsionet e sistemit e kompjuterëve lokal në mënyrë që përdoruesit mos të kenë të drejta të plota mbi softweret e sigurisë e antiviruset.
  - g. Bashkëpunojë me organet kompetente për sigurimin e informacionit të nevojshëm për çështje të sigurisë kombëtare dhe në rastet e tjera të parashikuara me ligj.
2. Me qëllim sigurimin e mbarëvajtjes së funksionimit të rrjetit të internetit dhe rritjen e efikasitetit të tij, punonjësi i njësisë së teknologjisë së informacionit mund të monitorojë në përputhje me dispozitat ligjore:
- Volumin e aktivitetit në internet dhe kapacitetin e sistemit, me qëllim sigurimin e funksionimit të tij në mënyrë efikente;
  - Faqet e aksesuara dhe kohën e shpenzuar për lundrimin e tyre.

## Neni 18

### Të drejtat dhe detyrimet e punonjësve të ASHSH lidhur me shërbimet TIK

1. Punonjësit e ASHSH kanë të drejtë të përdorin shërbimin e internetit për:
  - a. Komunikim dhe informim direkt në lidhje me problemet e institucionit;
  - b. Komunikim dhe bashkëpunim për zhvillimin e tij profesional;
  - c. Kërkime, studime, standarde, këshillime, analiza e aktivitete profesionale dhe sociale të lidhura me punën dhe në përputhje me detyrat e punonjësve në administratën publike;
  - d. Çdo aktivitet zyrtar që nuk kërkon një nivel sigurie të lartë të rrjetit.
2. Punonjësit janë përgjegjës për ruajtjen e fshehtësisë së fjalëkalimeve personale (username/password) të tyre. Ata duhet të përdorin këto dhe vetëm këto fjalëkalime dhe nuk duhet ti shpërdorjnë ato.
3. Punonjësit duhet që të mbyllin llogarinë e tyre personale në përfundim të punës;
4. Punonjësit janë përgjegjës për raportimin, nëse janë në dijeni, të shkeljeve dhe rreziqeve potenciale rreth sigurisë, si dhe të aktiviteteve joetike, që shkelin udhëzimet ose kodin e praktikës së institucionit.

5. Punonjësit janë përgjegjës për sigurimin e pajisjeve që ata përdorin nga keqpërdorimi, aksesit i paautorizuar ose dëmtimi i qëllimshëm gjatë punës.

6. Punonjësit u ndalohet përdorimi i shërbimit të internetit për të:

a. Shkarkuar, përdorur dhe/ose shpërndarë:

- Materiale me përmbajtje diskriminuese (racial, kulturor, politik, gjinor apo fizik);

- Literaturë negative rreth drogave/lëndëve psikotrope etj.;

- Materiale pornografike;

- Materiale që përmbajnë shpifje;

b. Favorizuar biznesin privat përfshirë këtu reklamën, lajmërimet etj, apo për qëllime politike.

c. Dërguar jashtë institucionit, shpërndarë, kopjuar ose modifikuar skedarët (file-s) dhe të dhëna të tjera që janë konfidenciale;

ç. Shfrytëzuar identitetin e një personi tjetër, gjatë përdorimit të internetit;

d. Mbledhur fonde publike dhe/ose për aktivitete që kanë të bëjnë me marrëdhëniet me publikun, jo specifikisht të lidhura me aktivitetin shtetëror të institucionit; \

dh. Shkëmbyer mesazhe (Instant Messaging) ose bashkëbiseduar (si CHAT) për qëllime personale.

e. Transmetimi i dokumenteve ose mesazheve të klasifikuara nëpërmjet internetit është i ndaluar, përveç rasteve kur specifikohet nga Drejtoria e Sigurimit të Informacionit të Klasifikuar (DISK).

7. Punonjësit detyrohen të përdorin postën elektronike zyrtare duke zbatuar rregullat e miratuara nga Agjencia Kombëtare e Shoqërisë së Informacionit, me rregulloren për përdorimin e postës elektronike në administratën publike, version 3.0, 08/201399.

