Republika e Kosovës
Republika Kosova-Republik of Kosovo
Komuna e Vushtrrisë
Opština Vučitrn – Municipality of Vushtrri

02.Nr.652/25 Datë 02.06.2025

RREGULLA
TË BRENDSHME PËR MASAT TEKNIKE DHE ORGANIZATIVE PËR MBROJTJEN E TË DHËNAVE PERSONALE NË KOMUNËN E VUSHTRRISË

Qershor, 2025

Bazuar në nenin 58 të Ligjit për Vetëqeverisjen Lokale nr. 03/L-040, nenin 40 të Ligjit Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale dhe nenin 43 të Statutit të Komunës, Kryetari i Komunës më datën **02.06.2025** aprovon këto:

Rregulla
të Brendshme për Masat Teknike dhe Organizative për Mbrojtjen e të Dhënave Personale në Komunën e Vushtrrisë

KAPITULLI I
DISPOZITAT E PËRGJITSHME

Neni 1
Qëllimi

1. Këto rregulla përcaktojnë procedurat dhe masat teknike e organizative që Komuna duhet të zbatojë për të mbrojtur të dhënat personale, duke garantuar siguri të lartë gjatë përpunimit dhe ruajtjes së tyre. Masat synojnë të sigurojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave, në përputhje me standardet e larta të sigurisë dhe ligjin për mbrojtjen e të dhënave personale.

2. Qëllimi i këtyre rregullave është minimizimi i rreziqeve të lidhura me përpunimin, duke garantuar se të dhënat personale trajtohen në mënyrë të ligjshme, transparente dhe për qëllimet e përcaktuara. Gjithashtu, Komuna angazhohet për mbikëqyrjen dhe raportimin e çdo shkeljeje të të dhënave, duke krijuar një ambient të sigurt për trajtimin e tyre.

Neni 2
Fushëveprimi

1. Ky akt zbatohet për të gjitha zyrat dhe strukturat e Komunës që përpunojnë të dhënat personale të qytetarëve, përfshirë mbledhjen, ruajtjen, përpunimin, transferimin dhe fshirjen e tyre. Ai aplikohet për çdo veprim të personelit të autorizuar dhe përpunuesve të të dhënave personale që bashkëpunojnë me Komunën përmes marrëveshjeve kontraktuale.

2. Aktivitetet e përpunimit duhet të kryhen në mënyrë të sigurt, ligjore dhe transparente, duke siguruar mbrojtjen dhe sigurinë e të dhënave personale në të gjitha fazat e përpunimit dhe menaxhimit të tyre.

3. Në rastet kur të dhënat personale transferohen ndërkombëtarisht ose përpunohen nga subjekte jashtë Kosovës, përpunuesit janë të obliguar të respektojnë dispozitat e Ligjit për Mbrojtjen e të Dhënave Personale.

Neni 3
Përkufizimet

Në kuptim të këtij akti, termat e mëposhtmë do të kenë këto kuptime:

1. **Të dhëna personale** – Çdo informacion që lidhet me një person fizik të identifikueshëm ose të identifikuar ("subjekti i të dhënave"); një person fizik i identifikueshëm është ai që mund të identifikohet drejtpërdrejt ose tërthorazi, veçanërisht përmes një identifikuesi si emri, numri i identifikimit, të dhënat e vendndodhjes, një identifikues në internet, ose një ose më shumë faktorë specifikë për identitetin fizik, fiziologjik, gjenetik, mendor, ekonomik, kulturor ose social të atij personi.

2. **Të dhëna personale të ndjeshme** - të dhëna personale që zbulojnë origjinën etnike ose racore, pikëpamjet politike ose filozofike, përkatësinë fetare, anëtarësimin në sindikatë ose çdo e dhënë për gjendjen shëndetësore ose jetën seksuale, çfarëdo përfshirje në ose heqje nga evidencat penale ose të kundërvajtjeve që ruhen në pajtim me ligjin. Karakteristikat biometrike gjithashtu konsiderohen si të dhëna personale të ndjeshme, nëse këto të fundit mundësojnë identifikimin e një subjekti të të dhënave.

3. **Zyrtar për Mbrojtjen e të Dhënave Personale (ZMDP)** – është personi përgjegjës për të siguruar pajtueshmërinë me ligjet për mbrojtjen e të dhënave personale dhe për trajtimin e duhur të këtyre të dhënave. I emëruar nga kontrolluesi dhe përpunuesi, ZMDP monitoron përpunimin e të dhënave personale, këshillon për detyrimet ligjore të mbrojtjes së të dhënave dhe vepron si pikë kontakti midis Komunës dhe autoritetit mbikëqyrës. Zyrtari caktohet mbi bazën e njohurive profesionale në ligjin dhe praktikat e mbrojtjes së të dhënave dhe duhet të jetë lehtësisht i qasshëm për të gjitha nivelet organizative, duke siguruar përpunimin ligjor dhe të sigurt të të dhënave personale.

4. **Përpunimi i të dhënave personale** – Çdo veprim ose grup veprimesh që kryhen mbi të dhënat personale, me mjete automatike ose joautomatike si: mbledhja, regjistrimi, organizimi, strukturimi, ruajtja, përshtatja ose ndryshimi, tërheqja, këshillimi, përdorimi, zbulimi me anë të transmetimit, përhapjes ose ndryshe vënies në dispozicion, renditja ose kombinimi, kufizimi, fshirja ose shkatërrimi.

5. **Kontrolluesi** – Personi fizik ose juridik, nga sektori publik apo privat që përcakton qëllimet dhe mjetet e përpunimit të të dhënave personale.

6. **Përpunuesi** – Personi fizik ose juridik, nga sektori publik apo privat që përpunon të dhënat personale në emër të kontrolluesit.

7. **Subjekti i të dhënave** – Personi fizik të cilit i përkasin të dhënat personale që përpunohen dhe për të cilin janë ndërmarrë veprimet e përpunimit.

8. **Pëlqimi** – Çdo deklaratë e lirë, specifike, e informuar dhe e qartë e vullnetit të subjektit të të dhënave, me të cilën ai ose ajo pranon përmes një deklarate ose një veprimi të qartë pohues përpunimin e të dhënave personale që kanë të bëjnë me të.

9. **Shkelje e të dhënave personale (Data Breach)** – Një shkelje e masave të sigurisë që çon në shkatërrimin e paautorizuar, humbjen, ndryshimin, ose zbulimin e paautorizuar të të dhënave personale të transmetuara, ruajtura ose përpunimi ndryshe, ose qasjen e paautorizuar në to.

10. **Masat teknike dhe organizative** – Masat që kontrolluesi dhe përpunuesi duhet të ndërmarrin për të siguruar një nivel të përshtatshëm të sigurisë për të dhënat personale duke përfshirë, por pa u kufizuar në përdorimin e teknologjive të sigurisë, kontrollet e qasjes, procedurat për menaxhimin e rreziqeve dhe trajnimin e stafit.

11. **Vlerësimi i Ndikimit mbi Mbrojtjen e të Dhënave (VNMD)** – Procesi i vlerësimit sistematik të veprimtarive të përpunimit të të dhënave personale për të identifikuar dhe menaxhuar rreziqet e mundshme për të drejtat dhe liritë e subjekteve të të dhënave.

Neni 4
Zbatimi

1. Dispozitat e këtij akti zbatohen për të gjitha drejtoritë dhe zyrat e Komunës, duke përfshirë edhe institucionet arsimore dhe shëndetësore që përpunojnë të dhënat personale të qytetarëve, duke përfshirë mbledhjen, ruajtjen, përpunimin, transferimin dhe shkatërrimin e këtyre të dhënave.

2. Ky akt zbatohet gjithashtu edhe gjatë përpunimit të të dhënave personale nga përpunuesit e jashtëm të të dhënave, të kontraktuar nga Komuna, për të siguruar që çdo përpunim i të dhënave personale të kryhet në përputhje me masat teknike dhe organizative të përcaktuara në këtë akt.

3. Të gjithë përpunuesit e të dhënave personale, qoftë të brendshëm apo të jashtëm, përveç se janë të detyruar, duhet t'i respektojnë standardet dhe masat e përcaktuara në këtë akt për të ofruar sigurinë, konfidencialitetin dhe integritetin e të dhënave personale.

KAPITULLI II

TË DREJTAT E SUBJEKTIT TË TË DHËNAVE PERSONALE

Neni 5
Marrja e Pëlqimit për Përpunimin e të Dhënave Personale

1. Kriteret për Pëlqimin

   Përpunimi i të dhënave personale nga zyrtarët komunal është i ligjshëm vetëm kur subjektet e të dhënave japin pëlqimin e tyre të qartë dhe të lirë, për një ose më shumë qëllime specifike. Pëlqimi duhet të dokumentohet dhe të përfshijë:

   1.1. Qëllimin e qartë për të cilin do të përdoren të dhënat personale;

   1.2. Ndërlidhjen specifike të pëlqimit me veprimtarinë përkatëse për të cilën të dhënat janë mbledhur.

2. Kushtet për Pëlqimin

   Pëlqimi duhet të sigurohet në formë të shkruar ose me anë të mjeteve teknike që lehtësojnë dokumentimin e tij. Zyrtarët janë të obliguar të përdorin një gjuhë të qartë, të thjeshtë dhe lehtë të kuptueshme për subjektet e të dhënave. Çdo informacion mbi të dhënat që do të përpunohen, qëllimi dhe mënyra e përdorimit të tyre duhet të jetë lehtë i qasshëm për qytetarët.

3. E Drejta për Tërheqjen e Pëlqimit

   Subjektet e të dhënave kanë të drejtën të tërheqin pëlqimin e tyre në çdo kohë pa ndikuar në ligjshmërinë e përpunimit të mëparshëm bazuar në pëlqimin e dhënë. Tërheqja duhet të jetë e lehtë për t'u bërë në mënyrën e njëjtë siç është dhënë pëlqimi fillimisht dhe qytetarët duhet të njoftohen për këtë të drejtë përpara se të japin pëlqimin e tyre.

4. Vlefshmëria e Pëlqimit për Fëmijë

   Kur subjektet e të dhënave janë fëmijë, përpunimi i të dhënave personale është i ligjshëm vetëm kur fëmiu ka të paktën 16 vjet dhe ka dhënë pëlqimin e tij, ose kur pëlqimi është dhënë nga prindi apo kujdestari ligjor në përputhje me ligjin për mbrojtjen e të miturve në fushën e shërbimeve të informacionit elektronik.

Neni 6
E Drejta për Informim dhe Qasje në të Dhënat Personale

1. Çdo subjekt i të dhënave ka të drejtë të informohet në mënyrë transparente dhe të qartë për përpunimin e të dhënave të tij personale. Kjo përfshinë:

1.1. Qëllimet e përpunimit të të dhënave personale nga Komuna;

1.2. Kategoritë e të dhënave personale të përpunuara;

1.3. Marrësit ose kategoritë e marrësve, veçanërisht në rastet kur të dhënat personale transmetohen te palë të treta ose organizata ndërkombëtare;

1.4. Periudhat e ruajtjes së të dhënave personale, ose nëse kjo nuk është e mundur, kriteret e përdorura për përcaktimin e kësaj periudhe;

1.5. E drejta për të kërkuar korrigjimin ose fshirjen e të dhënave personale ose kufizimin e përpunimit të tyre nga Komuna;

1.6. E drejta për të paraqitur një ankesë në Agjencinë për Mbrojtjen e të Dhënave Personale;

1.7. Nëse të dhënat nuk janë mbledhur drejtpërdrejt nga subjekti i të dhënave, çdo informacion për burimin e të dhënave;

1.8. Nëse ka vendimmarrje të automatizuar, përfshirë profilizimin, të mbështetur në përpunimin e të dhënave personale dhe të drejtën për të marrë informacion mbi logjikën e përpunimit automatik, si dhe rëndësinë dhe pasojat e pritshme për subjektin e të dhënave.

2. Subjekti i të dhënave ka të drejtë të marrë një kopje të të dhënave të tij personale të cilat janë duke u përpunuar nga Komuna. Çdo kërkesë e mëtejshme për kopje mund të jetë e lidhur me një tarifë administrative në përputhje me rregulloret e Komunës.

3. Nëse kërkesa bëhet me mjete elektronike, informacioni do të sigurohet në një format elektronik të përdorshëm, nëse nuk kërkohet ndryshe nga subjekti i të dhënave.

