==========

7/41-V1

Rregullore

Maj/2020

RR E G U LL O R E
PËR PRIVATËSI DHE SIGURI TË TE DHËNAVE PERSONALE STUDENTORE DHE ATYRE TË PERSONELIT

.....

PRISHTINË, Maj 2020

RR E G U LL O R E
PËR PRIVATËSI DHE SIGURI TË TE DHËNAVE PERSONALE STUDENTORE DHE ATYRE TË PERSONELIT

Mbështetur në nenin 3, nenin 4 alineja 1, nenin 5, nenin 16, si dhe nenin 17 të LIGJIT Nr. 03/L-172 PËR MBROJTJEN E TË DHËNAVE PERSONALE në Republikën e Kosovës, nenin 5, nenin 8, nenin 9, nenin 10, nenin 14, nenin 15 dhe nenin 16 të DRAFT AKTIT NËNLIGJOR PËR MASAT E SIGURISË në Republikën e Kosovës, nenin 88 të Statutit të BPrAL Kolegji UBT, Presidenti i këtij Kolegji, Prof. Dr. Edmond HAJRIZI, ë me datën **15.05. 2019**, nxjerr këtë:

RR E G U LL O R E
PËR PRIVATËSI DHE SIGURI TË TE DHËNAVE PERSONALE STUDENTORE DHE ATYRE TË PERSONELIT

I. DISPOZITA TË PËRGJITHSHME

Neni 1

Objekti i RREGULLORES PËR PRIVATËSI DHE SIGURI TË TE DHËNAVE PERSONALE STUDENTORE DHE ATYRE TË PERSONELIT **(me tej: Rregullore), është përcaktimi i procedurave organizative dhe teknike** gjatë përpunimit të te dhënave personale nga subjektet e përpunimit të te dhënave, **masave për mbrojtjen e të dhënave personale dhe sigurisë, si dhe ruajtjes dhe administrimit e dhënave personale nga** BPrAL Kolegji UBT **(me tej: "UBT-e").**

Neni 2

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 "UBT-e", në përputhje me "LIGJIN Nr. 03/L-172 PËR MBROJTJEN E TË DHËNAVE PERSONALE në Republikën e Kosovës" **(me tej: Ligji),** si dhe AKTIT NËNLIGJOR PËR MASAT E SIGURISË TË REPUBLIKËS SË KOSOVËS **(me tej: Akti).**

Përpunimi i të dhënave duhet të bëhet në përputhje me Kushtetutën, Ligjin dhe këtë Rregullore, duke respektuar të drejtat e studentëve dhe të punësuarve - si dhe te çdo subjekti tjetër.

Neni 3

Për qëllim të kësaj Rregullore, termat e mëposhtëm kanë këtë kuptim:

"Kontrollues" Për efekt të kësaj rregulloreje është: **Administrata e "UBT-e",** e cila vetëm apo së bashku me të tjerë, përcakton qëllimin dhe mënyrat e përpunimit të te dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj.

"Përpunues" Për efekt të kësaj rregulloreje është ose janë çdo departament i administratës se "UBT-e", përveç punonjësve të kontrolluesit, që përpunojnë të dhëna për vetë kontrolluesin.

"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.

"Personalitet" Person fizik i identifikuar drejtpërdrejt ose indirekt mbi bazën e cilitdo dokument mbi personalitetin.

"Shënimet e personalitetit" Shënimet që mund të ndërlidhën më personin – emri i veçantë, shenja identifikuese e personit si dhe njohurit karakteristike fizike, mentale, kulturore ose sociale identifikimi, si dhe konstatimi i cili mund të nxjerrët nda të dhënat në raport më personin.

"Shënime të ndjeshme" Shënimi mbi personin që ka të bëjë më origjinën, përkatësin nacionale, përkatësin politike, besimit fetar, gjendjen shëndetësore, jetën seksuale, si dhe të dhënat penale mbi personin.

"Përpunimi i të dhënave" Kryerja e detyrave teknike në lidhje më veprimet e udhëheqjes të te dhënave, më kusht që detyrat teknike të behën në formën e mbajtjes së të dhënave.

"Bartja e të dhënave" Mundësia e dhënies së shënimeve për një person të tretë.

