



REPUBLIKA E SHQIPËRISË
KOMISIONI QENDROR I ZGJEDHJEVE

KOMISIONERI SHTETËROR I ZGJEDHJEVE

Data: 23 Prill 2021

Nr: 206

U R D H Ë R

P Ë R

MIRATIMIN E PROCEDURAVE OPERACIONALE PËR RUAJTJEN DHE MBROJTJEN E TË DHËNAVE PERSONALE NË PAJISJEN ELEKTRONIKE TË IDENTIFIKIMIT (PEI), SISTEMI ELEKTRONIK I IDENTIFIKIMIT TË VOTUESVE (SEIV) NË KOMISIONIN QENDROR TË ZGJEDHJEVE, PËR ZGJEDHJET PËR KUVENDIN E SHQIPËRISË TË DATËS 25 PRILL 2021

Në mbështetje të neneve 14 dhe 19, pikat 1, shkronja “n”, e 2, të ligjit nr. 10019, datë 29.12.2008, “Kodi Zgjedhor i Republikës së Shqipërisë”, të ndryshuar

U R D H Ë R O J M Ë:

1. Miratimin e procedurave operacionale për ruajtjen dhe mbrojtjen e të dhënave personale në pajisjen elektronike të identifikimit (PEI), sistemi elektronik i identifikimit të votuesve (SEIV) të Komisionit Qendror të Zgjedhjeve, për zgjedhjet për Kuvendin e Shqipërisë të datës 25 Prill 2021, sipas tekstit që i bashkëlidhet këtij urdhri.
2. Ky urdhër hyn në fuqi menjëherë dhe publikohet në faqen zyrtare të Komisionit Qendror të Zgjedhjeve.

Nënkomisioneri Shtetëror i Zgjedhjeve

Lealba PELINKU

Komisioneri Shtetëror i Zgjedhjeve

Ilirjan CELIBASHI



Data: 23 Prill 2021

Nr. 206

“Për miratimin e procedurave operacionale për ruajtjen dhe mbrojtjen e të dhënave personale në pajisjen elektronike të identifikimit (PEI), sistemi elektronik i identifikimit të votuesve (SEIV) në Komisionin Qendror të Zgjedhjeve, për zgjedhjet për Kuvendin e Shqipërisë të datës 25 prill 2021”

PROCEDURA OPERACIONALE PËR RUAJTJEN DHE MBROJTJEN E TË DHËNAVE PERSONALE NË PAJISJEN ELEKTRONIKE TË IDENTIFIKIMIT (PEI), SISTEMI ELEKTRONIK I IDENTIFIKIMIT TË VOTUESVE (SEIV) NË KOMISIONIT QENDROR TË ZGJEDHJEVE (KQZ)

Përshkrimi i dokumentit

Ky dokument përshkruan hapat e nevojshëm të implementuar në nivel operacional dhe teknik nga Komisioni Qendror i Zgjedhjeve për menaxhimin, ruajtjen dhe asgjësimin e të dhënave personale të cilat përdoren nga ky institucion gjatë procesit zgjedhor, dhe jo vetëm, sipas ligjit nr.9887, datë 10.3.2008 “Për mbrojtjen e të dhënave personale” dhe akteve nënligjore në zbatim të tij.

Çfarë të dhënash mbledh KQZ

KQZ zotëron të dhënat personale të zgjedhësve të Republikës së Shqipërisë të cilat përfshijnë emër, mbiemër, nr. personal identifikimi, datëlindja, gjinia, qendra e votimit, dhe ID elektorale. Këto të dhëna merren sipas KQZ bazuar në nenin 45 të ligjit nr. 10019, datë 29.12.2008, “Kodi Zgjedhor i republikës së Shqipërisë, i ndryshuar, dhe në bazë të vendimit nr. 2, datë 31.10.2020 të Komisionit Rregullator, “Për llojin dhe karakteristikat teknike që duhet të plotësojnë sistemet dhe pajisjet e indentifikimit elektronik të zgjedhësve që prokurohen dhe përdoren në zgjedhje në Republikën e Shqipërisë”.

Infrastruktura elektronike e KQZ

KQZ ka në zotërim dy data center ku ndodhen serverat dhe pajisjet e komunikimit të cilat mundësojnë procesin e identifikimit elektronik të zgjedhësve në pajisjet PEI. Dy janë komponentët kryesor ku gjenden të dhënat personale të zgjedhësve.

1. Pajisja e identifikimit elektronik PEI
2. Serverat e bazave të të dhënave në datacenter primar dhe sekondar

Të gjitha pajisjet të cilat përmbajnë të dhëna personale janë në pronësi të KQZ dhe menaxhohen nga vet stafi i KQZ. Në rast kur stafi i KQZ nuk ka aftësi teknike për menaxhimin e programeve të ofruara nga palët e treta dhe konkretisht sistemi i identifikimit elektronik dhe pajisja PEI aksesit i të dhënave kryhet nga persona të specializuar të palëve të treta të mbikëqyrur nga stafi teknik i KQZ. Palët e treta duhet të ndjekin politika për ruajtjen dhe manipulimin e të dhënave personale bazuar në “European General Data Protection Regulation” (GDPR).