Neni 7
E Drejta për Korrigjimin dhe Fshirjen e të Dhënave

1. E Drejta për Korrigjim

   Subjekti i të dhënave ka të drejtë të kërkojë që të dhënat e tij personale të korrigjohen në rast se janë të pasakta ose të paplota. Komuna është e detyruar të kryej korrigjimin pa vonesë të panevojshme pas marrjes së një kërkese nga subjekti i të dhënave. Korrigjimi mund të përfshijë përditësime ose shtesa në të dhënat personale, bazuar në informacionin e dhënë nga subjekti.

2. E Drejta për Fshirje (E Drejta për t'u Harruar)

Subjekti ka të drejtë të kërkoi që të dhënat e tij personale të fshihen nëse përpunimi i të dhënave nuk është më i nevojshëm për qëllimin për të cilin ato janë mbledhur, ose nëse:

2.1. Tërheq pëlqimin për të cilin është bazuar përpunimi;

2.2. Të dhënat janë përpunuar në mënyrë të kundërligjshme;

2.3. Subjekti kundërshton përpunimin në bazë të neneve të aplikueshme të ligjit dhe nuk ka arsye të mjaftueshme për të vazhduar përpunimin;

2.4. Të dhënat personale duhet të fshihen për të përmbushur një detyrim ligjor që i përket kontrolluesit.

3. Kufizime dhe Përjashtime

Kërkesa për fshirje nuk do të zbatohet kur përpunimi i të dhënave është i nevojshëm për:

3.1. Ushtrimin e të drejtës së lirisë së shprehjes dhe informimit;

3.2. Përmbushjen e një detyrimi ligjor;

3.3. Për qëllime arkivistike ose kërkimore në interesin publik, nëse fshirja rrezikon qëllimet e përpunimit;

3.4. Ngritjen, ushtrimin, ose mbrojtjen e pretendimeve ligjore.

4. Pas fshirjes ose kufizimit të përpunimit të të dhënave, Komuna ka detyrimin të njoftoi çdo marrës të të dhënave përkatëse në përputhje me nenet e zbatueshme, përveç kur kjo duket e pamundur ose joproporcionale. Komuna do ta njoftoi gjithashtu subjektin e të dhënave për marrësit e informuar, nëse kërkohet nga subjekti i të dhënave.

Neni 8
E Drejta për Kufizimin e Përpunimit

1. Subjekti i të dhënave ka të drejtë të kërkoi kufizimin e përpunimit të të dhënave personale në rastet kur:

1.1. Saktësia e të dhënave personale kontestohet nga subjekti i të dhënave për një afat që i mundëson kontrolluesit të verifikojë saktësinë e të dhënave personale;

1.2. Përpunimi është i paligjshëm dhe subjekti i të dhënave kundërshton fshirjen e të dhënave personale dhe në vend të saj kërkon kufizimin e përdorimit të tyre;

1.3. Kontrolluesit nuk i duhen më të dhënat personale për qëllimet e përpunimit, por këto të dhëna kërkohen nga subjekti i të dhënave për ngritjen, ushtrimin ose mbrojtjen e pretendimeve ligjore;

1.4. Subjekti i të dhënave ka kundërshtuar përpunimin në pajtim me nenin 20, paragrafin 1 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, duke pritur të verifikohen nëse arsyet legjitime të kontrolluesit kanë përparësi ndaj të drejtave të subjektit të të dhënave.

2. Nëse përpunimi kufizohet sipas paragrafit 1 të këtij neni, këto të dhëna personale, përveç ruajtjes, përpunohen vetëm me pëlqimin e subjektit të të dhënave ose për ngritjen, ushtrimin ose mbrojtjen e pretendimeve ligjore, ose për mbrojtjen e të drejtave të një personi tjetër fizik apo juridik, ose për arsye të rëndësishme publike.

3. Kontrolluesi informon subjektin përpara revokimit të kufizimit të përpunimit dhe garanton që çdo përpunim që ka ndodhur gjatë periudhës së kufizimit është në përputhje me kërkesat ligjore.

Neni 9
E Drejta për Transferimin e të Dhënave

1. Subjekti i të dhënave ka të drejtë të marrë të dhënat personale që ka ofruar vetë në një format të strukturuar, të përdorshëm e të lexueshëm nga makinat dhe të kërkoi që këto të dhëna të transmetohen te një kontrollues tjetër, pa pengesa nga kontrolluesi fillestar, kur:

1.1. Përpunimi bazohet në pëlqimin e subjektit, siç përkufizohet në nenin 5, ose bazuar në një kontratë në përputhje me nenin 6 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale;

1.2. Përpunimi bëhet me mjete automatike.

2. E drejta për transferimin e të dhënave, sipas pikës 1 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, përfshin edhe të drejtën e subjektit që të ketë të dhënat e tij të transmetuara direkt nga një kontrollues te tjetri, nëse kjo është teknikisht e mundur.

3. Zbatimi i të drejtës së transferimit të të dhënave nuk ndikon negativisht në të drejtat dhe liritë e të tjerëve dhe kufizohet nga detyrimet ligjore që kërkojnë përpunimin e të dhënave nga kontrolluesi.

4. Përfitimi i të drejtës për transferimin e të dhënave nuk prek të drejtën e subjektit për të kërkuar fshirjen e të dhënave personale, siç përcaktohet në nenin 16 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

Neni 10
Procedurat për Ushtrimin e të Drejtave të Subjektit të të Dhënave

1. Kërkesat nga Subjekti i të Dhënave

   1.1. Çdo subjekt i të dhënave ka të drejtë të paraqesë një kërkesë për ushtrimin e të drejtave të tij/saj sipas këtij akti dhe Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale. Komuna duhet të lehtësoi ushtrimin e këtyre të drejtave duke siguruar formularë të qasshëm për kërkesat dhe udhëzime të qarta për paraqitjen e tyre;

   1.2. Kërkesat për ushtrimin e të drejtave duhet të dorëzohen në formë të shkruar, përmes mjeteve elektronike ose me gojë, me kusht që identiteti i subjektit të të dhënave të vërtetohet me dokumente të përshtatshme.

2. Afatet për Përgjigje

   Komuna është e detyruar t'i përgjigjet kërkesës së subjektit të të dhënave pa vonesë të panevojshme, dhe jo më vonë se një (1) muaj nga marrja e kërkesës. Në rast të ndonjë kompleksi ose rritje të numrit të kërkesave, ky afat mund të zgjatet me dy (2) muaj të tjerë. Komuna është e detyruar të informojë subjektin e të dhënave për çdo zgjatje të afatit brenda muajit të parë dhe të japë arsyet për vonesën.

3. Refuzimi i Kërkesave

   Nëse Komuna refuzon të veproi në lidhje me kërkesën e subjektit të të dhënave, ajo duhet të njoftoi subjektin për shkaqet e refuzimit brenda një (1) muaji nga marrja e kërkesës dhe ta informoi për të drejtën për të paraqitur një ankesë tek Agjencia për Informacion dhe Privatësi ose për të ndërmarrë veprime ligjore.

4. Lehtësimi i Ushtrimit të të Drejtave

   4.1. Komuna është e detyruar të lehtësoi ushtrimin e të drejtave të subjektit të të dhënave duke siguruar që procedurat dhe formularët për kërkesat të jenë lehtësisht të qasshëm dhe të kuptueshëm, përfshirë edhe në formë elektronike.

   4.2. Komuna është e detyruar të japë çdo informacion të kërkuar sipas këtij neni pa kosto, përveç kur kërkesat janë të ripërsëritshme, në të cilin rast mund të aplikohet një tarifë administrative e arsyeshme.

KAPITULLI III
ZYRTARI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Neni 11
Caktimi i Zyrtarit për Mbrojtjen e të Dhënave Personale

1. Komuna cakton një Zyrtar për Mbrojtjen e të Dhënave Personale (ZMDP) i cili do të jetë përgjegjës për të gjitha çështjet që kanë të bëjnë me mbrojtjen e të dhënave personale, duke përfshirë monitorimin e përputhshmërisë me këtë akt dhe ligjet në fuqi.

2. ZMDP përfshihet në kohën dhe mënyrën e duhur në të gjitha vendimmarrjet dhe çështjet që lidhen me përpunimin dhe mbrojtjen e të dhënave personale në Komunë.

Neni 12
Pavarësia dhe Autoriteti i ZMDP

1. ZMDP nuk merr udhëzime nga askush lidhur me ushtrimin e detyrave të tij/saj dhe raporton drejtpërdrejtë te menaxhmenti i lartë i Komunës.

2. ZMDP nuk mund të penalizohet, pushohet nga puna, ose të ndikohet për përmbushjen e detyrave të tij/saj sipas këtij akti dhe Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

Neni 13
Konfidencialiteti i ZMDP

ZMDP është i detyruar të mbaj fshehtësi dhe konfidencialitet për të gjitha çështjet që lidhen me mbrojtjen e të dhënave personale në Komunë, përfshirë procedurat e përpunimit dhe vlerësimet e ndikimit mbi mbrojtjen e të dhënave.

Neni 14
Detyrat e Zyrtarit për Mbrojtjen e të Dhënave Personale

1. Informimi dhe Këshillimi

   ZMDP informon dhe këshillon Komunën dhe të punësuarit e saj që kryejnë përpunimin e të dhënave personale mbi detyrimet e tyre në përputhje me Ligjin nr. 06/L-082 për mbrojtjen e të dhënave personale dhe aktet nënligjore përkatëse.

2. Monitorimi i Përputhshmërisë

   ZMDP monitoron përputhshmërinë e veprimeve të përpunimit të të dhënave me ligjet dhe rregulloret në fuqi, dhe ofron këshillime për vlerësimin e ndikimit mbi mbrojtjen e të dhënave personale, duke ndjekur procedurat e referuara në Nenin 35 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

3. Pikë Kontakti për Agjencinë për Informacion dhe Privatësi

   ZMDP vepron si pikë kontakti për Agjencinë për Informacion dhe Privatësi për të gjitha çështjet që lidhen me përpunimin e të dhënave personale, përfshirë konsultimin paraprak, sipas Nenit 36 të ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, dhe bashkëpunon me Agjencinë për sigurimin e përputhshmërisë me kërkesat ligjore.

4. Zbatimi i Detyrave të Tjera

   ZMDP, sipas nevojës, merr parasysh rrezikun që përpunimi i të dhënave personale paraqet për të drejtat dhe liritë e qytetarëve, duke vlerësuar natyrën, qëllimin dhe kontekstin e përpunimit.

Neni 15
Detyrat e Zyrtarëve të Tjerë Gjatë Përpunimit të të Dhënave në Komunë

1. Përgjegjësitë e Zyrtarëve

   Çdo zyrtar brenda Komunës që është i përfshirë në përpunimin e të dhënave personale është i detyruar të ndjekë udhëzimet dhe këshillat e ZMDP në lidhje me përpunimin e të dhënave në përputhje me këtë akt dhe Ligjin për mbrojtjen e të dhënave personale.

2. Trajnimi dhe Ndërgjegjësimi

   Zyrtarët e përpunimit janë të detyruar të marrin pjesë në trajnime të rregullta të organizuara nga ZMDP, për të siguruar që janë të përditësuar me praktikat më të mira dhe detyrimet ligjore në fushën e mbrojtjes së të dhënave personale.

3. Bashkëpunimi me ZMDP

   Zyrtarët që përpunojnë të dhëna personale bashkëpunojnë plotësisht me ZMDP për çdo kërkesë, vlerësim ose monitorim që ka të bëjë me përpunimin e të dhënave dhe sigurojnë qasje të plotë në të dhënat dhe dokumentacionet përkatëse.

Neni 16
Monitorimi dhe Vlerësimi i Performancës së ZMDP

1. Raportimi i Performancës

   ZMDP raporton rregullisht te zyrtari më i lartë administrativ i Komunës për statusin e përputhshmërisë së veprimeve të përpunimit të të dhënave dhe çdo problem të identifikuar që lidhet me përpunimin e të dhënave personale.

2. Rishikimi i Procedurave të Brendshme

ZMDP është përgjegjës për rishikimin dhe përditësimin e procedurave të brendshme për përpunimin e të dhënave personale, bazuar në ndryshimet ligjore dhe rreziqet e reja që paraqiten.

Neni 17
Publikimi i Vendimeve të Komunës

Gjatë publikimit të vendimeve të marrura nga Komuna, të cilat mund të përfshijnë të dhëna personale, duhet të respektohet parimi i minimizimit të të dhënave duke ndërmarrë masa për të siguruar që të dhënat personale që nuk janë të nevojshme të mos publikohen. Vendimet që përmbajnë të dhëna personale të ndjeshme duhet të redaktohen ose anonimizohen përpara publikimit, duke hequr emrat, numrat e identifikimit, adresat dhe çdo informacion tjetër që mund t'i identifikoi individët.