"Publikimi i të dhënave" Dhënia e mundësisë për shikim të te dhënave për cilindo person.

"Shlyerja e shënimeve" Bërja e shënimeve të pakuptueshme ashtu që rivendosja e atyre të dhënave është e pamundur.

"Emërimi i të dhënave" Përgatitja e shënimeve më shenjë identifikuese më qëllim diferencimi.

"Bllokimi i të dhënave" Pajisje e shënimeve më shenjë identifikimi më qëllim të kufizimit përfundimtar të përpunimit të tij të mëtejmë ose kufizimi për një kohë të caktuar.

"Asgjësimi i të dhënave" Shkatërrimi i tërësishëm fizik i bartësit të te dhënave.

Neni 4

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 apo kanë për qëllim të formojnë pjesë të sistemit të arkivimit pranë "UBT-e".

II. PËRPUNIMI I TË DHËNAVE PERSONALE

Neni 5

Subjektet e përpunimit të te dhënave në kuadër të "UBT-e", janë përgjegjëse për sigurinë e të dhënave personale duke i mbrojtur ato nga dëmtimet aksidentale apo të paligjshme ose nga shkatërrimi ose humbja aksidentale, ndryshimi, qasja e paautorizuar dhe vënia e tyre në dispozicion të personave të paautorizuar si dhe nga çdo forme tjetër e paautorizuar e përpunimit, dhe se çdo punonjës i strukturave të **Administratës së "UBT-e**", që merret me përpunimin e të dhënave personale të subjekteve, përgjithësisht detyrohet të zbatojë kërkesat nga nenit 2 dhe nenit 5 të Ligjit, si më poshtë:

- *respektimin e parimit për përpunimin e ligjshëm të te 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, si dhe*
- *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 6

Çdo punonjës i "UBT-e", 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 te dhënave personale.

Neni 7

Çdo departament i "UBT-e", që përpunojnë të dhëna personale të subjekteve, bazohen në kriteret e përcaktuara në nenin 6 të Ligjit, dhe sidomos:

- *për përmbushjen e një detyrimi ligjor të kontrolluesit,*
- *për përmbushjen e kontratave për te cilën subjekti i te dhënave është pale kontraktuese,*
- *për kryerjen e një detyre ligjore me interes publik,*
- *për ndjekjen e interesave legjitimë të kontrolluesit 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.*

Neni 8

Përpunimi i të dhënave sensitive kryhet në përputhje me kriteret e përcaktuara me poshtë:

- *te dhënat kërkohen për sigurimin e kujdesit shëndetësor, diagnostikimit mjekësore dhe përdorimi i tyre kryhet nga personeli mjekësor i institucionit gjegjës, dhe*

- *përpunimi është i nevojshme për përmbushjen e detyrimit ligjor dhe te te drejtave specifike te kontrolluesit ne fushën e punësimit, ne përputhje me Kodin e Punës.*

III. TË DREJTAT E SUBJEKTIT TË TE DHËNAVE

Neni 9

Kërkesën për informacion mund ta bëjë:

- *vetë personi, dhe*
- *përfaqësuesi ligjor i pajisur me autorizimin përkatës.*

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

IV. SIGURIA E TË DHËNAVE PERSONALE

Neni 11

"UBT-e" dhe organet e saj të varësisë, 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.

Ata marrin këto masa të veçanta sigurie:

- *përcaktojnë funksionet ndërmjet njësive organizative dhe operatorëve për përdorimin e të dhënave,*
- *përdorimi i të dhënave bëhet me urdhër të ekzekutiveve te "UBT-e", ose personave te autorizuar nga këta,*
- *ndalojnë hyrjen e personave të paautorizuar në mjediset e kontrolluesit ose përpunuesit të te dhënave,*
- *aksesi 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,*
- *vënia në punë e pajisjeve të përpunimit të të dhënave bëhet vetëm me autorizim të përfaqësuesve te "UBT-e", dhe çdo mjet sigurohet me masa parandaluese ndaj vënies së autorizuar në punë,*
- *regjistrojnë dhe dokumentojnë modifikimet, korrigjimet, fshirjet, transmetimet, përditësimet, etj.,*
- *sa herë që punonjësit e "UBT-e", largohen nga vendi i tyre i punës, ata duhet të mbyllin kompjuterët e tyre, dollapët, kasafortat dhe zyrën, në të cilat janë ruajtur të dhënat personale,*
- *nuk duhet të largohen nga mjediset e punës kur ka të dhëna të pambrojtura në tavolinë, dhe ndodhet në prani të personave të cilët nuk janë të punësuar nga ana e "UBT-e",*
- *nuk mbajnë në monitor të dhëna personale, kur është i pranishëm një person i paautorizuar dhe sidomos në vende jo publike,*
- *nuk nxjerrin jashtë zyrës, në asnjë rast, kompjuterë, 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,*

