Në bazë të nenit 27 të Statutit të Ndërmarrjes Publike për Rrugë Shtetërore, dhe në lidhje me nenet 119 dhe 120 të Ligjit për mbrojtjen e të dhënave personale (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 42/20) dhe nenit 47 të Rregullores për sigurinë e përpunimit të të dhënave personale (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 122/20), drejtori i Ndërmarrjes Publike për Rrugë Shtetërore miratoi

RREGULLORE

PËR MASAT TEKNIKE DHE ORGANIZATIVE PËR SIGURIMIN E SIGURISË SË PËRPUNIMIT TË TË DHËNAVE PERSONALE NË NDËRMARRJEN PUBLIKE PËR RRUGË SHTETËRORE

Neni 1

Me këtp Rregulla përshkruhen masat teknike dhe organizative të zbatuara nga Ndërmarrja Publike për Rrugë Shtetërore (në tekstin e mëtutejshëm NPRRSH) në cilësinë e kontrolluesit për të siguruar sigurinë dhe mbrojtjen e përpunimit të të dhënave personale.

Neni 2

NPRRSH regjistron dhe ruan të gjithë dokumentacionin për programet softuerike për përpunimin e të dhënave personale, si dhe për të gjitha ndryshimet e tij.

Neni 3

Dispozitat e këtyre rregullave zbatohen për:
- përpunimin e automatizuar plotësisht dhe pjesërisht të të dhënave personale dhe
- përpunimet tjera manuale të të dhënave personale, të cilat janë pjesë e një koleksioni ekzistues të të dhënave personale ose synohen të jenë pjesë e një koleksioni të të dhënave personale

Neni 4

(1) NPRRSH zbaton masa teknike dhe organizative që sigurojnë fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale të përshtatshme për natyrën, qëllimin, kontekstin dhe qëllimet e përpunimit, si dhe rreziqet në përpunimin e tyre.

(2) Masat teknike dhe organizative të përmendura në paragrafin (1) të këtij neni zbatohen në mënyrë proporcionale për aktivitetet e përpunimit të të dhënave personale, klasifikohen në dy nivele:
- standarde dhe
- të larta

Neni 5

(1) Masat teknike dhe organizative në nivel standard janë të detyrueshme për të gjitha grumbullimet e të dhënave personale.

(2) Për dokumentet që përmbajnë: kategori të veçanta të të dhënave personale, të dhënat personale të përpunuara për qëllime policore dhe të dhënat personale të përpunuara për mbrojtjen e sigurisë kombëtare dhe mbrojtjen e Republikës së Maqedonisë së Veriut, për dokumentet e transmetuara përmes rrjetit të komunikimit elektronik dhe që përmbajnë kategori të veçanta të të dhënave personale dhe/ose një numër amë të qytetarit, masat teknike dhe organizative në nivel standard dhe të lartë janë të detyrueshme.

Neni 6

Të dhënat që përmbajnë NVAQ duhet të zbatohen masa teknike dhe organizative të klasifikuara në nivel standard dhe të lartë.

NIVELI STANDARD

Masat teknike

Neni 7

NPRRSH zbaton masa përkatëse teknike për të siguruar konfidencialitetin dhe mbrojtjen e përpunimit të të dhënave personale, edhe atë:

1. një emër përdoruesi dhe fjalëkalim unik për çdo person të autorizuar;
2. një fjalëkalim i përbërë nga një kombinim i tetë karaktereve alfanumerike - shkronja (të vogla dhe të mëdha) dhe karaktere të veçanta;
3. emri i përdoruesit dhe fjalëkalimi që i lejon personit të autorizuar të hyjë në sistemin e informacionit në tërësi, qasje në aplikacione individuale dhe/ose koleksione individuale të të dhënave personale të nevojshme për kryerjen e detyrave të punës;
4. hyrja në sistemin e informacionit në të cilin të dhënat përpunohen, ruhen dhe menaxhohen përmes sistemeve të krijuara përmes një certifikate digjitale të kualifikuar dhe një emri përdoruesi dhe fjalëkalimi unik për secilin person të autorizuar në certifikatën digjitale;
5. evidentim të personave të autorizuar që kanë qasje të autorizuar në dokumente dhe në sistemin e informacionit dhe procedurat për identifikimin dhe verifikimin e qasjes së autorizuar;