Publikimi potencial i të dhënave personale duhet të bëhet vetëm nëse është absolutisht e nevojshme për të garantuar transparencë dhe respektim të ligjeve dhe rregulloreve përkatëse të Republikës së Kosovës, dhe në bazë të vlerësimit të ndikimit mbi mbrojtjen e të dhënave sipas Nenit 35 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

KAPITULLI IV
PROCEDURA PËR NJOFTIMIN E SHKELJEVE TË TË DHËNAVE PERSONALE

Neni 18
Detyrimi për Njoftim të Menjëhershëm

1. Në rastin e një shkeljeje të të dhënave personale, çdo zyrtar përgjegjës brenda Komunës është i detyruar të njoftoi Zyrtarin për Mbrojtjen e të Dhënave Personale (ZMDP), pa vonesë të panevojshme dhe jo më vonë se 24 orë pas zbulimit të shkeljes.

2. ZMDP është përgjegjës për të njoftuar Agjencinë për Informacion dhe Privatësi për çdo shkelje të të dhënave personale, jo më vonë se 72 orë pasi është informuar për shkeljen.

3. Përmbajtja e Njoftimit - Njoftimi i bërë nga ZMDP duhet të përfshijë të dhënat e mëposhtme:

   3.1. Përshkrim të natyrës së shkeljes së të dhënave, duke përfshirë kategoritë dhe numrin e përafërt të subjekteve të të dhënave të prekur dhe kategoritë me numrin e përafërt të regjistrave të të dhënave përkatëse;

   3.2. Emrin dhe kontaktet e ZMDP-së, dhe çdo kontakt tjetër ku mund të merret informacion i mëtejshëm;

3.3. Përshkrim të pasojave të mundshme të shkeljes së të dhënave personale për të drejtat dhe liritë e subjekteve;

3.4. Masat e marrura ose të propozuara për të trajtuar shkeljen, duke përfshirë masat për të zbutur efektet negative të mundshme.

4. Komunikimi me Subjektet e të Dhënave

4.1. Nëse shkelja e të dhënave personale rezulton në një rrezik të lartë për të drejtat dhe liritë e subjekteve të të dhënave, ZMDP njofton subjektet e të dhënave pa vonesë të panevojshme;

4.2. Ky komunikim duhet të përfshijë përshkrimin e qartë dhe të kuptueshëm të natyrës së shkeljes, si dhe informacionin dhe masat e përmendura në nenin 33, paragrafi 3, nën-paragrafët 3.2, 3.3 dhe 3.4 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

5. Dokumentimi i Shkeljes

ZMDP dokumenton çdo shkelje të të dhënave personale duke përfshirë faktet, pasojat dhe masat korrigjuese të ndërmarrura nga Komuna. Ky dokumentacion duhet të mbahet për të verifikuar përputhshmërinë me kërkesat ligjore dhe për t'i mundësuar Agjencisë të shqyrtoi përputhshmërinë me këtë akt dhe ligjin në fuqi.

KAPITULLI V
SIGURIMI DHE PËRPUNIMI I TË DHËNAVE PERSONALE

Neni 19
Sistemi i Mbrojtjes së të dhënave personale

1. Përgjegjësitë për Sigurinë e të Dhënave

Organet e komunës janë të detyruara të ndërmarrin të gjitha hapat e nevojshëm për të garantuar mbrojtjen e të dhënave personale gjatë çdo faze të përpunimit të tyre. Për të siguruar që të dhënat personale trajtohen në mënyrë të sigurt, masat teknike dhe organizative duhet të jenë të përshtatshme me nivelin e rrezikut dhe të përmbushin standardet më të fundit në fushën e sigurisë.

2. Masat për Integritetin dhe Disponueshmërinë e të Dhënave

Masat e sigurisë duhet të përfshijnë:

2.1. Ruajtjen e integritetit të të dhënave personale përmes kontrolleve teknike që parandalojnë ndryshimin ose manipulimin e paautorizuar të të dhënave;

2.2. Garantimin e qasjes së qëndrueshme dhe të kontrolluar në të dhënat personale, duke siguruar që ato të jenë të disponueshme vetëm për personat e autorizuar dhe në rastet e nevojshme për përmbushjen e funksioneve ligjore dhe administrative;

2.3. Masat për rikuperimin e të dhënave, në mënyrë që në rast të ndonjë incidenti teknologjik ose katastrofe të rikthehet shpejt qasja në të dhënat personale.

3. Përmirësimi dhe Vlerësimi i Masave të Sigurisë

Komuna kryen vlerësime të rregullta të efektivitetit të masave të sigurisë dhe të ndërmarrin veprime të nevojshme për të përmirësuar sigurinë e të dhënave në përputhje me rreziqet që paraqiten. Çdo masë e zbatuar duhet të përshtatet me ndryshimet në teknologji dhe me rreziqet e reja që mund të dalin.

4. Politika për Sigurinë e të Dhënave Personale

Komuna duhet të hartojnë dhe zbatojnë një Politikë për Menaxhimin e Sigurisë së të Dhënave, e cila përcakton qartë mënyrat e menaxhimit të të dhënave personale, duke përfshirë trajtimin e rreziqeve që lidhen me qasjen e paautorizuar, humbjen ose keqpërdorimin e të dhënave.

5. Rishikimi i Politikave të Sigurisë

Politikat e sigurisë duhet të rishikohen periodikisht dhe sa herë që ndodhin ndryshime në veprimtaritë e përpunimit të të dhënave. Nëse ka zhvillime të rëndësishme teknologjike ose rreziqe të reja, politika duhet të përditësohet për të garantuar mbrojtje maksimale për të dhënat personale.

Neni 20`
Menaxhimi i Rrezikut

1. Identifikimi dhe Vlerësimi i Rrezikut

Kontrolluesi është përgjegjës për përcaktimin dhe vlerësimin e rrezikut që lidhet me përpunimin e të dhënave personale, për të minimizuar kërcënimet ndaj integritetit, konfidencialitetit dhe disponueshmërisë së të dhënave. Ky proces përfshin identifikimin e rreziqeve që vijnë nga shkatërrimi aksidental ose i paligjshëm, humbja, ndryshimi ose zbulimi i paautorizuar i të dhënave personale, si dhe qasja e paautorizuar ndaj tyre. Ky vlerësim duhet të përditësohet periodikisht për të reflektuar ndryshimet në teknologji dhe rrezik.

2. Elementët Kryesorë të Menaxhimit të Rrezikut

2.1. Lista e proceseve të përpunimit të të dhënave personale për të cilat identifikohen dhe vlerësohen rreziqet. Kjo përfshin identifikimin e pajisjeve, sistemet IT, kanalet e komunikimit, dokumentet e shkruara dhe burimet njerëzore që përpunojnë të dhënat personale.

2.2. Vlerësimi i rrezikut për çdo proces përpunimi për të përcaktuar seriozitetin dhe probabilitetin e ndikimit të mundshëm mbi të drejtat dhe liritë e individëve. Rreziqet përfshijnë aksesin e paautorizuar, humbjen e të dhënave, dhe cenimin e sigurisë së të dhënave personale.

2.3. Masat për mbrojtjen e të dhënave personale që përfshijnë kontrollin e qasjes, përdorimin e pseudonimizimit dhe enenkriptimit, masat për sigurinë fizike dhe teknike të pajisjeve, si dhe proceset për testimin dhe vlerësimin periodik të masave të zbatuara.

3. Pajisjet dhe Sistemimet e Përdorura

Kontrolluesi duhet të mbajë një inventar të pajisjeve dhe sistemeve që përpunojnë të dhënat personale, duke përfshirë:

3.1. Pajisjet hardware (p.sh. serverat, laptopët, disqet e jashtëm);

3.2. Softuerët dhe sistemet operative që mbështesin përpunimin e të dhënave;

3.3. Dokumentet e shkruara dhe dosjet e tjera që përmbajnë të dhëna personale.

4. Kontrollet e Sigurisë dhe Verifikimi Periodik

Kontrolluesi duhet të kryejë verifikime të rregullta të masave teknike dhe organizative të zbatuara, për të siguruar efektivitetin e tyre në mbrojtjen e të dhënave personale. Këto kontrolle duhet të përfshijnë:

4.1. Identifikimi i burimeve të rrezikut që lidhen me proceset e përpunimit të të dhënave, duke marrë parasysh burimet e brendshme dhe të jashtme (si p.sh. administratorët e sistemeve, personeli i autorizuar, konkurrentët, sulmet e jashtme).

4.2. Vlerësimi i masave ekzistuese dhe planifikimi i masave të reja në përputhje me rreziqet e identifikuara. Ky vlerësim duhet të përfshijë zgjidhjet për minimizimin e rreziqeve (p.sh. kontrolli i qasjes, enkriptimi i të dhënave, dhe kontrollet e auditimit).

5. Vlerësimi i Ndikimit

Kur një proces përpunimi përfshin rrezik të lartë për të drejtat dhe liritë e personave fizikë, kontrolluesi duhet të kryejë një vlerësim të ndikimit mbi mbrojtjen e të dhënave, duke marrë parasysh të gjitha masat e sigurisë për të minimizuar rrezikun. Ky vlerësim përfshin:

5.1. Identifikimi i ndikimit të mundshëm në privatësinë e subjekteve të të dhënave;

5.2. Parashikimi i pasojave të mundshme në rast të mosrespektimit të masave të sigurisë;

5.3. Masat e zbutjes së rreziqeve, si përdorimi i enenkriptimit, pseudonimizimit dhe kontrollet e sigurisë.

6. Përditësimi dhe Rishikimi i Masave të Sigurisë

Kontrolluesi është i detyruar të rishikojë dhe përditësojë periodikisht masat teknike dhe organizative të sigurisë në përputhje me zhvillimet teknologjike dhe rreziqet e reja që mund të shfaqen në proceset e përpunimit të të dhënave.

7. Raportimi dhe Dokumentimi

Kontrolluesi duhet të mbajë dokumentacion të plotë mbi rreziqet e identifikuara, masat e sigurisë të zbatuara dhe rezultatet e kontrolleve të sigurisë, duke përfshirë rregullisht informacionet në rastet e inspektimit nga autoritetet e mbikëqyrjes për mbrojtjen e të dhënave personale.

Neni 21

Vlerësimi dhe Klasifikimi i Rreziqeve në Raste të Shkeljeve të të Dhënave

Nëse ndodh një shkelje e të dhënave personale, kontrolluesi është i detyruar të vlerësojë nivelin e rrezikut të shkaktuar për subjektet e të dhënave dhe të ndjekë procedurat përkatëse të njoftimit dhe dokumentimit, si më poshtë:

1. Nuk ka Rrezik

1.1. Një shkelje klasifikohet si "Nuk ka Rrezik" kur përpunimi i të dhënave personale nuk përbën asnjë rrezik për të drejtat dhe liritë e individëve. Në këtë kategori hyjnë rastet kur të dhënat personale të përpunuara nuk përfshijnë të dhëna të ndjeshme, të dhënat janë të kriptuara në mënyrë të sigurt, dhe nuk ka asnjë gjasë që shkelja të ndikojë negativisht mbi privatësinë, identitetin apo sigurinë e subjekteve të të dhënave. Në rastet kur nuk ka rrezik për subjektet e të dhënave, nuk është e nevojshme të njoftohet autoriteti mbikëqyrës ose subjektet e të dhënave;

1.2. Gjithsesi, edhe kur një shkelje nuk përbën rrezik, ajo duhet të dokumentohet në mënyrë të detajuar nga kontrolluesi dhe të ruhet për qëllime të auditimit dhe përputhshmërisë me masat e sigurisë së të dhënave. Kjo dokumentacion përfshin përshkrimin e shkeljes, veprimet e ndërmarra për zbutjen e saj, dhe arsyet për të cilat është vlerësuar se nuk ka pasur rrezik për subjektet e të dhënave;

1.3. Shembuj të një shkeljeje që nuk ka rrezik përfshijnë humbjen ose dëmtimin e të dhënave të kriptuara që nuk mund të dekriptohen pa një çelës të posaçëm dhe që nuk përfshijnë të dhëna të ndjeshme.