- *të dhënat të mbrohen duke verifikuar identitetin e përdoruesit dhe duke i lejuar akses vetëm individëve të autorizuar,*
- *udhëzimet për përdorimin e kompjuterit, duhet të ruhen në mënyrë të tillë që ato të mos jenë të aksesueshme nga persona të paautorizuar,*
- *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 "UBT-se",*
- *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,*
- *në dokumente që përmbajnë të dhëna të mbrojtura, duhet të sigurojnë shkatërrimin e materialeve ndihmëse, (p.sh. provat apo shkresat, matricat, llogaritjet, diagrame dhe skica) të përdorura ose të prodhuara për krijimin e dokumentit,*
- *të dhënat e dokumentuara nuk përdoren për qëllime të tjera, që nuk janë në përputhje me qëllimin e grumbullimit,*
- *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. Përjashtohet nga ky rregull rasti kur të dhënat përdoren për parandalimin ose ndjekjen e një vepre penale,*
- *ruajnë dokumentacionin e të dhënave për aq kohë sa është i nevojshëm për qëllimin, për të cilin është grumbulluar,*
- *niveli i sigurisë duhet të jetë i përshtatshëm me natyrën e përpunimit të të dhënave personale, dhe*
- *respektojnë aktet e tjera ligjore dhe nënligjore që përcaktojnë se si duhet të përdoren të dhënat personale.*
-

Neni 12

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.

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.

Në ambientet ku përpunohen të dhëna personale zbatohen këto masa sigurie:

- *ndalohet hyrja e personave të paautorizuar,*
- *personat që futen në këto ambiente duhet të pajisen me autorizimin përkatës,*
- *ambientet e hyrjes, survejohen me kamera gjatë 24 orëve,*
- *veç masave dhe sistemeve të tjera të mbrojtjes, vendosen pajisje dhe sisteme të sigurimit elektronik (sisteme sinjalizimi, telekamera, etj.),*
- *ambientet pajisen me dollap hekuri, të sigurta për mbrojtjen e dosjeve nga dëmtimi i tyre, me kasaforta e brava me çelësa, si dhe*
- *sigurohet mbikëqyrje e vazhdueshme, ditën dhe natën me roje fizike*

Neni 13

Njoftimi pranë AGJENCISË SHTETËRORE PËR MBROJTJEN E TË DHËNAVE PERSONALE (Agjencia) është i detyrueshëm, dhe ai kryhet në përputhje me Ligjin dhe aktet nënligjore.

Neni 14

Departamenti i Teknologjisë së Informacionit (DTI) duhet të ketë një kopje dhe një dublikatë të të gjitha të dhënave dhe software që mbahen ose ruhen në kompjuterin qendror. Kopja dublikatë duhet të mbahet në një vend të sigurt. DTI mban një kopje të te 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 cilat ato ruhen përcaktohen nga departamenti përkatës për çdo dokument.

Neni 15

Pajisjet elektronike për përpunimin e të dhënave dhe informacioneve në departamentet e "UBT-e", përdoren vetëm për kryerjen e detyrave të përcaktuara në Rregullore. Këto pajisje përdoren vetëm nga punonjës të "UBT-e", të trajnuar më parë për përdorimin e tyre. Trajnimi i personelit që merret me përpunimin automatik të te dhënave personale bëhet nga DTI-a, ose cilido subjekt tjetër i licencuar.

Për çdo gabim apo defekt në sistemet/data basët e institucionit të "UBT-e", njoftohet administratori i sistemit, i cili mbi bazën e kërkesës bën rregullimin përkatës.