6. rregullat e konfidencialitetit dhe integritetit gjatë raportimit, caktimit dhe ruajtjes së fjalëkalimeve dhe ndryshimit automatik të tyre pas një periudhe prej tre muajsh;
7. kriptimi i të dhënave personale;
8. dalja automatike nga sistemi i informacionit pas një periudhe të caktuar pasiviteti (jo më shumë se 15 minuta) dhe për aktivizimin e përsëritshëm të sistemit kërkon ri-futjen e emrit të përdoruesit dhe fjalëkalimit;
9. refuzimi i automatizuar i sistemit të informacionit pas tre përpjekjeve të pasuksesshme të hyrjes (futja e emrit të përdoruesit dhe fjalëkalimit të gabuar) dhe njoftimi i automatizuar i përdoruesit se ai duhet të kërkojë udhëzime nga administratori i sistemit;
10. një pengesë e instaluar e rrjetit mbrojtës harduerit/softuerit ("firewall") ose router midis sistemit të informacionit dhe internetit ose ndonjë forme tjetër të rrjetit të jashtëm, si një masë mbrojtëse kundër përpjekjeve të paautorizuara ose me qëllim të keq për të hyrë ose thyer sistemin;
11. mbrojtje efektive dhe të besueshme anti-virus dhe anti-spajver të sistemit të informacionit, i cili do të azhurnohet vazhdimisht për parandalim kundër kërcënimeve të panjohura dhe të paplanifikuara të viruseve dhe spajvereve të reja;
12. mbrojtje efektive dhe e besueshme anti-spam e cila do të azhurohet vazhdimisht për mbrojtje parandaluese kundër spamit;
13. lidhja e sistemit të informacionit (kompjuterët dhe serverët) me një rrjet energjetik përmes furnizimit të pandërprerë me energji
14. sigurimi i ueb-faqes së NPRRSH duke aplikuar masa teknike që garantojnë identitetin e saktë të faqes, si dhe konfidencialitetin e informacionit në faqe;
15. azhurnimi i rregullt i softuerit antivirus dhe një politikë e përcaktuar për azhurnimet e rregullta të programeve softuerike;
16. ruajtjen e të dhënave të përdoruesve të serverëve të kontrolluesit për të cilin bëhet rregullisht një kopje e sigurisë dhe në rastin kur të dhënat ruhen në nivel lokal, domosdoshmërisht me masa sinkronizimi ose me masa shtesë mbrojtëse rezervë bazuar në analizën e rrezikut;
17. kufizimi i mundësisë së lidhjes së mediave portative (USB, hard disqet e jashtme, etj.) ndaj sistemet e rëndësisë parësore;
18. çaktivizimi automatik i regjimit të punës për mediumet e trasmentimit (Disable autorun for removable media);
19. mjetet e administrimit të largët duhet të vendosen në mënyrë të tillë që ata të sigurojnë më parë pëlqimin e personit të autorizuar të NPRRSH-së në stacionin e punës së përdoruesit para çdo ndërhyrjeje në vetë stacionin e punës;
20. vendosja e sistemit të informacionit që do të sigurojë që personi i autorizuar i NPRRSH-së të kryejë administrimin në distancë të stacionit të punës së përdoruesit, si dhe kur të përfundojë të njëjtën (për shembull, duke shfaqur një mesazh në ekran që administrata në distancë ka përfunduar);

21. ndalimi i punës me programe softuerike të shkarkuara që nuk vijnë nga burime të sigurta;
22. kufizimi i përdorimit të programeve softuerike që kërkojnë të drejta administrative;
23. fshirja e të dhënave të vendosura në një stacion pune që do të transmetohet;
24. azhurnimi i programeve softuerike kur të metat kritike identifikohen dhe korrigjohen;
25. instalimi i azhurimeve në sistemet operative me verifikim automatik në përputhje me vlerësimin e rrezikut dhe të paktën një herë në javë; dhe
26. rritja e nivelit të ndërgjegjësimit në lidhje me atë që personat e autorizuar duhet t 'i kushtojnë vëmendje dhe dhënat e kontaktit të personave që do të kontaktohen në rast të një incidenti ose ndodhjes së një ngjarjeje të pazakontë që prek informacionin dhe komunikimin e sistemeve të kontrolluesit.

Sigurimi i mediave portative

Neni 8

(1) NPRRSH, në përputhje me analizën e rrezikut të shkeljes së sigurisë së të dhënave personale në rast vjedhjeje ose humbje tjetër të mediave portative (pajisjeve mobile) në të cilat kryhet përpunimi i të dhënave personale, zbaton masat e duhura teknike, edhe atë:
- ngritjen e vetëdijes së personave të autorizuar për rreziqet specifike që lidhen me përdorimin e mediave portative dhe marrjen e masave për zvogëlimin e rreziqeve

- përdorimi i shërbimeve reve (cloud services) për bërjen e kopje të sigurta vetëm pas analizës paraprake të termave dhe kushteve të tyre dhe garancive të sigurisë.