2. Rrezik i Ulët

2.1. Një shkelje konsiderohet si "Rrezik i Ulët" kur përbën një rrezik të ulët për subjektet e të dhënave personale, pa shkaktuar dëme të konsiderueshme mbi të drejtat dhe liritë e tyre. Situata të tilla përfshijnë ndikime minimale ose të përkohshme mbi individët, duke mos përfshirë të dhëna të ndjeshme ose implikime të mëdha financiare apo ligjore;

2.2. Në përputhje me Nenin 33 të Ligjit Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, në rastin e një shkeljeje që konsiderohet "rrezik i ulët," kontrolluesi është i detyruar të njoftojë Agjencinë për Mbrojtjen e të Dhënave Personale brenda 72 orëve nga momenti kur është bërë i vetëdijshëm për shkeljen, përveç kur shkelja nuk përbën një rrezik të lartë për të drejtat dhe liritë e individëve. Nëse njoftimi nuk mund të bëhet brenda këtij afati, duhet të shoqërohet me arsyet e vonesës;

2.3. Shembuj të shkeljeve që përfshijnë rrezik të ulët mund të jenë humbja e një pajisjeje që përmban të dhëna personale të kriptuara ose shkelje që nuk përfshin të dhëna të ndjeshme.

3. Rrezik i Lartë

3.1. Një shkelje klasifikohet si "Rrezik i Lartë" kur ka gjasa të ndikojë në mënyrë serioze mbi të drejtat dhe liritë e individëve, duke shkaktuar dëme të konsiderueshme si humbje financiare, rrezik për sigurinë e identitetit, apo dëmtim të privatësisë së individëve. Ky nivel rreziku zakonisht përfshin përpunimin e të dhënave të ndjeshme (si të dhëna biometrike, financiare, shëndetësore) dhe mund të rezultojë në dëme të rëndësishme ndaj subjekteve të të dhënave. Në rastet kur shkelja përbën një rrezik të lartë për të drejtat dhe liritë e individëve, kontrolluesi duhet të njoftojë jo vetëm autoritetin mbikëqyrës brenda 72 orëve, por edhe subjektet e të dhënave pa vonesë të panevojshme, sipas në përputhje me Nenin 33 të Ligjit Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale;

3.2. Shembuj të rrezikut të lartë përfshijnë shkelje që përfshijnë vjedhjen e të dhënave financiare, informacionet e llogarive bankare, të dhëna biometrike, të dhëna shëndetësore, apo informacion që mund të përdoret për vjedhje identiteti apo shantazh.

KREU VI
VLERËSIMI I NDIKIMIT MBI MBROJTJEN E TË DHËNAVE (VNMD)

Neni 22
Detyrimi për Kryerjen e VNMD

1. Në rastet kur përpunimi i të dhënave personale përbën rrezik të lartë për të drejtat dhe liritë e subjekteve të të dhënave, Komuna është e detyruar të kryejë një Vlerësim të Ndikimit mbi Mbrojtjen e të Dhënave (VNMD), përpara fillimit të përpunimit.

2. Një VNMD është i nevojshëm kur përpunimi përfshin përdorimin e teknologjisë së re, monitorimin sistematik në shkallë të gjerë, ose përpunimin e kategorive të veçanta të të dhënave, siç përkufizohet në Ligjin nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

Neni 23
Hapat e Kryerjes së VNMD

1. Përshkrimi i veprimeve të përpunimit - Komuna duhet të përshkruajë në mënyrë të detajuar veprimet e përpunimit që parashikohen të ndërmerren, duke përfshirë qëllimet e përpunimit dhe çdo interes legjitim të ndjekur nga Komuna.

2. Vlerësimi i domosdoshmërisë dhe proporcionalitetit - Komuna duhet të vlerësojë domosdoshmërinë dhe proporcionalitetin e operacioneve të përpunimit në lidhje me qëllimet e përcaktuara dhe të sigurojë që përpunimi është i kufizuar vetëm në të dhënat e nevojshme për realizimin e këtyre qëllimeve.

Neni 24
Vlerësimi i rreziqeve dhe masat për zbutjen e tyre

1. Komuna duhet të identifikojë dhe vlerësojë çdo rrezik të mundshëm për të drejtat dhe liritë e subjekteve të të dhënave, duke përfshirë rreziqet për sigurinë, privatësinë dhe përdorimin e paautorizuar të të dhënave personale.

2. Masa të zbutjes së rrezikut - VNMD duhet të përfshijë masat e propozuara për të zbutur këto rreziqe, duke përfshirë garancitë teknike dhe organizative që Komuna planifikon të zbatojë për të mbrojtur të dhënat personale.

Neni 25
Konsultimi me Zyrtarin për Mbrojtjen e të Dhënave Personale

1. Roli i Zyrtarit për Mbrojtjen e të Dhënave - Komuna është e detyruar të kërkojë këshillën dhe bashkëpunimin e Zyrtarit për Mbrojtjen e të Dhënave Personale gjatë kryerjes së VNMD për të siguruar përputhshmëri me kërkesat ligjore të Ligjit Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

2. Ndikimi i këshillës së Zyrtarit - Zyrtari për Mbrojtjen e të Dhënave siguron që masat e zbatimit të propozuara nga Komuna janë të përshtatshme për zbutjen e rreziqeve dhe përmbushjen e detyrimeve ligjore.

Neni 26
Monitorimi dhe Rishikimi i VNMD

1. Monitorimi i Masave të Zbatimit - Zyrtari për Mbrojtjen e të Dhënave Personale monitoron zbatimin e masave të identifikuara në VNMD dhe siguron që ato zbatohen në mënyrë efektive nga Komuna.

2. Rishikimi Periodik i VNMD - Komuna kryen një rishikim periodik të VNMD për të siguruar që përpunimi i të dhënave vazhdon të jetë në përputhje me masat e propozuara, veçanërisht kur ka ndonjë ndryshim të natyrës ose rrezikut të përfaqësuar nga përpunimi.

KAPITULLI VII
PËRPUNIMI I TË DHËNAVE NGA PALË TË TRETA PËRMES KONTRATËS

Neni 27
Kontraktimi i Përpunuesve të Dhënave Personale

1. Komuna mund t'i besojë përpunimin e të dhënave personale një përpunuesi të jashtëm përmes një kontrate të shkruar që përcakton qartë të drejtat dhe detyrimet reciproke midis palëve, si dhe masat dhe procedurat që duhet të ndiqen nga përpunuesi, në përputhje me këtë akt dhe ligjin në fuqi.

2. Përpunuesi i të dhënave mund të përpunojë të dhënat vetëm brenda kufijve të autorizimeve të dhëna nga Komuna dhe nuk mund të përdorë të dhënat për qëllime të tjera, përveç atyre të përcaktuara në kontratë.

3. Përpunuesi i të dhënave duhet të zbatojë masat teknike dhe organizative të përcaktuara në kontratë për të siguruar që të dhënat personale mbrohen nga çdo qasje e paautorizuar ose keqpërdorim, përfshirë enkriptimin, firewall, dhe kontrolle fizike për pajisjet ku të dhënat përpunohen dhe ruhen.

Neni 29
Mbikëqyrja e Përpunuesve të Jashtëm

Komuna është përgjegjëse për të mbikëqyrur përpunuesin e jashtëm dhe për zbatimin e masave dhe procedurave të përcaktuara në kontratë. Kjo përfshin:

1. Kontrollet periodike në lokacionet e përpunimit për të siguruar përputhshmërinë me kërkesat ligjore dhe kontraktuale, përfshirë kryerjen e vizitave në vend për të verifikuar sigurinë e pajisjeve që përpunojnë të dhënat personale.

2. Në rast të ndonjë shkeljeje të masave të sigurisë, Komuna ka të drejtë të ndërpresë kontratën pa njoftim paraprak dhe të kërkojë kthimin ose asgjësimin e të gjitha të dhënave personale të përpunuara.

Neni 30
Kthimi dhe Asgjësimi i të Dhënave Personale

1. Në rast të përfundimit të kontratës për përpunimin e të dhënave, përpunuesi i jashtëm është i detyruar t'i kthejë menjëherë të gjitha të dhënat personale Komunës, pa mbajtur kopje ose të dhëna të tjera.
2. Nëse përpunuesi i jashtëm ndalon aktivitetet e tij, ai është i detyruar të kthejë menjëherë të gjitha të dhënat personale Komunës dhe të ndalojë çdo përpunim të mëtejshëm të të dhënave.

KAPITULLI VIII
MASAT TEKNIKE PËR SIGURINË E TË DHËNAVE PERSONALE

Neni 31
Proceset e Përdorura për Sigurinë e Informacionit

Kontrolluesi duhet të përfshijë politika dhe procedura të dokumentuara për identifikimin dhe menaxhimin e rreziqeve të përpunimit të të dhënave personale në këtë nivel. Proceset duhet të përfshijnë:

1. Identifikimi i rreziqeve të lidhura me përpunimin e të dhënave dhe kategorizimi i këtyre rreziqeve.

2. Aktivitetet e ngritjes së vetëdijes për stafin që ka qasje në të dhënat personale dhe përgjegjësitë që lidhen me sigurinë e tyre.

Neni 32
Dokumentimi i Masave

Kontrolluesi është i detyruar të mbajë dokumentacion të plotë për masat teknike dhe organizative të zbatuara, përfshirë ndryshimet që bëhen për përmirësimin e sigurisë së përpunimit të të dhënave në këtë nivel të rrezikut. Ky dokumentacion duhet të përditësohet të paktën një herë në vit për të reflektuar ndryshimet teknologjike dhe rreziqet e reja që mund të lindin gjatë përpunimit.

Neni 33
Raportimi i Incidenteve

Në rast të ndonjë incidenti sigurie që përfshin përpunimin e të dhënave personale në këtë nivel, kontrolluesi është i detyruar të njoftojë autoritetet përkatëse brenda një periudhe prej 72 orësh dhe të ndjekë procedurat e parapara për menaxhimin e incidenteve.

Neni 34
Sigurimi i Pajisjes në të cilën Përpunohen të Dhënat Personale

1. Kontrolluesi është i detyruar të sigurojë që pajisjet dhe sistemet në të cilat përpunohen të dhënat personale janë të mbrojtura në përputhje me masat teknike dhe organizative të përshtatshme për të garantuar sigurinë e të dhënave personale.

   Këto masa përfshijnë:

   1.1. Aktivizimin automatik të funksioneve për mbylljen e sistemit pas periudhave të caktuara të pasivitetit, jo më të gjata se 15 minuta.

   1.2. Kufizimin e qasjes në pajisjet e informacionit përmes kërkesës për autentifikim me përdorim të mekanizmave të kontrollit të qasjes, duke përfshirë fjalëkalimet, kartat e mençura, ose autentifikimin me shumë faktorë.

   1.3. Përdorimin e firewall-it dhe mjeteve të tjera mbrojtëse për të mbrojtur rrjetin e brendshëm dhe për të kufizuar hyrjet e paautorizuara në sistemet e kontrolluesit.

   1.4. Instalimin dhe konfigurimin e rregullt të përditësimeve të sistemit operativ dhe softuerit për të parandaluar cenueshmëritë dhe rreziqet e sigurisë.

2. Në rastet kur informacioni përpunohet në pajisje portative ose jashtë ambienteve të kontrolluesit, masat për sigurinë e pajisjes përfshijnë:

   2.1. Kufizimin e qasjes në pajisjet portative përmes aktivizimit të funksioneve të autorizimit automatik dhe enkriptimit të të dhënave për të parandaluar qasjen e paautorizuar.

   2.2. Ndalimin e përdorimit të pajisjeve portative pa miratimin paraprak nga kontrolluesi, duke përfshirë mekanizmat për ndjekjen e qasjes dhe sigurinë fizike të pajisjeve në përdorim.

   2.3. Parandalimin e përdorimit të medias së lëvizshme (p.sh., USB, hard disqe të jashtëm) në sistemet kritike të informacionit, përveç rasteve kur janë të miratuara dhe monitoruara nga kontrolluesi.

3. Kontrolluesi duhet të garantojë që të dhënat e ruajtura në pajisje të mbrohen përmes masave teknike përfshirë:

   3.1. Backup i rregullt i të dhënave në pajisje të jashtme të sigurta, për të parandaluar humbjen ose dëmtimin e të dhënave në rast të cenimit të sistemit kryesor.

   3.2. Enkriptimi i të dhënave të ndjeshme, veçanërisht në rastet e transferimit të të dhënave përmes rrjetit të brendshëm ose në përdorimin e pajisjeve portative.