Neni 16

Të gjitha dokumentet e përpunuara në mënyrë manuale që përmbajnë të dhëna personale duhet të mbahen të sigurta në mënyrë që të parandalohet shpalosja e paligjshme, shkatërrimi dhe humbja e tyre, në vendin e punës dhe gjatë transferimit të tyre.

Të gjitha kopjet e kërkuara mund të vihen në dispozicion vetëm me kusht që përdorimi i tyre i mëtejshëm të jetë i gjurmueshëm, nga krijimi deri në shkatërrimin e tyre.

Në rast të përpunimit të përzier elektronik dhe manual, shkresat e përkohshme duhet të kufizohen në domosdoshmëri absolute.

Personeli përgjegjës për punimin e të dhënave duhet të jetë në gjendje të përcjellë gjithsesi origjinën e printimit.

Pas skadimit të periudhës së lejuar ligjërisht për përpunimin e të dhënave, dokumentet duhet të:

- *arkivohen në rast se një detyrim i tillë ligjor ekziston, ose*
- *shkatërrohen fizikisht, në një mënyrë që e bënë të pamundur leximin e tyre.*

Duhet të ketë mjete të mjaftueshme dhe të arritshme teknike për shkatërrimin e dokumenteve në kopje fizike, grirëse letre të poseduara nga subjekti ose shërbimi i jashtëm i kontraktuar.

Shportat e mbeturinave duhet të kontrollohen rregullisht nëse ato përmbajnë dokumente të pa shkatërruara.
Në rast të rreziqeve shtesë, duhet të ketë kontrolle shtesë për të siguruar se dokumentet në të vërtetë janë shkatërruar fizikisht në mënyrë të parevokueshme, në rast se shkatërrimi i tillë urdhërohet.

Mjete organizative duhet të zbatohen për të verifikuar se masat e tilla mbrojtëse për trajtimin e dokumenteve në kopje fizike zbatohen në të vërtetë, nga krijimi deri në shkatërrimin e tyre, veçanërisht për të zbuluar shkelësit e masave të sigurisë.

Neni 17.

Programet për trajtimin e të dhënave dhe informacioneve të blera apo të dhuruara nga donatorë të ndryshëm, menaxhohen nga DTI. Kur një program i destinuar për trajtimin e të dhënave të institucionit të "UBT-e", është krijuar me iniciativën e një punonjësi të "UBT-e", 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 DTI. Pas miratimit, DTI organizon instalimin e tij në pajisjet elektronike.

Neni 18

Shumë nga aplikimet dhe sistemet kompjuterike janë të mbrojtura me një fjalëkalim. Për arsye sigurie, këto fjalëkalime herë pas here duhet të ndryshohen *(çdo 3 muaj ose çdo 6 muaj)*.

Disa rregulla mbi përdorimin dhe vendosjen e fjalëkalimeve:

- *fjalëkalimi për aksesimin e burimeve te teknologjisë dhe informacionit (p.sh. kompjuteri, etj.) nuk duhet të ndahet me persona të tjerë brenda apo jashtë organit. Punonjësit janë përgjegjës për ruajtjen dhe mos shpërndarjen e këtij informacioni, dhe*
- *gjatë vendosjes së fjalëkalimit, duhet të vendoset një fjalë apo frazë që mund të mbahet mend lehtësisht, por jo diçka që identifikon lehtësisht, si psh: emri apo adresa. Këshillohet të përdorni një fjalëkalim të fortë. Një fjalëkalim i fortë konsiderohet ai që përmban shkronja të mëdha dhe të vogla, numra dhe karaktere pikësimi.*

Neni 19

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. 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.

Përdoruesit duhet të njihen me llojin e të dhënave në regjistrimet e përditshme dhe kohën e ruajtjes së këtyre regjistrimeve.

Regjistrimet e përditshme administrohen nga njësi organizative të administratës së përgjithshme të "UBT-e", 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 te 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.

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 20

Dokumentet 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 konfidencialiteti.

Sekretimi dhe niveli i kofidencialitetit përcaktohet në përputhje me aktet normative në fuqi.

Neni 21

Kur krijohen dokumente që përmbajnë të dhëna që konsiderohen **"shumë sekrete"** ose **"sekrete",** në dokumentin origjinal 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.

Në qoftë se 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.