Mbrojtja e rrjetit të brendshëm

Neni 9

(1) NPRRSH siguron mbrojtjen e rrjetit të saj të brendshëm duke ofruar vetëm funksionet e nevojshme të rrjetit të nevojshme për përpunimin e të dhënave personale, dhe në veçanti përmes:
- kufizimit të qasjes në internet duke bllokuar shërbimet dhe shërbimet jo-thelbësore (VoIP, peer-to-peer, etj.);
- menaxhimi i rrjetit të Wi-Fi që mbulon përdorimin e metodave më të fundit të kriptimit (WPA2 ose WPA2-PSK dhe duke përdorur një fjalëkalim kompleks e cila ndryshon gjatë një periudhe kohore të caktuar);
- në rastin e qasjes në distancë, vendosja e detyrueshme e një lidhjeje VPN, me vërtetimin e detyrueshëm të personit të autorizuar duke përdorur një certifikatë digjitale të kualifikuar;

- sigurimin e asnjë paneli administrativ për menaxhimin e përmbajtjes dhe vendosjen e sistemit që të mos jetë drejtpërdrejt i arritshëm përmes internetit (mirëmbajtja në distancë duhet të kryhet përmes një VPN); dhe
- kufizimi i rrjetit trafikor duke filtruar trafikun hyrës/dalës në pajisjet me murë mbrojtës dhe servere proksi.

Sigurimi i serverëve

Neni 10

(1) Zbatimi i masave teknike dhe organizative për serverat e NPRRSH-së, në të cilat është e centralizuar përpunimi i një sasie të madhe të të dhënave personale, detyrimisht duhet të përfshijë:
- qasje në mjetet dhe panelet administrative të serverëve mund të ketë vetëm personat e autorizuar nga drejtori
- aplikimi i autorizimeve me më pak privilegje për personat që nuk janë administratorë të sistemit të informacionit (operacione të zakonshme për përdoruesit standardë);
- zbatimin e një politike të veçantë për krijimin dhe përdorimin e fjalëkalimeve për administratorët e sistemit të informacionit
- instalimi i të gjitha azhurimeve (updates) të rëndësishme për sistemet operative dhe aplikacionet në një interval kohor të bazuar në analizën e rrezikut, por jo më të gjatë se azhurimi javor me rregullimin e sistemit automatik të auzhurimit (auto update);
- bërja e kopjeve të sigurisë dhe t 'i kontrollojë ato rregullisht; dhe
- zbatimi i një protokolli TLS (zëvendësimi i SSL13) ose protokolli tjetër që siguron shifrimin dhe vërtetimin, si minimum për çdo shkëmbim të të dhënave përmes internetit dhe konfirmimin e aplikimit të tij të përshtatshëm përmes mjeteve të duhura.
(2) Në rastin kur kryhet administrimi i bazave të të dhënave, zbatohen masat në vijim:
- përdorimi i profileve të personalizuara për qasje në bazat e të dhënave dhe krijimin e një emri të veçantë të përdoruesit për secilin aplikacion (specific account for each application); dhe
- aplikimi i masave kundër sulmeve duke injektuar kodin SQL, skriptet dhe të ngjashme.

Sigurimi i ueb-faqes të kontrolluesit

Neni 11

(1) Për ueb-faqen e NPRRSH, zbatohen masa teknike për të garantuar identitetin e saktë të faqes (pharming prevention), si dhe konfidencialiteti i informacionit të dërguar ose të mbledhur përmes ueb-faqes, dhe në veçanti përmes masave të mëposhtme:
- zbatimi i një protokolli kriptografik (TLS duke zëvendësuar SSL) në të gjitha ueb-faqet, duke përdorur vetëm versionin e fundit dhe duke kontrolluar zbatimin e tij të duhur;

- përdorimi i detyrueshëm i një protokolli kriptografik (TLS) për të gjitha ueb-faqet, duke përfshirë edhe formularët për mbledhjen e të dhënave personale ose për të mundësuar vërtetimin e përdoruesit dhe ato në të cilat shfaqen ose transmetohen të dhënat personale që nuk janë në dispozicion të publikut;
- kufizimi i porteve të komunikimit në ato që janë rreptësisht të nevojshme për funksionimin e duhur të aplikacioneve të instaluara. Nëse ueb serveri pranon vetëm lidhjet e protokollit HTTPS, lejohet vetëm trafiku i rrjetit IP që hyn përmes portit 443 dhe të gjitha portet e tjera të hyrjes duhet të bllokohen;
- qasje në mjetet dhe ndërfaqet administrative, mund të kenë persona të autorizuar me privilegje administrative të cilët janë pjesë e ekipit përgjegjës për teknologjinë e informacionit dhe vetëm për aktivitetet administrative që janë të nevojshme; dhe
- nëse përdoren biskotat që nuk kërkohen nga shërbimi, sigurohet pëlqimi paraprak nga përdoruesi i internetit pasi do të njofton përdoruesin, ndërsa para se të depozitohet biskotat;

(2) Nuk duhet të zbatohen praktika që rrisin rrezikun e keqpërdorimit të mundshëm, të padëshiruar (aksidental) ose të qëllimshëm të përpunimit të paautorizuar të të dhënave personale, dhe në veçanti:
- të mos transmetojë të dhëna personale përmes URL pa aplikimin e një protokolli të kriptimit (për shembull, identifikuesit ose fjalëkalimet);
- përdorimi i shërbimeve të pasigurta;
- përdorimi i serverëve që hostirojnë bazat e të dhënave ose serverat si stacione pune, veçanërisht jo për shfletim në ueb-faqen, qasje deri te porositë elektronike dhe të ngjashme;
- instalimin e bazave të të dhënave në serverat e qasme direkt nëpërmjet internetit; dhe
- ndarja dhe përdorimi i llogarive të përdoruesve (user accounts) midis dy ose më shumë personave të autorizuar.