4. Në rastet e një përpjekjeje të pasuksesshme për hyrje të paautorizuar në sistem, kontrolluesi është i detyruar të njoftojë personelin e tij të autorizuar për reagimin dhe të zbatojë masa të menjëhershme për të parandaluar ndërhyrjet e mëtejshme.

5. Monitorimi i rregullt i sistemeve dhe pajisjeve është thelbësor për të identifikuar në kohë ndonjë incident ose rrezik të mundshëm. Kontrolluesi është përgjegjës për vlerësimin dhe testimin e masave të sigurisë së pajisjeve të tij të paktën një herë në gjashtë muaj.

Neni 35
Ndarja e Detyrimeve dhe Përgjegjësive

1. Kontrolluesi përcakton qartë detyrat e personelit të autorizuar për qasje në sistemin e informacionit që trajton të dhënat personale. Secili person i autorizuar ka të drejtë të qaset vetëm në ato të dhëna personale që janë të nevojshme për kryerjen e detyrave të tij në përputhje me Ligjin Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

2. Përfundimi i Qasjes: Kontrolluesi siguron që kur një person i autorizuar përfundon mandatin e tij ose në rastet kur detyrat e tij ndryshojnë, qasja në të dhënat personale të revokohet menjëherë.

3. Rishikimi i Qasjes së Autorizuar: Kontrolluesi është përgjegjës për verifikimin periodik të qasjes së personelit të autorizuar, duke bërë kontrolle të rregullta, të paktën çdo tre muaj, për të garantuar që qasjet janë të nevojshme dhe të justifikuara.

4. Trajnimi dhe Ndërgjegjësimi: Kontrolluesi siguron që të gjithë personat e autorizuar të trajnohen për mbrojtjen e të dhënave personale dhe për rreziqet e sigurisë që mund të paraqiten gjatë përpunimit të tyre.

Neni 36
Kontrolli i Qasjes në Sistemin e Informacionit

1. Qasja e autorizuar

   Personat e autorizuar kanë të drejtë të qasen vetëm në të dhënat personale dhe pajisjet e komunikimit të informacionit që janë të nevojshme për përmbushjen e detyrave të tyre, në përputhje me rolet dhe përgjegjësitë e tyre të punës. Kontrolluesi duhet të sigurojë që qasjet e

të gjithë personave të autorizuar të jenë në përputhje me masat e sigurisë të përcaktuara në këtë akt.

2. Mekanizmat e kontrollit të qasjes

Kontrolluesi duhet të vendosë mekanizma sigurie që bëjnë të pamundur qasjen e personave të paautorizuar në të dhënat personale dhe pajisjet e informacionit. Këto mekanizma duhet të përfshijnë kontrolle të autentifikimit me shumë faktorë (p.sh., fjalëkalime komplekse, karta inteligjente, ose metoda biometrike), në përputhje me rrezikun e identifikuar gjatë vlerësimit të ndikimit të sigurisë.

3. Rishikimi i privilegjeve të qasjes

Administratori i sistemit të informacionit i caktuar nga kontrolluesi duhet të rishikojë në mënyrë periodike qasjet e autorizuara për të siguruar që qasjet janë të justifikuara dhe në përputhje me funksionet përkatëse të personave të autorizuar. Kontrolluesi është përgjegjës për miratimin, ndryshimin ose revokimin e qasjeve, nëse është e nevojshme.

4. Regjistrimi i qasjeve (logs)

Çdo qasje në të dhënat personale duhet të regjistrohet përmes evidencave të qarta (logs), duke përfshirë identitetin e personit që ka bërë qasjen, datën, orën dhe qëllimin e qasjes. Këto regjistrime duhet të ruhen për një periudhë të përcaktuar dhe të jenë të disponueshme për rishikim në rastet e hetimeve ose incidenteve të sigurisë.

5. Shkeljet e qasjes

Në rast të përpjekjeve të pasuksesshme për të hyrë në sistemin e informacionit ose qasjeve të paautorizuara, kontrolluesi është i detyruar të veprojë menjëherë për të bllokuar qasjen dhe të njoftojë autoritetin mbikëqyrës.

Neni 37

Sigurimi i Evidencës për Çdo Qasje (Logs) dhe Parandalimi i Hyrjeve të Paautorizuara

1. Identifikimi dhe Regjistrimi i Qasjes

Kontrolluesi është i detyruar të krijojë dhe mirëmbajë një regjistër të qasjeve për çdo hyrje të autorizuar dhe të paautorizuar në sistemet që përpunojnë të dhënat personale. Ky regjistër duhet të përfshijë detaje të qarta mbi:

1.1. Emrin e përdoruesit;

1.2. Datën dhe orën e qasjes;

1.3. Aktivitetet e kryera gjatë sesionit të qasjes;

1.4. Sistemet ose pajisjet e aksesuara;

1.5. Çdo hyrje e autorizuar duhet të përfshihet automatikisht në sistemet e logs dhe të monitorohet vazhdimisht nga zyrtarët e sigurisë së të dhënave. Logs do të jenë të enkriptuara për të garantuar mbrojtjen e informacioneve sensitive.

2. Ruajtja e Evidencës

2.1. Regjistrat e qasjes duhet të ruhen për një periudhë prej të paktën pesë (5) vitesh për të siguruar gjurmueshmërinë e veprimeve dhe për të mbështetur auditimet ose hetimet e mundshme;

2.2. Evidenca e hyrjeve të paautorizuara dhe përpjekjet për qasje të paautorizuar duhet të ruhen me masat më të forta të sigurisë, duke përfshirë enkriptimin dhe aksesin e kufizuar;

3. Evidenca e Hyrjeve të Paautorizuara dhe Njoftimi

Sistemi i informacionit është i obliguar të monitorojë vazhdimisht për çdo përpjekje për qasje të paautorizuar. Në rastet kur detektohet hyrje e paautorizuar, sistemi duhet të njoftojë menjëherë zyrtarët e përgjegjës për mbrojtjen e të dhënave brenda 12 orësh. Ky njoftim duhet të përmbajë detaje mbi burimin e përpjekjes për qasje, metodën e përdorur, dhe masat parandaluese të ndërmarra për të siguruar që qasja të mos përsëritet.

4. Monitorimi dhe Kontrolli i Evidencave (Logs)

Zyrtari kompetent qe është përgjegjës për monitorimin e logs dhe për identifikimin e çdo aktiviteti të dyshimtë. Çdo hyrje e dyshimtë duhet të vlerësohet menjëherë për rrezikun që përfaqëson për sigurinë e të dhënave personale.

Logs për qasjet duhet të kontrollohen rregullisht dhe të përditësohen për t'iu përshtatur ndryshimeve teknologjike dhe rreziqeve të reja.

5. Auditimi i Sistemeve të Regjistrave

Regjistrat e mbajtura duhet të auditohet të paktën dy herë në vit për të siguruar që të gjitha hyrjet dhe të dhënat e ruajtura janë të sakta dhe në përputhje me standardet e sigurisë. Kontrolluesi është përgjegjës për përgatitjen e një raporti të rregullt mbi qasjet dhe incidentet e regjistruara në sistemin e informacionit. Ky auditim do të përfshijë kontrollin e logs për qasjet e autorizuara dhe të paautorizuara, si dhe masat parandaluese të ndërmarra për të mbrojtur të dhënat.

6. Parandalimi i Hyrjeve të Paautorizuara

Administratori i sistemit është i obliguar të ndërmarrë masa parandaluese për të minimizuar rrezikun e hyrjeve të paautorizuara, duke përfshirë:

6.1. Testime të rregullta të sistemit për të identifikuar dobësi të mundshme;

6.2. Përdorimin e firewalls dhe sistemeve të avancuara për monitorimin e rrjetit;

6.3. Pseudonimizimin dhe enkriptimin e të dhënave për të rritur nivelin e mbrojtjes.

Neni 38
Sigurimi i Mediave Portative

1. Analiza e Rrezikut dhe Zbatimi i Masave

   Kontrolluesi është i obliguar që, bazuar në analizën e rrezikut, të zbatojë masa teknike dhe organizative për të siguruar mbrojtjen e të dhënave personale të ruajtura në mediat portative (pajisje mobile, USB, hard disk të jashtëm, CD-ROM, etj.), duke përfshirë mbrojtjen ndaj vjedhjes, humbjes apo qasjes së paautorizuar.

2. Masat Teknike për Mbrojtjen e Mediave Portative

   Kontrolluesi zbaton masat teknike për mbrojtjen e mediave portative, të cilat përfshijnë:

   2.1. Enkriptimi i Pajisjeve – Mediat portative që përmbajnë të dhëna personale duhet të jenë të kriptuara për të siguruar mbrojtjen e të dhënave në rast të humbjes apo vjedhjes;

   2.2. Kopje Rezervë dhe Sinkronizim – Kontrolluesi zbaton masa për të siguruar që të dhënat të ruhen në mënyrë të rregullt duke bërë kopje rezervë dhe, nëse është e nevojshme, duke përdorur shërbime cloud të sigurta.

3. Kufizimi i Ruajtjes së të Dhënave në Pajisje të Lëvizshme

   Kontrolluesi është i obliguar të kufizojë volumin e të dhënave që ruhen në pajisje të lëvizshme, duke përjashtuar çdo të dhënë të panevojshme për funksionimin e punës. Në veçanti, kur pajisjet përdoren për udhëtime ose për mbledhje të të dhënave jashtë vendit të punës, masat e mbrojtjes duhet të përfshijnë kufizimin e qasjes dhe mbrojtjen fizike të pajisjeve.

4. Masat për Parandalimin e Vjedhjes apo Humbjes

   Kontrolluesi zbaton masa shtesë për të mbrojtur pajisjet nga vjedhja apo humbja, të tilla si:

   4.1. Shenjimi dhe Ndjekja e Pajisjeve – Pajisjet duhet të jenë të shënuara qartë dhe të kenë sisteme për ndjekjen e tyre (p.sh., gjeolokacion);

   4.2. Mbyllja Automatike e Pajisjeve – Pajisjet portative duhet të mbyllen automatikisht pas një periudhe të caktuar të mosaktivitetit për të parandaluar qasjen e paautorizuar.

5. Monitorimi dhe Evidentimi i Hyrjeve në Pajisje

   Kontrolluesi është i obliguar të regjistrojë dhe monitorojë hyrjet në pajisjet portative që përpunojnë të dhëna personale. Çdo hyrje dhe aktivitet duhet të regjistrohet automatikisht dhe të jetë e monitoruar nga zyrtarët e sigurisë së të dhënave.

6. Veprime në Rast të Vjedhjes apo Humbjes së Pajisjeve

   Në rast të humbjes apo vjedhjes së një pajisjeje që përmban të dhëna personale, kontrolluesi duhet të njoftojë menjëherë personelin përgjegjës dhe të ndërmarrë masa për të izoluar apo shkatërruar të dhënat nga distanca (p.sh., me teknologji remote wipe).

Neni 39
Menaxhimi i Mediave Portative

1. Sigurimi i Vendndodhjes së Mediave Portative: Kontrolluesi siguron që mediat portative që përpunojnë të dhëna personale të mbahen në vende të sigurta, ku qasjen e kanë vetëm personat e autorizuar dhe të përcaktuar prej tij. Këto pajisje duhet të mbrohen me masa të përshtatshme fizike dhe teknike, të cilat përfshijnë, por nuk kufizohen në:

   1.1. Kriptim të dhënave;

   1.2. Monitorim dhe logje të qasjes;

   1.3. Kontroll të rreptë të hyrjes dhe daljes.

2. Transferimi dhe Ruajtja e Mediave Portative

   Transferimi i mediave që përmbajnë të dhëna personale jashtë hapësirave të punës lejohet vetëm me autorizim paraprak nga kontrolluesi dhe duhet të bëhet përmes rrugëve të sigurta të transportit. Përdorimi i teknologjive për ruajtjen e të dhënave, si enkriptimi i të dhënave gjatë transportit, është i detyrueshëm.

3. Pastrimi dhe Shkatërrimi i Mediave Portative

   Pas transferimit të të dhënave personale nga media ose pas skadimit të periudhës së caktuar të ruajtjes, media duhet të shkatërrohet në mënyrë të tillë që të dhënat të mos jenë më të rikuperueshme. Shkatërrimi duhet të bëhet në përputhje me standardet e sigurisë që garanton fshirjen e plotë të të dhënave (p.sh., ndarje mekanike ose fshirje elektronike).