8. Të gjitha informacionet që vendosen, hartohen, dërgohen dhe/ose merren në sistemet elektronik të institucionit nga punonjësit ose jo, janë pronë e institucionit duke respektuar dispozitat e parashikuara në Ligjin nr. 35/2016 *Për të drejtat e autorit dhe të drejtat e tjera të lidhura me to.*

9. Ndalohet çdo formë diskriminimi bazuar në moshë, racë, gjini, aftësi fizike apo mendore, burimet e të ardhurave, besimi fetar apo përkatësia politike duke përdorur burimet dhe shërbimet e TIK. Përdorimi i rrjetit kompjuterik dhe postës elektronike me qëllim përulje apo diskriminimi për një nga këto arsye është i ndaluar sipas legjislacionit në fuqi.

## Neni 19

### Mbrojtja e pajisjeve elektronike

1. Pajisjet elektronike për përpunimin e të dhënave e informacioneve në ASHSH përdoren vetëm për kryerjen e detyrave të përcaktuara në rregullore.

Këto pajisje përdoren vetëm nga punonjësit të ASHSH të trajnuar më parë për përdorimin e tyre. Trajnimi i personelit që merret me përpunimin automatik të të dhënave bëhet nga njësia e teknologjisë së informacionit.

2. Punonjësit në ASHSH janë përgjegjës për sigurimin e pajisjeve që ata përdorin nga keqpërdorimi, aksesit i paautorizuar ose dëmtimi i qëllimshëm gjatë punës. Njësia e IT ose specialisti, duhet të kryejë këshillime herë pas here si dhe trajnime rreth rregullores dhe përdorimit të pajisjeve.

3. Njësia IT-së ose specialisti duhet të sigurojë që për çdo kompjuter të lidhur në internet të aplikohet fireëall dhe kontrollet e sigurisë së aksesit të konfigurohen në mënyrë të tillë që asnjë aplikacion i brendshëm të mos hapë porta alternative komunikimi me internetin, përveç atyre të lejuara.

4. Për çdo gabim apo defekt në sistemet/databaset e institucionit të ASHSH njoftohet administratori i sistemit ose specialisti i IT-së, i cili mbi bazën e kërkesës bën rregullimin përkatës.

#### Neni 20

##### Mbrojtja e programeve kompjuterike (software)

1. Programet për trajtimin e të dhënave dhe informacioneve të blera apo të dhuruara nga donatorë të ndryshëm menaxhohen nga njësia e IT (njësia) ose specialisti. Kur një program i destinuar për trajtimin e të dhënave të institucionit të ASHSH është krijuar me iniciativën e një punonjësi të institucionit i cili nuk është i përfshirë në zhvillimin e organizimit dhe të planifikimit të programeve, para se të përfshihet në përdorimin e programit duhet të jetë miratuar nga njësia e IT ose specialisti. Pas miratimit, njësia ose specialisti organizon instalimin e tij në pajisjet elektronike.

2. Për secilin program njësia ose specialisti mund të përcaktojë:

a. Kush mund ta fshijë, kopjojë ose ta ndryshojë atë;

b. Ku duhet të ruhet kopja e programit dhe kush është përgjegjës për mbajtjen e tij të përditësuar.

#### Neni 21

Një program i blerë nga ASHSH duhet të pajiset me një licensë që e lejon ASHSH të instalojë e të përdorë atë.

#### Neni 22

##### Fjalëkalimet

Shumë nga aplikimet dhe sistemet kompjuterike janë të mbrojtura me një fjalëkalim. Fjalëkalimet ndryshohen *çdo 6 muaj ose çdo 9 muaj*.

Disa rregulla mbi përdorimin dhe vendosjen e fjalëkalimeve:

a. Fjalëkalimi për aksesimin e burimeve të teknologjisë dhe informacionit (*psh kompjuteri, etj*) nuk duhet të ndahet me persona të tjerë brenda apo jashtë organit. Punonjësit janë përgjegjës për ruajtjen dhe mosshpërndarjen e këtij informacioni.

b. Gjatë vendosjes së fjalëkalimit duhet të vendoset një fjalë apo frazë që mund të mbahet mend lehtësisht, por jo dicka që identifikon lehtësisht. Një fjalëkalim i fortë konsiderohet ai që përmban shkronja të mëdha dhe të vogla, numra dhe karaktere pikësimi.