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 22

Dokumentet që mbajnë të dhëna që janë *"shumë sekrete"* ose *"sekrete"* duhet të kyçen në njësi prej hekuri teknikisht të sigurta, ose të mblidhen në një pllakë hekuri të kyçur dhe sigluar e siguruar nga një kod, megjithëse ato janë drejtpërdrejtë të kontrolluara nga një punonjës që i nevojiten dokumente përkatëse (të caktuara) për punën e tij.

Çelësat e këtyre njësive duhet të mbrohen nga nëpunësit në kontakt të ngushtë fizik, në vendet e tyre ose në zarfe të vulosura nga zyra kryesore. Çelësa të tjerë duhet të mbahen nga zyra

kryesore e drejtuesit të njësisë organizative përkatëse. Në qoftë se një çelës humbet, kyçi duhet të ndryshohet.

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

Neni 23

Materialet përgatitore të përdorura për krijimin e dokumenteve që përmbajnë të dhëna "shume sekrete" ose "sekrete" *(matrica, llogaritje, diagrami, skica, çështje ose printime skerco)* 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 lejueshmërinë dhe të pengojë riprodhimin e përmbajtjes.

Komisioni i vëzhguesve mban një raport për shkatërrimin e materialit të përmendur në paragrafin e mësipërm i cili firmoset nga të gjithë anëtarët e komisionit. Komisioni i vëzhguesve 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.

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

Neni 24

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 ose lokale 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 25

Në qoftë se një dokument me të dhëna konfidenciale humbet ose zhduket, nëpunësi kompetent ka për detyrë të informojë menjëherë eprorin e tij dhe te 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.

V. ANALIZA DHE VLERËSIMI I THJESHTËSUAR I RREZIKUT

Neni 26

Analiza e rrezikut duhet të identifikojë kërcënimet që prekin pjesë individuale të sistemit të dosjeve, të cilat çojnë në cenueshmeri dhe që mund të materializohen me shkelje të sigurisë së përpunimit të te dhënave.

Rezultati i analizës së rrezikut duhet të rezultojë në një vlerësim që përmban:

- *listën e kërcënimeve dhe cënueshmërisë të cilat mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale që përpunohen dhe sistemin e përdorur për atë përpunim, dhe*
- *listën e atyre kërcënimeve dhe cënueshmërisë që mund të materializohen me dëmtim të vërtetë të të dhënave dhe sistemit të përpunimit të tyre.*

Këtu përfshihen ato të cilat:

- *vlerësohen që me gjasë mund të ndodhin, dhe*
- *kostoja e masave për parandalimin e paraqitjes së tyre janë të përballueshme për subjektin ekonomik "UBT-e".*

Analiza e rrezikut duhet të kryhet periodikisht, së paku një (1) herë në vit, dhe duhet të dokumentohet në gjuhën që zakonisht përdoret në praktikën e biznesit të "UBT-e".

VI. POLITIKA PËR SIGURINË E INFORMACIONIT

Neni 27.

Politika për Sigurinë e Informacionit **(shkurt: PSI-ja),** specifikon objektivat themelore të sigurisë që duhet të arrihen për mbrojtjen e sistemit të dosjeve të të dhënave personale kundër shkeljes së sigurisë së tij.

Në mënyrë të veçantë ai duhet të:

- *përshkruajë sistemin e dosjeve dhe lidhjen e tij me shkeljet e mundshme të sigurisë,*
- *specifikojë objektivat e sigurisë themelore dhe masat minimale të kërkuara për siguri,*
- *specifikojë masat teknike, organizative dhe të lidhura me personelin për mbrojtjen e të dhënave personale në sistemin e dosjeve dhe mënyrën e përdorimit të tyre, si dhe*
- *përcaktojë kufijtë duke përcaktuar rreziqet e mbetura.*

Politika mbi sigurinë duhet të përmbajë deklaratën e angazhimit të "UBT-e", për të mirëmbajtur nivelin e duhur të sigurisë, si dhe udhëzimet mbi drejtimet kryesore dhe mjetet e caktuara teknike dhe organizative që do të përdoren për të arritur këtë qëllim.

Ky dokument i politikave duhet të vihet në dispozicion për të gjithë personat përgjegjës për mbrojtjen e sigurisë, duke përfshirë personelin e vetë subjektit dhe palëve të treta të kontraktuara si përpunues të te dhënave.