Administrator i sistemit të informacionit dhe personave të autorizuar

Neni 12

(1) Administratori i sistemit është një person profesional në fushën e informacionit dhe komunikimit, i punësuar në NPRRSH, i cili kujdeset për funksionalitetin e sistemit të informacionit në drejtim të sigurimit të integritetit dhe sigurisë së të dhënave, aplikimit për qasje në të dhëna dhe pajisjeve teknike që janë në funksion të sistemit të informacionit, si dhe sigurimit të konfidencialitetit dhe mbrojtjes së të dhënave.
(2) Sistemi i informacionit i NPRRSH është i gjithë sistemi i përbërë nga kompjuterë personalë, serverë dhe pajisje komunikimi, pajisje për sigurimin e sigurisë së të dhënave, bazës së të dhënave, aplikimit dhe aplikacioneve dhe pajisjeve të tjera të përdorura për përpunimin e të dhënave.
(3) Detyrimet dhe përgjegjësitë e administratorit të sistemit të informacionit definohen dhe përcaktohen në Rregulloren për përcaktimin e detyrimeve dhe përgjegjësive të administratorit të sistemit të informacionit dhe personave të autorizuar.

(4) Zyrtari për mbrojtjen e të dhënave personale detyrimisht kryen kontroll periodik mbi punën e administratorit të sistemit të informacionit dhe përgatit raport për kontrollin e kryer.
(5) Raporti duhet të përmbajë parregullsitë e konstatuara dhe masat e propozuara për eliminimin e këtyre parregullsive.

Detyrimet dhe përgjegjësitë e personave të autorizuar

Neni 13

(1) Detyrimet dhe përgjegjësitë e secilit person të autorizuar i cili ka qasje deri në të dhëna personale dhe në sistemin e informacionit, NPRRSH i definon dhe përcakton në Rregullat për përcaktimin e detyrimeve dhe përgjegjësive të administratorit në sistemin e informacionit dhe të personave të autorizuar.
(2) NPRRSH i njofton detyrimisht personat e autorizuar të përmendur në paragrafin (1) të këtij neni me dokumentacionin për masat teknike dhe organizative që lidhen me kryerjen e detyrave dhe përgjegjësive të tyre.

Identifikimi dhe kontrollimi

Neni 14

(1) NPRRSH detyrimisht duhet të mbajë evidencës për personat e autorizuar të cilët kanë qasje të autorizuar në dokumente dhe në sistemin e informacionit, si dhe të përcaktojë procedurat për identifikimin dhe verifikimin e qasjes së autorizuar.
(2) Kur kontrillimi kryhet në bazë të emrit të përdoruesit dhe fjalëkalimit, NPRRSH zbaton gjithmonë rregullat që garantojnë konfidencialitetin dhe integritetin e tyre gjatë raportimit, caktimit dhe ruajtjes së të njëjtave.
(3) Fjalëkalimet duhet të ndryshohen automatikisht pas një periudhe kohore që nuk mund të jetë më e gjatë se tre muaj.
(4) Për të siguruar identifikimin e çdo qasje të paautorizuar (mashtrues) ose keqpërdorim të të dhënave personale, si dhe për të përcaktuar origjinën e këtyre incidenteve, NPRRSH krijon dhe mban evidencë për secilën qasje në sistemin e informacionit – logs (nga sistemet operative, nga muri mbrojtës (firewall), serveri i projektuar posaçërisht për t 'u përdorur si një server skedar (file server), bazat e të dhënave, sistemi (softueri) për menaxhimin e dokumenteve (DMS System);
(5) Zyrtari për mbrojtjen e të dhënave personale i emëruar në Departamentin e TIK-ut dhe/ose nga një person tjetër i autorizuar nga kontrolluesi i cili ka njohuritë dhe

aftësitë e nevojshme, por nuk ka privilegje administrative, kryen kontroll të evidentimit të të dhënave nga paragrafët (2) dhe (3) të kësaj të paktën një herë në muaj dhe përgatit një raport për kontrollin e kryer dhe për parregullësitë e konstatuara
(6) Evidenca e përmendura në paragrafin (1) të këtij neni ruhet të paktën pesë vjet.
(7) Personat e autorizuar për menaxhimin e sistemit të evidencës për qasje në sistemin e informacionit duhet të njoftojnë udhëheqësin e udhëheqësisë së departamentit të TIK-ut dhe drejtorin për çdo anomali apo incident të sigurisë, menjëherë dhe më së voni brenda 12 orëve nga momenti i incidentit.
(8) Udhëheqësi i departamentit të TIK-ut ose personi i autorizuar për menaxhimin e sistemit të evidencës njofton Agjencinë për mbrojtjen e të dhënave personale për çdo shkelje të sigurisë së të dhënave personale dhe nëse kjo mund të shkaktojë rrezik të lartë për të drejtat dhe liritë e personave fizikë dhe subjekteve të të dhënave personale, me qëllim kufizimin e pasojave të shkeljes së sigurisë.