## Neni 23

### 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 për përditësimin e tyre. Sistemi është i ndërtuar në mënyrë të tillë që vërteton identitetin e përdoruesit. Kjo kërkon që serveri qendror 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 përditshme administrohen nga njësia e IT ose specialisti (në mungesë të një njësie) të administratës së përgjithshme të ASHSH, i cili përgjegjës për mbrojtjen e të dhënave të ruajtura dhe të administruara nga këto sisteme, 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 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 vetjake.
4. 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 24

### Mbrojtja e dokumentave

Dokumentat e klasifikuar dhe mjetet e tjera të komunikimit në të cilat mbahen të dhëna personale duhet të shënohen me një lloj sekretimi dhe një nivel i caktuar kofidencialiteti. Sekretimi dhe niveli i kofidencialitetit përcaktohet në përputhje me aktet normative në fuqi.

## Neni 25

### Dokumente sekrete

1. Kur krijohen dokumente që përmbajnë të dhëna që konsiderohen “shumë sekrete” ose “sekrete”, në dokumentin original përcaktohen të dhëna lidhur me numrin e kopjeve që i janë bërë dokumentit (të shkruar, printuara, vizatuara, duplikuara) dhe kujt i janë dhënë. Çdo kopje duhet të ketë numrin e vet të regjistrimit.
2. Nëqoftëse materiali i përmendur në paragrafin e mësipërm përbëhet nga disa faqe ose lidhet me dokumente të tjera ose ka pjesë të tjera përbërëse atëherë çdo faqe duhet të sigurohet nga një nivel i caktuar kofidencialiteti

ose të sigurohet që faqet dhe lidhjet të mos hiqen ose grisen pa një paralajmërim të mëparshëm.

3. Kur të dhënat konfidenciale prezantohen në një ekran ose në sisteme të tjera mediatike, niveli i fshehtësisë ose konfidencialitetit duhet të tregohet në çdo pjesë (ilustrime, piktura, vrojtime, parashikime) të prezantimit (paraqitjes).

#### Neni 26

##### Ruajtja e dokumenteve sekrete

1. Dokumentet që mbajnë të dhëna që janë “shumë sekrete” ose “sekrete” duhet të ruhen duke iu nënshtruar legjislacionit në fuqi për informacionin e klasifikuar “sekret shtetëror”.

2. Në vendet ku mbrohen dokumentet e përmendura në paragrafin e mësipërm hyjnë vetëm punonjës që krijojnë, përdorin, mbrojnë ose sigurojnë këto dokumente.

#### Neni 27

##### Asgjësimi i dokumenteve sekrete

1. Materialet përgatitore të përdorura për krijimin e dokumenteve që përmbajnë të dhëna “shumë sekrete” ose “sekrete” (matrica, llogaritje, diagrama, skica, çështje ose printime skarco) duhet të shkatërrohet nga një komision dëshmitarësh ose vëzhguesish. Mënyra që përdoret për shkatërrimin e tyre duhet të jetë e tillë që të sigurojë pa lexueshmërinë dhe të pengojë riprodhimin e përmbajtjes.

2. Komisioni i krijuar për shkatërrimin/asgjësimin e dokumenteve sekrete, mban një raport për shkatërrimin e materialit të përmendur në paragrafin e mësipërm i cili firmoset nga të gjithë anëtarët e komisionit. Ky komision përbëhet nga tre anëtarë të caktuar nga eprori i njësisë përkatëse. Procedura që përdoret për shkatërrimin e dokumenteve që përmbajnë të dhëna personale përcaktohet nga eprori përkatës.

3. E njëjta procedurë përdoret edhe për shkatërrimin e të dhënave dhe dokumenteve dhe mjeteve të tjera të komunikimit koha e përdorimit të të cilave ka mbaruar.

#### Neni 28

##### Dublikata e programeve

Dublikata e programeve me të dhëna që përdoren në rastin e fatkeqësive natyrore ose në raste të gjendjes së jashtëzakonshme ose gjendje lufte duhet të ruhen në vende që ndodhen jashtë zyrës kryesore të njësisë organizative përkatëse. 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 fatkeqësive natyrore.