4. Proceset për Fshirjen e të Dhënave

Nëse media portative është e nevojshme të fshihet për ri-përdorim, pastrimi i të dhënave duhet të bëhet në atë mënyrë që të dhënat personale të mos jenë më të rikuperueshme. Përdorimi i metodave të fshirjes për të parandaluar ripërtëritjen e mëtejshme është i detyrueshëm, duke përfshirë:

4.1. Shkatërrim fizik të mediave ose ndarje mekanike;

4.2. Fshirje e të dhënave përmes mjeteve softuerike për pastrim të sigurt.

5. Gjurmimi dhe Dokumentimi i Shkatërrimit

Kontrolluesi është i detyruar të mbajë evidencë për shkatërrimin e mediave, duke përfshirë detaje për identifikimin e mediave, kategoritë e të dhënave personale të regjistruara dhe provat e shkatërrimit. Evidenca duhet të përmbajë detaje si:

5.1. Procesverbal për shkatërrimin e mediave;

5.2. Data dhe personi përgjegjës për shkatërrimin;

5.3. Metodat e përdorura për shkatërrimin.

6. Ruajtja e Gjurmëve të Mediave Portative

Kontrolluesi është i detyruar të mbajë gjurmë informacioni për çdo media portative dhe veprimet e kryera mbi të, për të siguruar gjurmueshmëri të plotë dhe për të mbështetur çdo hetim të mëtejshëm mbi përpunimin e të dhënave personale.

Neni 40

Përgatitja dhe Ruajtja e Vazhdueshme e Procesit të Përpunimit të të Dhënave Personale

1. Planifikimi i vazhdimësisë

Kontrolluesi është i detyruar të hartojë dhe zbatojë një plan për vazhdimësinë e përpunimit të të dhënave personale, që të sigurohet se operacionet kritike mund të rikthehen dhe të funksionojnë normalisht edhe pas ndonjë ndërprerje të papritur apo incidenti.

2. Masat mbrojtëse

Plani për vazhdimësinë e përpunimit duhet të përfshijë masa specifike për ruajtjen e integritetit, besueshmërisë dhe qasshmërisë së të dhënave personale, duke përfshirë:

2.1. Ruajtja e kopjeve rezervë të të dhënave në pajisje të sigurta dhe jashtë vendit të përpunimit të të dhënave;

2.2. Implementimi i energjisë së pandërprerë për sistemet që përpunojnë të dhëna personale;

2.3. Vlerësimi periodik dhe testimi i masave për të siguruar rikthimin e sistemit në kohë të arsyeshme.

3. Veprimet në rast incidentesh

Kontrolluesi përcakton mekanizma për raportimin dhe regjistrimin e çdo incidenti që ndikon në qasjen apo përdorimin e të dhënave personale. Çdo incident duhet të dokumentohet në mënyrë të detajuar dhe të raportohet sipas standardeve të përcaktuara nga rregulloret e përpunimit të të dhënave.

4. Parandalimi dhe përgjigjja

Për të parandaluar ndërprerjet në përpunimin e të dhënave, kontrolluesi ndërmerr masa mbrojtëse për ruajtjen e sigurisë fizike dhe teknike të sistemeve. Në rast të ndonjë incidenti, të gjitha veprimet e nevojshme për rikuperimin e operacioneve të përpunimit duhet të ndërmerren brenda një periudhe të përcaktuar nga politika e kontrolluesit.

5. Ndërgjegjësimi dhe trajnimi

Kontrolluesi siguron që personeli i autorizuar dhe përpunuesit të trajnohen për procedurat e rikuperimit të të dhënave dhe zbatimin e masave mbrojtëse gjatë situatave të papritura.

Neni 41
Kopje Rezervë dhe Rikuperimi i të Dhënave Personale

1. Strategjia e Kopjeve Rezervë Baza mbi Rrezikun

Kontrolluesi, bazuar në analizën e rrezikut, është i detyruar të kryejë kopje të rregullta rezervë të të dhënave personale për të minimizuar humbjen ose dëmtimin e padëshiruar të të dhënave. Kopjet rezervë duhet të sigurojnë që në rast incidenti, qasja dhe rikuperimi i të dhënave të jetë i mundur pa humbje të dhënash apo ndërprerje të gjatë.

2. Testimi dhe Plani i Vazhdueshmërisë së Shërbimeve

Kopjet rezervë të bëra sipas paragrafit 1 duhet të testohen rregullisht për të siguruar që funksionojnë siç duhet. Kontrolluesi duhet të hartojë një plan të vazhdueshmërisë së biznesit që përfshin të gjitha incidentet e mundshme dhe masat për rikuperimin e të dhënave në mënyrë të shpejtë.

3. Kopje Rezervë Inkrementale

Bazuar në analizën e rrezikut, kopjet rezervë duhet të përfshijnë kopje inkrementale, që ruajnë vetëm ndryshimet që kanë ndodhur që nga kopja rezervë e fundit e plotë. Këto kopje duhet të kryhen në intervale të rregullta për të minimizuar rrezikun e humbjes së të dhënave.

4. Kopjet e Plota të Sigurisë

   Përveç kopjeve inkrementale, duhet të kryhen kopje të plota të të dhënave personale të paktën një herë në muaj për të garantuar që të dhënat mund të rikuperohen në tërësi në rast incidenti.

5. Siguria Fizike dhe Kriptografike

   Kopjet rezervë duhet të ruhen në vende të sigurta fizikisht, të ndara nga serverët operacionalë. Këto kopje duhet të mbrohen me masa shtesë sigurie, përfshirë enkriptimin e të dhënave, për të parandaluar çdo qasje të paautorizuar ose manipulim.

6. Zbatimi i Masave Teknike dhe Organizative

   Kontrolluesi është i obliguar të zbatojë masa teknike dhe organizative për ruajtjen e kopjeve rezervë në serverë të posaçëm. Kopjet duhet të mbrohen me enkriptim dhe vendosja e tyre duhet të jetë në përputhje me praktikat më të mira të sigurisë për të minimizuar rreziqet e zjarrit, vjedhjes, përmbytjeve ose incidenteve të tjera fizike.

Neni 42
Arkivimi dhe Ruajtja e Të Dhënave Personale

1. Arkivimi i të Dhënave

   Kur të dhënat personale nuk janë më të nevojshme për përpunim të rregullt dhe të përditshëm, por ende nuk ka skaduar afati i ruajtjes së tyre ligjore, kontrolluesi duhet t'i arkivojë ato në mënyrë të sigurt. Nëse të dhënat e arkivuara përfshijnë kategori të veçanta të të dhënave personale, apo të dhëna që mund të shkaktojnë rrezik të madh për subjektet e të dhënave, kontrolluesi duhet të ndërmarrë masa shtesë mbrojtjeje për të parandaluar kompromet imin e tyre.

2. Procedura për Arkivimin dhe Ruajtjen

   Kontrolluesi është i detyruar të përcaktojë procedura të qarta për arkivimin dhe ruajtjen e të dhënave personale. Këto procedura duhet të përfshijnë përshkrimin e vendit të ruajtjes së materialit arkivor, qasjen e autorizuar, kushtet për qasjen dhe masat mbrojtëse që do të zbatohen për të garantuar sigurinë e të dhënave të arkivuara. Kontrolluesi është përgjegjës për përgatitjen dhe zbatimin e një dokumenti të quajtur "Lista e Periudhave të Ruajtjes", e cila specifikon periudhat e ruajtjes për çdo kategori të të dhënave personale, duke përfshirë:

2.1. Llojin e të dhënave personale;

2.2. Afatet specifike të ruajtjes për secilën kategori të të dhënave;

2.3. Arsyet e mbajtjes së të dhënave personale, bazuar në nevoja operative dhe kërkesa ligjore;

2.4. Personat përgjegjës për mbajtjen dhe administrimin e të dhënave gjatë periudhave të caktuara;

2.5. Procedurat për rishikimin dhe përditësimin periodik të këtyre periudhave.

Kjo listë duhet të përditësohet dhe të rishikohet të paktën një herë në vit për të siguruar përputhshmërinë me ligjet në fuqi dhe kërkesat operacionale.

3. Rishikimi dhe Përditësimi

Kontrolluesi është i detyruar të rishikojë dhe përditësojë dokumentin e afateve për ruajtjen e të dhënave çdo vit, për të siguruar që ruajtja e të dhënave është në përputhje me ndryshimet në ligjin përkatës dhe me rregulloret e brendshme të kontrolluesit.

4. Afatin e ruajtjes së dokumenteve, Kontrolluesi duhet ta harmonizoj me Rregulloren (MPB) Nr. 05/2020 për Ndryshimin dhe Plotësimin e Rregullores (MAP) Nr. 01/2015 për Shenjat Unike të Klasifikimit të Dokumenteve dhe Afatet e Ruajtjes së Tyre.
5.

Neni 43
Mënyra e arkivimit dhe ruajtjes së të dhënave

1. Arkivimi i të dhënave personale

Kontrolluesi është i detyruar të krijojë dhe zbatojë masa për arkivimin e të dhënave personale të cilat nuk përpunohen më për qëllime të përditshme, sipas kritereve të përcaktuara në ligjin për Administrimin e Punës në Zyrë (Nr. 04/L-184) dhe legjislacionet dhe rregulloret tjera relevante.

2. Klasifikimi i të dhënave

Kontrolluesi përcakton dhe përfshin në procedurat e arkivimit klasifikimin e të dhënave, duke i ndarë në kategori të ndjeshme dhe jo të ndjeshme, bazuar në vlerësimin e ndikimit që mund të ketë kompromentimi i të dhënave mbi subjektet e të dhënave personale.

3. Ruajtja e të dhënave në servera të dedikuar

Sipas Ligjit Nr. 04/L-184 për Administrimin e Punës në Zyrë, të dhënat personale ruhen në servera që përmbushin standardet e sigurisë së të dhënave elektronike, ku vendoset një mbrojtje shtesë për dokumentet arkivore. Për të siguruar mbrojtjen e të dhënave, është e detyrueshme të ketë një kopje (back-up) të të dhënave dhe ruajtjen fizike të të dhënave elektronike në ambiente të mbrojtura nga faktorë të jashtëm si zjarri, uji dhe ndërhyrjet e paautorizuara.

4. Dokumentacioni për periudhat e ruajtjes së të dhënave

   Kontrolluesi miraton një dokument të quajtur "Lista e Afateve për Ruajtjen e të Dhënave Personale". Ky dokument përfshin të dhëna për periudhat e ruajtjes, bazat ligjore për ruajtje, dhe informacionin mbi pronarin e të dhënave.

5. Siguria fizike dhe teknike

   Masat për sigurinë fizike dhe teknike të të dhënave përfshijnë mbrojtjen e pajisjeve IT dhe serverëve ku ruhen të dhënat personale. Kontrolluesi siguron që vetëm personat e autorizuar të kenë qasje në këto pajisje, dhe se të dhënat janë të mbrojtura nga rreziqe të tilla si vjedhja, zjarri dhe dëmtimet fizike. Në rastet e arkivimit të të dhënave elektronike, serverët duhet të përmbajnë nivele të larta të sigurisë kibernetike sipas ligjeve të Kosovës dhe standardeve ndërkombëtare.

Neni 44
Enkriptimi i të Dhënave Personale

1. Kontrolluesi, bazuar në analizën e rrezikut, dhe duke marrë parasysh natyrën, përmasën, kontekstin dhe objektivat e përpunimit të të dhënave personale, bën enkriptimin e të dhënave personale me qëllim sigurimin e konfidencialitetit, integritetit dhe besueshmërisë së të dhënave personale. Zbatohen zgjidhjet më moderne të enkriptimit teknik për të cilat sigurojnë mbrojtje të të dhënave personale nga aksesi i paautorizuar dhe modifikimi i paautorizuar, siç përcaktohet në Nenin 31 të Ligjit Nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

2. Sipas Nenit 31 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, kontrolluesi duhet të zbatojë masa të përshtatshme teknike dhe organizative, përfshirë pseudonimizimin dhe enenkriptimin e të dhënave personale. Zbatohet një nivel i sigurisë së përputhur me analizën e rrezikut për të garantuar që të dhënat të mos ekspozohen ndaj akseseve të paautorizuara.