Përshkrimet e hollësishme të politikave të veçanta, të cilat përbëjnë sistemin e sigurisë, duhet të :

- *udhëzojë mbi udhëzimet dhe procedurat e veçanta duke ndjekur serinë e standardeve ISO-27000, dhe*
- *të vihen në dispozicion sipas "nevojës për njohuri" të atyre që janë përgjegjës për ekzekutimin dhe mbikëqyrjen e tyre.*

PSI-ja duhet të hartohet, zbatohet dhe mirëmbahet në përputhje me rregullat bazë te sigurisë së informacionit, të përcaktuara në aktet ligjore dhe sekondare në fuqi dhe legjislacionin e ratifikuar ndërkombëtar, i rekomanduar nga standardet e përcaktuara të sigurisë siç janë seria e ISO-27000 dhe rekomandimet e Agjencisë.

Analiza e rreziqeve dhe vlerësimi duhet të bëhet një komponentë përbërës i PSI-së.

Dokumenti i PSI-së duhet të specifikojë në mënyrë të qartë objektivat e sigurisë dhe të përcaktojë masat teknike, organizative dhe të lidhura me personelin të nevojshme për identifikimin e kërcënimeve dhe zbutjen e rreziqeve që ndikojnë në sistemet e dosjeve

PSI-ja duhet të përkufizohet në termat e mëposhtëm:

- *konfidencialiteti, duke siguruar që të dhënat janë të qasshme vetëm për personat e autorizuar, dhe integriteti, duke siguruar se të dhënat janë të sakta dhe të plota dhe ruajtjen e metodave të përpunimit,*
- *disponueshmëria, duke siguruar qasje të përdoruesve të autorizuar në të dhënat dhe të sistemet e përpunimit, dhe*
- *përgjegjshmëria e sistemeve të përdorura të për përpunimin e të dhënave dhe të personelit që operon me to, duke garantuar se çdo aktivitet / operacion i tyre në të dhëna është i gjurmueshëm dhe i audituesshëm.*

Gjatë zbatimit të dispozitave të këtij neni, pikat në vijim duhet të adresohen veçanërisht nga PSI-ja:

- *përpunimi i të dhënave të ndjeshme,*
- *përformanca aktuale e menaxhimit të drejtave të qasjes ,*
- *rreziqet që vijnë nga qasja në rrjetet publike, veçanërisht nga internet,*
- *menaxhimi i përpunimit portative, si dhe*
- *menaxhimi i të gjitha llojeve të qasjes nga largësia.*

VII. SANKSIONE ADMINISTRATIVE

Neni 28

Çdo punonjës i "UBT", qe 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 29

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.

VIII. DISPOZITA TË FUNDIT

Neni 30

Çdo punonjës i "UBT-e", 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.

Çdo person që vepron nën autoritetin e kontrolluesit, nuk duhet t'i përpunojë të dhënat personale, tek të cilat ka akses, pa autorizimin paraprak te kontrolluesit, përveçse kur për këtë gjë është i detyruar me ligj.

Neni 31

"UBT-e", është e ndërgjegjshme për detyrimet që ka për të bashkëpunuar me Komisionarët dhe për ti siguruar të gjithë informacionin që ai kërkon për përmbushjen e detyrave, pasi Komisionari ka akses në sistemin e kompjuterëve, 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 32

Të gjithë aktet ligjore të Komisionarit janë të detyrueshme për zbatim nga "UBT-e", dhe strukturat vartëse të saj.

Çdo punonjës i "UBT-e", që merret me përpunimin e të dhënave personale është i ndërgjegjshëm se përpunimi i të dhënave personale në kundërshtim me kërkesat e Ligjit, përbën kundërvajtje administrative dhe dënohet me gjobë.

Neni 33.

"UBT-e" është e obliguar qe me se voni brenda dy (2) muajve llogaritur nga dita e hyrjes ne fuqi të kësaj Rregulloreje, të miratoj EVIDENCËN E AKTIVITETEVE PËR PËRPUNIMIN E TË DHËNAVE PERSONALE.

Neni 34

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.

PRISHTINË,
Datë, 15.05.2019 viti

BPrAL Kolegji UBT
Presidenti
Prof. Dr. Edmond HAJRIZI,

_____