#### Neni 29

## Detyrimi për të informuar

1. Nëqoftëse një dokument me të dhëna konfidenciale humbet ose zhduket, nëpunësi kompetent ka për detyrë të informojë menjëherë eprorin e tij dhe të marrë çdo masë që vlerësohet e domosdoshme për të përcaktuar rrethanat në të cilat ka humbur dokumenti si dhe për eliminimin e pasojave të dëmshme.
2. Strukturat apo punonjësit e ASHSH të cilët gjatë ushtrimit të detyrës së tyre përpunojnë të dhëna personale, detyrohen që nëpërmjet eprorit apo/dhe personit përgjegjës në institucion për ruajtjen e të dhënave personale (burimet njerëzore, koordinatori për të drejtën e informimit etj., sipas rastit), njoftojnë zyrën e komisionerit për të drejtën e informimit dhe mbrojtjen e të dhënave personale sipas parashikimeve të ligjit specifik për mbrojtjen e të dhënave personale.

## Kreu V Sanksione administrative

### Neni 30 Masat administrative

Çdo punonjës i ASHSH që shkel detyrën për të mbrojtur të dhënat personale është përgjegjës për thyerje të disiplinës, rregullave dhe detyrimeve në veprimtarinë e punës së tij. Në qoftë se veprimet e tyre nuk përbëjnë vepër penale ndaj tyre merren masa administrative dhe disiplinore sipas akteve normative në fuqi.

### Neni 31 Mbikqyrja e masave dhe procedurave mbrojtëse

Mbikëqyrja e implementimit të rregullave për mbrojtjen e të dhënave personale për respektimin 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 personat përgjegjës për mbikëqyrjen dhe mbrojtjen e të dhënave respektive.

## Kreu VI Dispozita të fundit

### Neni 32 Konfidencialiteti për përpunimin e të dhënave

1. Çdo punonjës i ASHSH që përpunon të dhëna apo vihet në dijeni me të dhënat e përpunuara nuk mund ti 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.

### Neni 33 Detyrimi për bashkëpunim

ASHSH dhe njësitë e qendrat e kërkimit të ngritura pranë saj, janë të ndërgjegjshëm për detyrimin që kanë për të bashkëpunuar me Komisionerin dhe për t'i siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave, pasi Komisioneri ka akses në sistemin e kompjuterave, në sistemet e arkivimit, që kryejnë përpunimin e të dhënave personale dhe në të gjithë dokumentacionin, që lidhet me përpunimin dhe transferimin e tyre, për ushtrimin e të drejtave dhe të detyrave që i janë ngarkuar me ligj.

### Neni 34 Detyrimi për zbatim

1. Të gjithë aktet ligjore të Komisionerit janë të detyrueshme për zbatim nga Akademia e Shkencave dhe strukturat vartëse të saj.
2. Çdo punonjës që merret me përpunimin e të dhënave personale është i ndërgjegjshëm se përpunimi i të dhënave personale në kundërshtim me kërkesat e ligjit *Për mbrojtjen e të dhënave personale* përbën kundërvajtje administrative dhe dënohet me gjobë.

### Neni 35 Përgatitja e kodeve të etikës

Kontrolluesi harton kodin e etikës në përputhje me ligjin për mbrojtjen e të dhënave personale dhe përpara miratimit dërgon atë për mendim pranë Komisionerit.

### Neni 36 Afati i ruajtjes së të dhënave

1. Të dhënat personale të personelit të ASHSH dhe të punonjësve mbi organikë ruhen sipas afateve të përcaktuara në legjislacionin për arkivat.
2. Të dhënat e dorëzuara për një aplikim pune duhet të ruhen për një afat deri në 6 (gjashtë) muaj nga data e dorëzimit të tyre në institucion.
3. Të dhënat personale të vizitorëve ruhen për një afat 2 (dy) muaj.