3. Kontrolluesi zbaton vetëm algoritmet e pranuara dhe të sigurta të enkriptimit, siç janë:

   3.1. SHA-256, SHA-512 ose SHA-341 si funksion hash;

   3.2. HMAC duke përdorur SHA-256;

3.3. bcrypt, scrypt ose PBKDF2 për ruajtjen e fjalëkalimeve;

3.4. AES ose AES-CBC për kriptim simetrik;

3.5. RSA-OAEP v2.1 për kriptim asimetrik.

Gjithashtu, sigurohet mbrojtje për çelësat sekret të enkriptimit, përmes përdorimit të fjalëkalimeve të sigurta dhe masave të tjera mbrojtëse për kufizimin e aksesit, siç përcaktohet në Nenin 31 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

4. Kontrolluesi miraton procedura të brendshme për menaxhimin dhe mbrojtjen e çelësave sekret të enkriptimit dhe certifikatave, duke marrë parasysh rreziqet që lidhen me fjalëkalimet e harruara ose çelësa të kompromentuar, siç parashikohet në Nenin 31 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

5. Sipas Nenit 31 të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale, kontrolluesi siguron që procedurat e sigurisë së enkriptimit përfshijnë vlerësimin e rregullt të efektivitetit të masave teknike dhe organizative për garantimin e sigurisë gjatë përpunimit të të dhënave personale.

Neni 45
Sigurimi i Faqeve të Internetit për Kontrolluesin

1. Masat Teknike të Sigurisë për Faqet e Internetit: Kontrolluesi është i detyruar të zbatojë masa të forta teknike për të siguruar identitetin e saktë dhe integritetin e faqes së internetit të menaxhuar nga Komuna, duke parandaluar çdo sulm si "phishing" ose "farming." Masa të tilla duhet të përfshijnë:

1.1. Implementimi i Protokollit TLS (Transport Layer Security): Të gjitha faqet dhe formularët që mbledhin të dhëna personale duhet të përdorin TLS për të siguruar që të dhënat transmetohen të koduara dhe të mbrojtura nga aksesi i paautorizuar. Versioni më i fundit i TLS duhet të përdoret për të siguruar që faqja është e sigurte;

1.2. Përdorimi i HTTPS dhe Filtrimi i Trafikut: Kontrolluesi duhet të sigurojë që trafiku në faqen e tij të internetit është vetëm përmes protokollit HTTPS dhe se trafiku nga porte ose IP të paautorizuara bllokohet;

1.3. Mbrojtja e Qasjes në Aplikacione dhe Sisteme Administrative: Qasja në faqet ose aplikacionet administrative të kontrolluesit duhet të kufizohet vetëm për personat me autorizime të veçanta, dhe çdo qasje e paautorizuar duhet të regjistrohet dhe monitorohet vazhdimisht për të parandaluar keqpërdorimin.

2. Evidentimi dhe Kontrolli i Cookies

Përdorimi i cookies duhet të bëhet vetëm me pëlqimin paraprak të përdoruesit dhe cookies duhet të përdoren vetëm për funksione të nevojshme teknike ose për përmirësimin e përvojës së përdoruesit. Në asnjë rast, cookies nuk duhet të përdoren për të mbledhur të dhëna personale pa leje të qartë.

3. Parandalimi i Rreziqeve të Keqpërdorimit

Kontrolluesi duhet të ndërmarrë masa të veçanta për të parandaluar çdo lloj hyrjeje të paautorizuar ose përdorimi të gabuar të shërbimeve të faqes së internetit. Këto masa duhet të përfshijnë:

3.1. Përdorimi i Sistemeve të Sigurisë Shtesë (firewalls, DDoS protection): Përdorimi i sistemit të mbrojtjes kundër sulmeve në internet, si firewalls dhe sisteme për mbrojtjen nga DDoS, për të siguruar që faqet janë të mbrojtura nga sulmet e jashtme;

3.2. Enkriptimi i URL-ve dhe Fjalëkalimeve: Të dhënat personale që mbledhin përmes formularëve në internet duhet të jenë të enkriptuara në mënyrë që qasja në to të bëhet vetëm përmes kredencialeve të sigurta dhe autentifikimit të dyfishtë.

4. Raportimi i Rasteve të Shkeljes së Sigurisë

Në rast se ndodh një incident sigurie që përfshin shkeljen e të dhënave personale përmes faqes së internetit, kontrolluesi është i detyruar të njoftojë menjëherë personat përgjegjës dhe, nëse është e nevojshme, autoritetet kompetente për mbrojtjen e të dhënave personale. Njoftimi duhet të bëhet jo më vonë se 72 orë pas incidentit.

Neni 46

Detyrimet dhe Përgjegjësitë e Administratorit të Sistemit dhe Personave të Autorizuar për Përdorimin e Sistemit të Informacionit

1. Përcaktimi i Detyrimeve

Kontrolluesi, bazuar në një analizë të rrezikut, përcakton qartë detyrimet dhe përgjegjësitë e administratorit të sistemit të informacionit dhe personave të autorizuar për përdorimin e tij. Këto detyrime përfshijnë përdorimin e sigurt të pajisjeve dhe dokumenteve të komunikimit elektronik (TI) dhe zbatimin e masave të sigurisë të përcaktuara me rregullore.

2. Kontrolli dhe Auditimi i Sistemit

Kontrolluesi është i detyruar të kryejë kontrolle periodike mbi punën e administratorit të sistemit të informacionit. Ky auditim përfshin monitorimin e të gjithë aksesit në sistemet e brendshme dhe hartimin e raporteve për çdo parregullsi ose anomali të identifikuar gjatë kontrollit.

3. Raportimi i Parregullsive dhe Masat për Përmirësim

Në raportet e përgatitura nga kontrolli periodik, duhet të evidentohen çdo lloj parregullsie e zbuluar dhe të propozohet një plan masash për eliminimin e tyre. Ky raport duhet t'u dërgohet zyrtarëve të lartë përgjegjës për mbrojtjen e të dhënave dhe menaxhimit të IT.

4. Njoftimi i Personave të Autorizuar

Kontrolluesi duhet të njoftojë të gjithë personat e autorizuar për përdorimin e sistemit të informacionit lidhur me çdo ndryshim në politikat e sigurisë, masat teknike të ndërmarra dhe detyrimet që ata kanë për të ruajtur sigurinë e të dhënave gjatë përdorimit të sistemeve TI.

Neni 47
Menaxhimi i Incidentëve dhe Sigurimi i Vazhdueshmërisë

1. Planifikimi i Menaxhimit të Incidentëve

Kontrolluesi krijon një plan të hollësishëm për menaxhimin e incidenteve që prekin sigurinë e të dhënave personale. Ky plan përfshin parashikimin dhe identifikimin e rreziqeve, parandalimin e aksidenteve, si dhe menaxhimin e ndonjë aksesi të paautorizuar apo humbjes së të dhënave.

2. Menaxhimi dhe Raportimi i Incidentëve

Në rast incidenti që cenon konfidencialitetin ose integritetin e të dhënave, sistemi duhet të raportojë menjëherë incidentin tek autoritetet përkatëse. Njoftimi përmban detaje të qarta për ngjarjen, përfshirë kohën, natyrën e incidentit, dhe masat korrigjuese të ndërmarra.

3. Veprimet për Korrigjimin e Incidentëve

Pas zbulimit të një incidenti, kontrolluesi duhet të marrë masa të menjëhershme për të rikthyer integritetin dhe sigurinë e të dhënave, duke siguruar një raport të plotë për çdo aksion të ndërmarrë.

4. Rivendosja e Qasjes dhe Rihyrja në Sisteme

Pasi të jenë marrë masat për parandalimin e ndonjë incidenti të mëtejshëm, rivendosja e qasjes në sistem do të bëhet vetëm për personat dhe pajisjet që kanë kaluar të gjitha kontrollet e sigurisë.

5. Trajnimi i Personelit dhe Komunikimi i Incidentëve

Kontrolluesi siguron që personeli të trajnohet vazhdimisht për identifikimin e rreziqeve dhe raportimin e tyre në mënyrë të duhur. Gjithashtu, në rast incidenti, të gjithë individët përkatës duhet të njoftohen për të minimizuar rrezikun e ndonjë përhapjeje të mëtejshme të cenimit të sigurisë.

6. Masat e Vazhdueshmërisë së Operacioneve

Kontrolluesi krijon një plan për të garantuar vazhdimësinë e operacioneve gjatë dhe pas incidenteve, duke përfshirë masat për ruajtjen e të dhënave, rikthimin e sistemeve dhe rifillimin e operacioneve me ndërprerje minimale.

KAPITULLI IX
MASAT ORGANIZATIVE PËR SIGURINË E TË DHËNAVE PERSONALE

Neni 48
Siguria Fizike e Pajisjeve të të Dhënave Personale

1. Kontrolli i Qasjes në Ambientet e Serverëve

Kontrolluesi duhet të sigurojë që qasjen në ambientet ku ndodhen serverët dhe pajisjet që përpunojnë dhe ruajnë të dhënat personale ta kenë vetëm personat e autorizuar. Pajisjet dhe serverët duhet të vendosen në dhoma me qasje të kontrolluar fizikisht, duke përfshirë monitorim të vazhdueshëm, instalimin e kamerave të sigurisë, dhe përdorimin e kartave identifikuese për hyrje.

2. Sistemet e Alarmit dhe Mbikëqyrjes
Pajisjet dhe serverët duhet të jenë të mbrojtura nga ndërhyrjet fizike dhe të jenë të pajisura me sisteme alarmi që sinjalizojnë hyrje të paautorizuara ose incidente sigurie. Këto sisteme duhet të jenë të lidhura me njësi të sigurisë ose personel të autorizuar për të ndërhyrë menjëherë në rast nevoje.

3. Masat ndaj Rreziqeve të Jashtme

Kontrolluesi duhet të ndërmarrë masa për të mbrojtur pajisjet dhe serverët nga rreziqet e jashtme si zjarri, përmbytjet, pluhuri, tymi, ndikimet elektromagnetike, dhe ndërprerjet e energjisë elektrike. Përdorimi i gjeneratorëve rezervë ose UPS duhet të garantojnë furnizim të vazhdueshëm me energji për pajisjet që ruajnë të dhënat.

4. Lista e Personave të Autorizuar

Kontrolluesi është i detyruar të mbajë një listë të përditësuar të personave ose kategorive të personave që kanë të drejtë të hyjnë në ambientet ku ruhen pajisjet që përpunojnë të dhënat personale. Kjo listë duhet të përditësohet rregullisht për të siguruar që vetëm personeli i autorizuar ka akses në këto ambiente.

5. Kontrolli dhe Monitorimi i Vizitorëve

Kontrolluesi duhet të sigurojë që vizitorët që kanë nevojë të hyjnë në këto ambiente të ndjekin një proces të kontrolluar. Një person i autorizuar duhet të jetë gjithmonë prezent për të monitoruar vizitorët gjatë kohës që ata ndodhen në këto ambiente.

6. Raportimi i Incidenteve

Çdo incident sigurie që përfshin ndërhyrje fizike në pajisjet që përpunojnë të dhënat personale duhet të raportohet menjëherë tek personeli përgjegjës për mbrojtjen e të dhënave. Masat e marra pas incidentit duhet të regjistrohen dhe të rishikohen për të siguruar përmirësime të ardhshme në sigurinë fizike.

Neni 49
Njoftimi për ndryshimet në statusin e përdoruesve:

Çdo ndryshim në statusin e punësimit ose angazhimit të përdoruesve që kanë qasje në sistemet e informacionit, duke përfshirë pushimin nga puna, duhet të raportohen menjëherë për të siguruar mbylljen e qasjes së tyre dhe fshirjen e të gjitha kredencialeve përkatëse.

Neni 50
Informimi dhe edukimi për mbrojtjen e të dhënave personale

1. Punonjësit ose personat e angazhuar nga kontrolluesi

Para fillimit të detyrave të tyre, kontrolluesi është i obliguar t'i njohë me politikat për mbrojtjen e të dhënave personale, rregullat e brendshme, dhe masat teknike dhe organizative që janë në fuqi për përpunimin e të dhënave personale.

2. Detyrimet për mbrojtjen e të dhënave

Për personat e angazhuar për një periudhë të caktuar apo me kontrata, kontrolluesi siguron që në kontratën e tyre të përcaktohen qartë detyrimet dhe përgjegjësitë lidhur me mbrojtjen e të dhënave personale, në përputhje me dispozitat e ligjit në fuqi.

3. Paraqitja e detyrave për mbrojtjen e të dhënave

Kontrolluesi, përpara fillimit të detyrave të drejtpërdrejta për punonjësit apo personat e autorizuar, i informon ata për mënyrën e trajtimit të të dhënave personale dhe përgjegjësitë që ata mbajnë për të siguruar mbrojtjen e tyre, si dhe hapat që duhet të ndjekin për të shmangur shkeljet e mundshme.