Personat e autorizuar për të punuar me pajisjet elektronike

Personat e autorizuar për të punuar, menaxhuar apo aksesuar pajisjet elektronike të cilat përmbajnë të dhëna personale janë punonjës të KQZ dhe palë të treta të cilat menaxhojnë programin software i cili nevojitet për identifikimin elektronik të zgjedhësve.

Kontrolluesit, përpunuesit dhe personat e autorizuar që vihen në dijeni me të dhënat e përpunuara nëpërmjet sistemit objekt i këtij akti, gjatë ushtrimit të funksioneve të tyre, detyrohen të ruajnë konfidencialitetin dhe besueshmërinë edhe pas përfundimit të funksionit apo mbledhjes së të dhënave. Këto të dhëna nuk përhapen, përveç rasteve të parashikuara në ligj.

Punonjësit e KQZ menaxhojnë dhe aksesojnë këto të dhëna bazuar në rregulloren e brendshme të KQZ për menaxhimin e pajisjeve elektronike.

Palët e treta menaxhojnë dhe aksesojnë të dhënat bazuar në kontratë, duke firmosur marrëveshjen e mos nxjerrjes së sekretit dhe e zhvillojnë aktivitetin e tyre në ambientet e vendosura në dispozicion nga KQZ pa pasur qasje në internet dhe të mbikëqyrur nga punonjës të autorizuar të KQZ.

Aksesi në internet për të gjithë infrastrukturën e cila ka të dhëna personale nuk lejohet. Punonjësit apo palët e treta të cilat janë të autorizuar të punojnë dhe menaxhojnë të dhënat nuk lejohen të përdorin pajisje personale por përdorin pajisje të ofruara dhe në pronësi të KQZ. Memoriet e jashtme të të gjitha tipeve janë në pronësi të KQZ dhe përdoren vetëm në ambientet e brendshme të godinave ku ndodhet data center për të transferuar të dhëna. Pas përdorimit të dhënave të këtyre memorieve shkatërrohen nëpërmjet formatimit të tyre minimumi 10 herë duke alternuar tipin e file sistem gjatë formatimit. Nëse këto memorie duhet të ruhen atëherë ato vendosen në një vend të sigurt brenda data center tek e cila kanë akses vetëm persona të autorizuar.

Mënyra e ruajtjes së të dhënave personale

Pajisjet të cilat përmbajnë të dhëna personale janë:

- a) Sistemi elektronik i identifikimit të votuesve (SEIV)
- b) Pajisja elektronike e identifikimit (PEI)

Të gjitha pajisjet të cilat përmbajnë të dhëna personale duhet të plotësojnë minimalisht kërkesat e mëposhtme:

Nëse pajisja është e tipit server atëherë:

- a) Kjo pajisje nuk duhet të ketë qasje në internet dhe për rrjedhojë të mos jetë e kapshme nga pajisje apo përdorues të cilët ndodhen jashtë godinave ku ndodhet data center.
- b) Pajisja duhet të mbrohet nga një sistem firewall për aksesin e saj edhe nga vet rrjeti i brendshëm LAN.

- c) Të gjithë përdoruesit lokal të pajisjes duhet të kenë një fjalëkalim i cili respekton politikat e një fjalëkalimi të komplikuar.
- d) Të gjithë përdoruesit e bazës së të dhënave duhet të kenë një fjalëkalim i cili respekton politikat e një fjalëkalimi të komplikuar.
- e) Vetë pajisja duhet të ketë një sistem fireëall i cili bllokun aksesin nga LAN
- f) Dhoma ku qëndron pajisja duhet të jetë e siguarur nga aksesit fizik nga persona të paautorizuar
- g) Ambienti rrethues duhet të mbikëqyret me kamera

Nëse pajisja është e tipit desktop, laptop, mobile, vet pajisja PEI apo çdo pajisje tjetër e cila ndërvepron në mënyrë të drejtpërdrejtë me sistemin SEIV atëherë:

- a) Pajisja nuk duhet të ruaj asnjë të dhënë personale në memorien e saj të brendshme
- b) Të dhënat duhet të ruhen vetëm në memorie të jashtme dhe të jenë të enkriptuara
- c) Pajisja nuk duhet të jetë e lidhur me internetin gjatë përpunimit apo aksesimit të memories e cila ka të dhëna personale
- d) Pajisja duhet të jetë pajisje e cila është në pronësi të KQZ
- e) Nëse pajisja transportohet nga një vend në një tjetër atëherë ajo duhet të transportohet e vulosur me vula me numër në mënyrë që memoria e jashtme e saj mos të aksesohet fizikisht apo nëpërmjet software pa prishur këtë vullë.