Kontrolli i qasjes

Neni 15

(1) Personat e autorizuar duhet të kenë qasje të autorizuar vetëm në të dhënat personale dhe pajisjet e informacionit dhe komunikimit që janë të nevojshme për kryerjen e detyrave të tyre të punës.
(2) NPRRSH vendos mekanizma për të parandaluar personat e autorizuar nga qasja në të dhënat personale dhe pajisjet e informacionit dhe komunikimit me të drejta të ndryshme nga ato të autorizuara.
(3) Administratori i sistemit të informacionit i cili është i autorizuar në përputhje me Rregullat për përcaktimin e detyrimeve dhe përgjegjësive të administratorit të sistemit të informacionit dhe personave të autorizuar mund të ndajë, modifikojë ose revokojë qasjen e autorizuar në të dhënat personale dhe pajisjet e informacionit dhe komunikimit vetëm në bazë të një urdhri të dhënë nga drejtori i NPRRSH dhe në përputhje me kriteret e përcaktuara nga NPRRSH.

Parandalimi, reagimi dhe korrigjimi i incidenteve

(sigurimi i vazhdimësisë)

Neni 16

(1) NPRRSH përgatit një Plan (Rregulla) për parandalimin, reagimin dhe korrigjimin e incidenteve në sistemin e tij të informacionit dhe një listë të personave të autorizuar përgjegjës për parandalimin, si dhe për rivendosjen në kohë të disponueshmërisë së të dhënave personale dhe qasjen në to në rast të një incidenti fizik ose teknik.
(2) NPRRSH përcakton procedurat e zbatueshme për kthimin e të dhënave personale dhe mënyrën e regjistrimit të personave të autorizuar të përmendur në paragrafin (1) të këtij neni, të cilët kanë kryer operacionet për kthimin e të dhënave personale, kategoritë e të dhënave personale që janë kthyer ose që janë futur manualisht gjatë kthimit.
(3) Parandalimi i incidenteve mbulon të gjitha masat dhe kontrollet e përcaktuara me këtë Rregullore, ndërsa në bazë të analizës së rrezikut të kryer mbulon (përdorimin e furnizimit me energji të pandërprerë për të mbrojtur pajisjet e përdorura për përpunimin e të dhënave personale, përdorimin e njëkohshëm të pajisjeve të shumta në një sekuencë për ruajtjen e të dhënave personale/teknologjisë RAID/, testimin e rregullt të funksionalitetit të pajisjeve dhe të ngjashme).

Kopjet e sigurta dhe rivendosja e të dhënave personale të ruajtura (sigurimi i vazhdimësisë)

Neni 17

(1) NPRRSH, bazuar në analizën e rrezikut, bën kopje të sigurta të të dhënave personale në intervale të rregullta në mënyrë që të zvogëlojë efektin në rast të humbjes ose dëmtimit të tyre të padëshiruar.
(2) Kopjet e sigurisë të përmendura në paragrafin (1) të këtij neni do të bëhen dhe testohen rregullisht, për të cilat do të miratohet një plan i vazhdimësisë së biznesit (business continuity plan) që parashikon të gjitha incidentet e mundshme (për shembull: incidentet e harduerit).
(3) NPRRSH do të bëjë një kopje të fragmentuar (incremental back-up), përkatësisht një kopje individuale në baza ditore në lidhje me të gjitha ndryshimet e ndodhura gjatë ditës, dhe një rezervë të plotë (full back-up) në intervale të rregullta sipas vlerësimit të saj, ndërsa të paktën një herë në muaj, në një mënyrë që do të garantojë rivendosjen e disponueshmërisë së të dhënave personale në rast të një incidenti fizik ose teknik.
(4)NPRRSH kontrollon funksionalitetin e kopjeve të sigurisë për kryerjen e rindërtimit të të dhënave personale.
(5) Kopjet e sigurisë ruhen jashtë hapësirës së serverit dhe mbrohen fizikisht dhe kriptografikisht në mënyrë që të parandalohet çdo modifikim.
(6) Në lidhje me kopjet e sigurisë, zbatohet i njëjti nivel sigurie i masave teknike dhe organizative si për të dhënat e ruajtura në serverat operativ në të cilët kryhet përpunimi i të dhënave personale duke kriptuar kopjet e sigurisë, duke ruajtur në një vend të sigurt kopjen e sigurisë për të cilën janë zbatuar masa dhe kontrolle që minimizojnë rrezikun e përmbytjeve, zjarrit, vjedhjes dhe të ngjashme, ose në rastin e rregullimit kontraktual dhe transferimit të shërbimit, mbrojtje e përshtatshme që do të zbatohet nga përpunuesi.