4. Deklarata e konfidencialitetit

Para fillimit të punës, çdo punonjës apo person i angazhuar nga kontrolluesi duhet të nënshkruajë një deklaratë për konfidencialitetin dhe mbrojtjen e të dhënave personale, që siguron respektimin e rregullave dhe politikave në fuqi.

5. Përmbajtja e deklaratës së konfidencialitetit

Deklarata duhet të përfshijë: angazhimin për të respektuar parimet e mbrojtjes së të dhënave personale, përpunimin vetëm sipas udhëzimeve të kontrolluesit dhe ruajtjen e sigurisë së të dhënave gjatë përpunimit të tyre, në përputhje me masat e sigurisë.

6. Regjistrimi dhe ruajtja e dokumentacionit

Deklaratat e konfidencialitetit të punonjësve apo personave të angazhuar nga kontrolluesi duhet të ruhen në dosjet e tyre, duke siguruar që janë të lehta për t'u verifikuar në rast të ndonjë incidenti apo inspektimi.

7. Trajnimi i vazhdueshëm dhe informimi

Kontrolluesi është i obliguar të ofrojë trajnim dhe informim të rregullt për të gjithë personat që kanë qasje në të dhënat personale. Ky trajnim duhet të fokusohet në përgjegjësitë e tyre për mbrojtjen e të dhënave dhe mënyrën e duhur të reagimit në rast të shkeljeve apo incidenteve të sigurisë, në përputhje me ligjet në fuqi në Kosovë.

Neni 51
Rregullimi dhe Organizimi i Zyrës - Zyra e pastër

1. Zbatimi Rregullimi dhe Organizimi i Zyrës

Kontrolluesi është i detyruar të zbatojë rregullin "Zyra e pastër" gjatë përpunimit të të dhënave personale që përfshijnë dokumente fizike ose digjitale. Kjo nënkupton mbajtjen e të gjitha dokumenteve të mbrojtura nga qasja e personave të paautorizuar në çdo moment.

2. Mbyllja e dokumenteve dhe pajisjeve

Të gjitha dokumentet dhe pajisjet që përmbajnë të dhëna personale duhet të mbahen të mbyllura ose të kyçura kur nuk përdoren aktivisht, për të parandaluar qasjen e paautorizuar, siç përcaktohet në rregullat organizative dhe procedurat teknike të kontrolluesit.

3. Dokumentacioni digjital

Për dokumentet digjitale, duhet të sigurohet që ekranet të jenë të mbyllura kur punonjësit nuk janë në vendin e punës dhe çdo pajisje që përmban të dhëna personale duhet të ketë mbrojtje të kyçjes për të shmangur qasjen e paautorizuar.

Neni 52
Menaxhimi i Fjalëkalimeve për Pajisjet dhe Sistemet e Informacionit

1. Përcaktimi i Politikave të Fjalëkalimeve

   Kontrolluesi është përgjegjës për të zbatuar dhe menaxhuar politika të sigurisë së fjalëkalimeve në përputhje me masat teknike dhe organizative të përcaktuara nga ASHI, duke siguruar që të gjitha pajisjet dhe sistemet e informacionit që përpunojnë të dhëna personale të jenë të mbrojtura me fjalëkalime të forta dhe unike.

2. Kompleksiteti i Fjalëkalimeve

   Fjalëkalimet duhet të përmbajnë të paktën 12 karaktere, duke përfshirë kombinime të shkronjave të mëdha dhe të vogla, numrave, dhe simboleve speciale, duke minimizuar mundësinë e sulmeve të brendshme ose të jashtme. Për më tepër, fjalëkalimet duhet të rinovohen çdo 30 ditë.

3. Shtesa të Sigurta të Autorizimit

   Në përputhje me politikat e ASHI-së, për personat e caktuar me autorizim (p.sh., administratorët e sistemit ose përdoruesit kryesorë), shpërndarja e fjalëkalimeve duhet të realizohet në mënyrë të sigurt, duke përdorur metoda si shtesa shtesë të sigurisë (p.sh., autentikimi me dy faktorë).

4. Ndarja e Fjalëkalimeve

   Fjalëkalimet për qasje kritike në sistemet e informacionit nuk mund të ndahen në mënyrë direkte me një individ të vetëm, por duhet të menaxhohen në grup, ku vetëm një grup i caktuar personash me nivel të lartë sigurie ka qasje të kontrolluar për ndryshimin dhe përdorimin e tyre.

5. Monitorimi dhe Rishikimi i Politikave

   Kontrolluesi është përgjegjës për monitorimin dhe rishikimin e vazhdueshëm të përdorimit të fjalëkalimeve dhe aksesit, duke kryer auditime të rregullta për të siguruar përputhjen me ASHI dhe ligjet në fuqi për mbrojtjen e të dhënave personale.

Neni 53
Vërtetimi dhe Certifikimi i Procedurave për Mbrojtjen e të Dhënave Personale

1. Kontrolluesi, përpunuesit dhe subjektet e tjera që përpunojnë të dhëna personale mund të kërkojnë certifikim nga një organ i autorizuar, për të dëshmuar përputhshmërinë e masave dhe procedurave të tyre me ligjin për mbrojtjen e të dhënave personale.

2. Certifikimi jepet bazuar në një vlerësim të detajuar të masave teknike dhe organizative të implementuara për mbrojtjen e të dhënave personale, duke përfshirë edhe mekanizmat për sigurinë e përpunimit, ruajtjen dhe transferimin e të dhënave.

3. Për të marrë certifikimin, subjektet duhet të plotësojnë këto kritere minimale:

   3.1. Të demonstrojnë njohuri dhe kompetenca të mjaftueshme në fushën e mbrojtjes së të dhënave personale;

   3.2. Të kenë implementuar masa dhe procedura të sigurta për mbrojtjen e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave;

   3.3. Të përmbushin standardet ndërkombëtare për sigurinë e të dhënave.

4. Certifikata është e vlefshme për një periudhë prej tre (3) vitesh dhe mund të rinovohet pas përmbushjes së kritereve përkatëse. Certifikimi mund të tërhiqet në rast të mosrespektimit të vazhdueshëm të masave të sigurisë.

5. Certifikimi nuk zëvendëson përgjegjësinë e drejtpërdrejtë të kontrolluesit ose përpunuesit për respektimin e plotë të ligjit për mbrojtjen e të dhënave personale, por shërben si një mekanizëm vlerësimi të pavarur për të garantuar përputhshmërinë me standardet e mbrojtjes së të dhënave.

Neni 54
Mbrojtja e të Dhënat Personale në Sportel

1. Gjatë përpunimit të të dhënave personale në sportel, përpunuesi është i detyruar të sigurojë që të dhënat personale të mbledhura nga qytetarët të mos jenë të qasshme për individë të tjerë që ndodhen në të njëjtin ambient. Ky obligim përfshin:

   1.1. Fshehjen e dokumenteve personale dhe të dhënave të tjera të ndjeshme nga qytetarët e tjerë, duke përdorur masa të tilla si ekrane të fshehura, distanca fizike, dhe kontrollet vizuale për të parandaluar aksesin vizual të paautorizuar;

   1.2. Instalimin e ndarjeve fizike apo përdorimin e barrierave, si ekranet mbrojtëse (për shembull xhamat e pandjeshëm ndaj dritës) për të siguruar që informacioni i ndjeshëm të mos jetë i dukshëm për individë të tjerë;

   1.3. Përdorimin e sistemit të thirrjes për shërbim, ku qytetarët thirren një e nga një për të shmangur grumbullimet e individëve pranë sportelit;

1.4. Përdorimin e softuerëve që enkriptojnë të dhënat personale kur ato futen në sistemin elektronik në sportel dhe sigurimi që vetëm personeli i autorizuar ka qasje në këto të dhëna;

1.5. Edukimin dhe trajnimin e rregullt të stafit mbi masat e sigurisë dhe privatësisë në lidhje me përpunimin e të dhënave personale, për të shmangur shkeljet aksidentale të sigurisë së të dhënave.

Neni 55
Masat e Sigurisë për Sistemin e Vëzhgimit me Kamerë

1. Çdo sistem i vëzhgimit me kamerë dhe regjistrimet duhet të mbrohen duke aplikuar masat teknike dhe organizative të sigurisë, duke përfshirë, por pa u kufizuar si:

1.1. emrin e përdoruesit dhe fjalëkalimin;

1.2. fjalëkalimi duhet të përbëhet nga së paku tetë (8) karaktere, duke përfshi një shkronjë të madhe, numër dhe shenjë speciale;

1.3. ndërrimi i fjalëkalimit të bëhet çdo tre (3) muaj;

1.4. sistemi duhet të ruaj çdo gjurmë të qasjes në sistem (llog file);

1.5. instalimi i sistemit të vëzhgimit me kamerë duhet të jetë i qarkut të mbyllur dhe ndalohet transmetimi përmes internetit apo mjeteve të tjera të telekomunikimit.

2. Dhoma e monitorimit duhet të jetë e veçantë dhe qasje në të duhet të ketë vetëm personat e autorizuar.

Neni 56
Sigurimi i Ambientit të Posaçëm për Shkëmbimin e të Dhënave Personale

Komuna është e obliguar të sigurojë një ambient të posaçëm dhe privat ku qytetarët mund të diskutojnë informacione të ndjeshme pa frikë nga qasja ose dëgjimi i paautorizuar. Ky ambient duhet të jetë i izoluar nga zona e përgjithshme e sportelit, duke garantuar konfidencialitetin dhe respektimin e privatësisë së qytetarëve. Për më tepër, zyrtarët komunal janë të obliguar të sigurojnë që ky ambient të jetë i ulët për t'u përdorur nga qytetarët dhe t'i informojnë ata për mundësinë e përdorimit të tij kur kërkohet trajtimi i të dhënave të ndjeshme.

KAPITULLI X
DISPOZITAT PËRFUNDIMATRE

Neni 57
Shtojca

Shtojca: Deklarata për Konfidencialitetin dhe Mbrojtjen e të Dhënave Personale gjatë Përpunimit

1. Përfshirja e Deklaratës në Rregullore

   1.1. Deklarata për Konfidencialitetin dhe Mbrojtjen e të Dhënave Personale gjatë Përpunimit, e cila do të nënshkruhet nga të gjithë punonjësit dhe zyrtarët e Komunës që kanë qasje në të dhënat personale, përbën një pjesë të pandashme të kësaj rregulloreje;

   1.2. Kjo deklaratë përcakton detyrimet ligjore dhe etike të çdo punonjësi për të mbrojtur konfidencialitetin dhe integritetin e të dhënave personale me të cilat ata punojnë në përputhje me Ligjin nr. 06/L-082 për Mbrojtjen e të Dhënave Personale.

2. Detyrimi për Nënshkrim

   2.1. Para fillimit të punës së tyre, çdo punonjës ose zyrtar i Komunës që ka qasje në të dhënat personale është i detyruar të nënshkruajë Deklaratën për Konfidencialitetin dhe Mbrojtjen e të Dhënave Personale;

   2.2. Nënshkrimi i kësaj deklarate është një kusht i domosdoshëm për përpunimin e të dhënave personale, dhe çdo shkelje e saj mund të rezultojë në masa disiplinore, përfshirë përjashtimin nga detyra dhe ndjekjen penale.

3. Ruajtja e Deklaratës

Deklaratat e nënshkruara do të ruhen në dosjet personale të punonjësve dhe do të monitorohen rregullisht nga Zyrtari për Mbrojtjen e të Dhënave Personale për të siguruar që të gjithë punonjësit janë në përputhje me rregulloret dhe detyrimet e përpunimit të të dhënave.

Ferit Idrizi

Kryetar i Komunës

Shtojca 1

DEKLARATË

Deklaratë për Ruajtjen e Konfidencialitetit dhe Mbrojtjen e të Dhënave Personale gjatë Përpunimit

Unë, _____ (Emri, mbiemri), me funksionin _____, në bazë të Ligjit nr. 06/L-082 për Mbrojtjen e të Dhënave Personale dhe rregulloreve të Komunës, me këtë deklaratë përkushtohem për respektimin e konfidencialitetit dhe mbrojtjen e të dhënave personale gjatë ushtrimit të detyrave të mia në _____ (emri i departamentit/sektorit në Komunë), duke përfshirë përgjegjësitë e mia për të mbrojtur të drejtat e subjekteve të të dhënave dhe për të siguruar përputhshmërinë me ligjet në fuqi.
Data: _____

Nënshkrimi: _____