### Neni 37 Sanksionet



**Kjo rregullore është pjesë e rregullores së brendshme dhe mosrespektimi i kërkesave të saj përbën shkelje të disiplinës në punë dhe ndëshkohen sipas legjislacionit në fuqi.**

#### **Neni 38**

#### **Ndryshimet e plotësimet e rregullores**

- 1. Ndryshimet në këtë rregullore, për nene të veçanta, bëhen me propozim të kancelarit e miratim të Kryesisë. Rishikimi i saj, në një kapitull a me gjerë, pas miratimit, i kalon Asamblesë për ratifikim. Ndryshimet bëhen në përputhje me legjislacionin në fuqi për mbrojtjen e të dhënave personale.**
- 2. Në zbatim të saj, Kryesia a Kryetari mund të nxjerrin udhëzime për veprimtarinë e administratës për çështje të veçanta.**

#### **Neni 39**

#### **Hyrja në fuqi**

- 1. Kjo rregullore hyn në fuqi pas miratimit të saj.**
- 2. Rregullorja publikohet në faqen zyrtare të institucionit dhe u bëhet me dije të gjithë punonjësve.**

## Deklaratë konfidencialiteti

### Objekti

Kjo deklaratë i drejtohet të gjithë stafit të Akademisë së Shkencave të Shqipërisë, si dhe punonjësve të përkohshëm, vullnetarëve dhe palëve të tjera të cilët kanë akses në informacionin e mbajtur nga ASHSH.

### Qëllimi

Kjo deklaratë duhet të nënshkruhet nga të gjithë ata punonjës të cilët kanë akses në të dhënat konfidenciale të Akademisë së Shkencave. Ajo përcakton kërkesat dhe përgjegjësitë e atyre që kanë akses në informacione të tilla dhe siguron që të gjitha palët e interesuara të kuptojnë detyrimet e tyre të konfidencialitetit.

### Fusha e veprimit

Fushë veprimi i kësaj deklarate shtrihet në të gjitha të dhënat personale, sensitive dhe informacione konfidenciale që njihen gjatë punës në ASHSH. Dispozitat përkatëse zbatohen edhe pasi marrëdhënia e punës me ASHSH, ka përfunduar.

### Deklarata e konfidencialitetit

1. Me nënshkrimin e kësaj deklarate marr përsipër të mos përdor dhe të mos i transmetoj personave të paautorizuar të dhëna personale, sensitive apo informacione konfidenciale në lidhje me ASHSH ose informacione dhe të dhëna të marra gjatë ushtrimit të funksionit përkatës në këtë institucion, përveç rasteve ku autorizohem shprehimisht nga ASHSH, ose kërkohet me ligj. Unë e kuptoj se ky detyrim vlen gjatë afatit të punësimit si dhe pas përfundimit të tij.
2. Unë e kuptoj se përdorimi dhe zbulimi i të dhënave personale në lidhje me individët, trajtohet nga Ligji nr. 9987 datë 10.3.2008 *Për mbrojtjen e të dhënave personale*, i ndryshuar. Unë nuk do të përdor ose përhap asnjë të dhënë personale, sensitive që marr dijeni gjatë punës time për asnjë qëllim që bie në kundërshtim me dispozitat ligjore.
3. Unë e kuptoj se jam i/e detyruar të ruaj konfidencialitetin për të dhënat personale dhe t'i mbaj ato të sigurta, duke marrë të gjitha masat organizative dhe teknike të përshtatshme.
4. Marr përgjegjësinë e plotë që në qoftë se konstatohet që kam vepruar në kundërshtim me udhëzimet dhe dispozitat ligjore në lidhje me konfidencialitetin e të dhënave personale apo në rast të mosruajtjes së tyre, ndaj meje të merren masa të menjëhershme. Unë e kuptoj këtë veprim si një nevojë për të mbajtur standarde të larta profesionale në institucionin e Akademisë së Shkencave të Shqipërisë.
5. Unë pasi lexova dhe kuptova përmbajtjen e kësaj deklarate, me vullnetin tim të lirë nënshkruaj këtë deklaratë dhe mbaj përgjegjësi për zbatimin e saj.

Firma e të punësuarit

Emër/Mbiemër \_\_\_\_\_

Datë \_\_. \_\_. \_\_\_\_

Firma e eprorit

Emër/Mbiemër \_\_\_\_\_

Datë \_\_. \_\_. \_\_\_\_