Mënyra e arkivimit dhe ruajtjes së të dhënave

Neni 18

(1) NPRRSH, në lidhje me të dhënat personale për të cilat ende nuk ka skaduar afati për ruajtjen e tyre në përputhje me ligjin dhe për të cilat është ndërprerë nevoja për përpunimin e tyre të drejtpërdrejtë dhe të përditshëm, do t 'i arkivojë ato në mënyrë të sigurt, veçanërisht nëse të dhënat e arkivuara janë të dhëna të ndjeshme (kategori të veçanta të të dhënave personale), ose të dhëna që mund të kenë ndikim serioz në subjektet e të dhënave personale, nëse ato kompromethohen.

(2) NPRRSH përshkruan procedurën për menaxhimin e materialit arkivor për sa i përket asaj se cilat të dhëna duhet të arkivohen, si dhe ku ruhen ato dhe kush, dhe në çfarë kushtesh, ka qasje deri tek ata.

(3) NPRRSH përgatit "Listën (rishikimin) me afate për ruajtjen e të dhënave personale" që përmban informacion për momentin e aktivizimit të periudhës (afatit) për ruajtjen e të dhënave personale, afatet (afatet) e identifikuara për ruajtjen e të dhënave personale, arsyet për ruajtjen e të dhënave personale, bazën ligjore për ruajtjen e të dhënave personale dhe pronarin e të dhënave, e cila rishikohet dhe harmonizohet çdo vit në përputhje me ndryshimet në funksionimin dhe kushtet ligjore për ruajtjen e të dhënave personale.

Menaxhimi me mediat

Neni 19

(1) NPRRSH krijon sistem për regjistrimin e mediumeve të pranuara, me qëllim që të mundësohet identifikimi i drejtpërdrejtë ose i tërthortë i llojit të mediumit të pranuar, datës dhe kohës së pranimit, dërguesit, numrit të mediumeve të pranuara, llojit të dokumentit të regjistruar në medium, mënyrës së dërgimit të mediumit, emri dhe mbiemri i personit të autorizuar për pranimin e mediumit.

(2)Dispozitat e paragrafit (1) të këtij neni do të zbatohen edhe për regjistrimin e mediave të dërguara nga NPRRSH.

(3) Mediat portative në të cilat kryhet përpunimi i të dhënave personale duhet të ruhen në një vend në të cilin kanë qasje vetëm personat e autorizuar të përcaktuar me këtë Rregullore.

(4)Transferimi i mediave jashtë ambienteve të punës do të kryhet vetëm me autorizim paraprak nga Drejtori i NPRRSH.
(5)Për mediat e transferuara jashtë ambienteve të punës së NPRRSH, do të ndërmerren masat e nevojshme për parandalimin e përpunimit të paautorizuar të të dhënave personale të regjistruara në to. Media mund të transferohet jashtë vendit të punës nëse të dhënat personale janë të koduara ose të mbrojtura me metoda të përshtatshme që sigurojnë që të dhënat nuk do të jenë të lexueshme, me anë të të cilave vetëm administratori i sistemit të informacionit mund t 'i dekriptojë ato ose një person i autorizuar prej tij.
(6) Pas transferimit të të dhënave personale nga mediumi ose pas skadimit të periudhës së caktuar për ruajtje, media duhet të shkatërrohet, fshihet ose pastrohet nga çdo e dhënë personale e regjistruar në to.
(7) Shkatërrimi i mediumit kryhet duke ndarë mekanikisht pjesët përbërëse të tij ashtu që i njëjti nuk mund të përdoret.
(8) Fshirja ose pastrimi i medias duhet të bëhet në një mënyrë që parandalon ripërtrirjen e mëtutjeshëm të të dhënave personale të regjistruara.
(9)Për rastet e përmendura në paragrafët (7) dhe (8) të këtij neni, duhet të sigurohet një gjurmë informacioni (për shembull: procesverbal), i cili përmban të gjitha të dhënat për identifikimin e plotë të mediumit, si dhe për kategoritë e të dhënave personale që janë regjistruar në të.