Procedura operacionale e pajisjes PEI

Pajisja PEI do të përdoret në zgjedhjet për kuvend të 25 Prill 2021 në 5199 qendra votimi në të gjithë territorin e Republikës së Shqipërisë. Procedurat operacionale për menaxhimin e kësaj pajisjeje në terren janë si më poshtë:

1. Pajisja do të transportohet nën kujdesin e KQZ dhe do të jetë e vulosur me vula me kode sigurie të KQZ.
2. Pajisjet do të dorëzohen në çdo KZAZ duke mbajtur procesverbalin përkatës
3. KZAZ do të dorëzojë çdo qendër votimi (QV) një pajisje PEI me procesverbalin përkatës
4. Pajisja PEI në çdo QV do të menaxhohet dhe konfigurohet nga një punonjës i KQZ i cili sigurohet që pajisja të funksionoj pa probleme dhe vulat e sigurisë të cilat mbrojnë memoriet USB nuk janë të dëmtuara.
5. USB-të të cilat përmbajnë informacione personale janë gjithmonë të koduara (enkriptuara) në mënyrë që mos të jenë të lexueshme në pajisje elektronike.
6. Pajisja PEI gjatë procesit të votimit regjistron gjurmën biometrike të gishtit në memorien USB të enkriptuar.

7. Pajisja PEI pas çdo tentative identifikimi e suksesshme apo e pasuksesshme printon informacionin në letër i cili përmban të dhëna personale.
8. Këto letra të printuara administrohen nga operatori i pajisjes PEI dhe gjatë procesit futen në një zarf i cili bashkohet me materialet zgjedhore të cilat vulozen dhe transportohen drejt KZAZ-së e më pas KQZ-së.
9. Këto letra të printuara me të dhëna personale të zgjedhësve ruhen për një periudhe kohe sipas ligjeve në fuqi dhe më pas asgjësohen me djegie në prani të një komisioni të ngritur për këtë qëllim.
10. Pajisjet PEI pas përfundimit të procesit të votimit paktohen në kutinë e posaçme nga operatori përkatës dhe dërgohen të vulosura me vula me kode sigurie në magazinat qendrore të KQZ.
11. Procesi i dedublikimit të të dhënave kryhet në ambientet e KQZ nga punonjës të cilët janë punonjës të KQZ duke u ndihmuar nga stafi i kompanisë e cila ka prodhuar sistemin SEIV.
 - a. Pajisjet mbledhen në ambientet e KQZ nga çdo ZAZ.
 - b. Punonjësit e specializuar të KQZ për procesin e dedublikimit të shenjave të gishtërinjve kryejnë kontrollin e vulave të sigurisë dhe më pas këputjen e tyre në mënyrë që të kryhet kalimi i të dhënave personale nga memoria e jashtme e pajisjes PEI në bazën e të dhënave të serverit të sistemit SEIV.
 - c. Të dhënat transferohen nga memoria USB në serverin e të dhënave SEIV
 - d. Memoriet USB ruhen në një vend të sigurt pasi kryhet importimi i të dhënave në sistemin SEIV.
 - e. I gjithë ky proces kryhet në prani të personave të autorizuar të KQZ dhe punonjësve të kompanisë e cila ka ndërtuar sistemin.
 - f. Veprimet operacionale si, këputja e vulave, transportimi i memorieve USB dhe importimi i të dhënave në serverin SEIV kryhen nga persona të autorizuar të KQZ.
 - g. Persona të autorizuar të kompanisë e cila ka ndërtuar sistemin SEIV kryen mbikëqyrjen e procesit dhe jep mbështetje teknike kur i kërkohet kjo gjë.
12. Pasi kryhet leximi i memorieve USB, dekriptimi i të dhënave që ato përmbajnë dhe kalimi i tyre në server atëherë personat e specializuar të KQZ marrin memorien dhe e fshijnë menjëherë.
13. Memoria e brendshme e pajisjeve PEI të vulosura ruhen në magazinat e KQZ të paprekura për 3 muaj nga data e shpalljes së rezultatit përfundimtar të zgjedhjeve e më

pas të dhënat shkatërrohen sipas udhëzimeve të Komisionerit Shtetëror të Zgjedhjeve dhe Nënkomisionerit Shtetëror të Zgjedhjeve.

14. Të dhënat në server fshihen duke ekzekutuar komandat përkatëse për fshirjen e të dhënave nga serveri në prani të komisionit.
15. Çdo backup ekzistues asgjësohet në prani të komisionit sipas procedurës së përcaktuar në udhëzimet e përcaktuara në aktin referuar në pikën 13 më lart.