Kriptimi i të dhënave personale

Neni 20

(1) Të dhënat personale mund të transmetohen përmes rrjetit të komunikimit elektronik vetëm nëse ato janë të koduara ose nëse mbrohen në mënyrë specifike me metoda të përshtatshme që sigurojnë që të dhënat nuk do të jenë të lexueshme gjatë transmetimit.
(2) Kriptimi i të dhënave personale kryhet duke aplikuar zgjidhjet më të fundit teknike të kriptimit që sigurojnë integritetin, konfidencialitetin dhe vërtetësinë e të dhënave personale, edhe atë: të theksohen nga gjërat e përmendura mëposhtë

NPRRSH riemëron SHA-256, SHA-512 ose SHA-341 si një funksion hash, HMAC duke përdorur SHA-256, bcrypt, scrypt ose PBKDF2 për të ruajtur fjalëkalimet, AES ose AES-CBC për kriptime simetrike, RSA-OAEP v2.1 për kriptime asimetrike...), algoritme të sigurta për kriptim, dhe në të njëjtën kohë siguron mbrojtje për çelësat e fshehtë për kriptim me të drejtat e qasjes kufizuese dhe një fjalëkalim krijuar posaçërisht qasje të sigurt.

(3) NPRRSG miraton një procedurë të brendshme që përshkruan në mënyrë të detyrueshme mënyrën e menaxhimit të çelësave dhe certifikatave sekrete, duke marrë parasysh menaxhimin e rrezikut të fjalëkalimeve të harruara.

Siguria fizike e sistemit të informacionit

Neni 21

(1)Serverët në të cilët janë instaluar programet softuerike për përpunimin e të dhënave personale janë të vendosur fizikisht, të hostifikuara dhe të administruar nga NPRRSH.

(2) NPRRSH siguron një nivel të përforcuar sigurie në lidhje me ambientet në të cilat ndodhen dhe ruhen serverat dhe pajisjet e rrjetit përmes të cilave kryhet përpunimi i të dhënave personale edhe atë:

-Qasja fizike në një hapësirë ku ndodhen serverat kanë vetëm persona të autorizuar në mënyrë specifike nga Drejtori i NPRRSH-së.

- Hapësira në të cilën ndodhen serverat mbrohet nga rreziqet duke zbatuar masa dhe kontrolle për parandalimin e vjedhjes, zjarrit, shpërthimeve, tymit, ujit, pluhurit, dridhjeve, ndikimeve kimike, ndërhyrjes në furnizimin me energji elektrike dhe rrezatimit elektromagnetik;

- nëse një person tjetër ka nevojë për qasje në hapësirat dhe të dhënat personale të ruajtura në server, atëherë ai person do të shoqërohet dhe mbikëqyret nga personi i autorizuar nga Drejtori i NPRRSH.

- lista e azhuruar e personave ose kategorive të personave të autorizuar për të hyrë në hapësirat ku ruhen pajisjet në të cilat kryhet përpunimi i të dhënave personale;

- mirëmbajtjen e hapësirave të serverit (ajër të kondicionuar, UPS, etj.).

- mbajtjen e evidencës të qasjes në hapësirat ku ruhen serverët që përmbajnë të dhëna personale;

(2) Me përjashtim të paragrafit 1 të këtij neni, serverët në të cilët janë instaluar programet softuerike për përpunimin e të dhënave personale mund të vendosen fizikisht, të hostifikoen dhe të administrohen jashtë hapësirave të kontrollorit.

(3) Në rastin e përmendur në paragrafin (2) të këtij neni, të drejtat dhe detyrimet e ndërsjella të NPRRSH dhe personit juridik ose fizik me të cilin serverët janë fizikisht të vendosur, të hostifikuar dhe të administruar do të rregullohen me një marrëveshje me shkrim, e cila do të përmbajë domosdoshmërisht masa për sigurinë e të dhënave personale në përputhje me rregullativat për mbrojtjen e të dhënave personale.

Kontrolli i sistemit të informacionit dhe infrastrukturës së informatikës

Neni 22

(1) Zyrtari për mbrojtjen e të dhënave personale kryen kontrolle periodike për të monitoruar harmonizimin e punës të kontrolluesit me rregullativat për mbrojtjen e të dhënave personale dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

(2) Sistemi i informacionit dhe infrastruktura e informatikës e NPRRSH duhet t 'i nënshtrohen kontrollit të brendshëm vjetor me qëllim të kontrollimit nëse zbatohen procedurat dhe udhëzimet që përmbahen në (masat teknike dhe organizative të cilat zbatohen) rregullat dhe politikat për sigurinë e të dhënave personale dhe janë në përputhje me rregullativat për mbrojtjen e të dhënave personale.

Menaxhimi me përpunuesit

Neni 23

(1) NPRRSH siguron mbrojtjen e të dhënave personale në formë elektronike në shkëmbimin e tyre me subjektet e jashtme, nëpërmjet sistemeve të sigurisë duke siguruar një lidhje të koduar për shkëmbimin e rregullave strikte për identifikimin gjatë shkëmbimit.

(2) Të drejtat dhe detyrimet e ndërsjella të NPRRSH dhe përpunuesit duhet të rregullohen me një marrëveshje me të cilën NPRRSH, para lidhjes së marrëveshjes, është e detyruar t 'i kërkojë nga përpunuesit (ofruesit të shërbimit) të paraqesë politikën e saj të sigurisë në lidhje me sistemin e informacionit dhe infrastrukturën e informatikës në të cilën përpunimi i të dhënave personale do të kryhet në emër të kontrolluesit.

Politika e sigurisë e përmendur në paragrafin (2) të këtij neni duhet të përmbajë të dhëna që garantojnë sigurinë e të dhënave personale, edhe atë:

- nëse dhe si të dhënat janë tëkriptohen sipas ndjeshmërisë së tyre;
- ekzistencën e procedurave për të siguruar që askush të mos ketë qasje të paautorizuar në të dhëna;
- nëse dhe si kryhet kriptimi i transmetimit të të dhënave;
- garancitë në lidhje me gjurmueshmërinë (loget);
- menaxhimin e të drejtave të qasjes;
- autentifikimi; dhe
- masa të tjera sigurie për përpunimin e të dhënave personale.

(4) Marrëveshja e përmendur në paragrafin (2) të këtij neni do të përmbajë dispozita në veçanti për:

- lëndën, kohëzgjatjen dhe qëllimin e përpunimit të të dhënave personale;
- detyrimet e përpunuesit për të ndërmarrë masa teknike dhe organizative për të siguruar sigurinë e përpunimit të të dhënave personale;
- detyrimet në lidhje me konfidencialitetin e të dhënave personale të besuara;
- standardet minimale për autentifikimin e personave të autorizuar;
- kushtet për kthimin e të dhënave dhe/ose shkatërrimin e tyre pas skadimit ose prishjes së kontratës;
- rregullat për menaxhimin dhe njoftimin e kontrolluesit në rast të incidenteve, përkatësisht në rast të shkeljes së sigurisë së të dhënave personale;
- detyrimet e përpunuesit për të vepruar vetëm në përputhje me udhëzimet e marra nga kontrolluesi; dhe

- detyrime dhe përgjegjësi të tjera në përputhje me rregullativat për mbrojtjen e të dhënave personale dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

2. Masat organizative

Neni 24

(1) NPRRSH do të zbatojë masat e duhura organizative për fshehtësinë dhe mbrojtjen e të dhënave personale edhe atë:
1. qasja ose identifikimi i kufizuar për qasje në të dhënat personale;
2. shkatërrimin e dokumenteve pas skadimit të afatit për ruajtjen e tyre;
3. masat për sigurinë fizike të ambienteve të punës dhe pajisjeve të informacionit dhe komunikimit, mbi të cilat përpunohen të dhënat personale;
4. respektimi i udhëzimeve teknike gjatë instalimit dhe përdorimit të informacionit-pajisjet e komunikimit në të cilat përpunohen të dhënat personale.
(2) Personi i punësuar në njësinë organizative për resurset njerëzore në NPRRSH, nëpërmjet personit udhëheqës në institucion, informon administratorin e sistemit të informacionit për punësimin ose angazhimin e çdo personi të autorizuar me të drejtë qasje në sistemin e informacionit, që të ju caktohet një emër përdoruesi dhe fjalëkalim, si dhe për ndërprerjen e punës ose angazhimin për të fshirë emrin e përdoruesit dhe fjalëkalimin e tij, përkatësisht e mbyllur për qasje të mëtejshme. Njoftimi do të bëhet me shkrim.
(3) Njoftimi i përmendur në paragrafin (2) të këtij neni do të bëhet gjithashtu në rast të ndonjë ndryshimi tjetër në statusin e punës ose statusin e angazhimit të personit të autorizuar që ka ndikim në nivelin e qasjes së lejuar në sistemin e informacionit.

Informimi dhe edukimi për mbrojtjen e të dhënave personale

Neni 25

(1) Personat të cilët janë të punësuar ose të angazhuar në NPRRSH, përpara se të fillojnë punën e tyre, njihen me rregullativat për mbrojtjen e të dhënave personale, si dhe me dokumentacionin e miratuar për masat teknike dhe organizative.
(2) Për personat të cilët janë të angazhuar për kryerjen e punëve në NPRRSH në kontratën për angazhimin e tyre, theksohen detyrimet dhe përgjegjësitë për mbrojtjen e të dhënave personale.
(3) Para fillimit të menjëhershëm të punës së personave të autorizuar, një person përgjegjës nga Departamenti për menaxhimin me resurset njerëzore në mënyrë shtesë do t 'i informojë për detyrimet dhe përgjegjësitë e menjëhershme për mbrojtjen e të dhënave personale.

(4) Personat të cilët janë të punësuar ose të angazhuar te kontrolluesi, para fillimit të punës së tyre, nënshkruajnë një deklaratë të fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale.
(5) Deklarata nga paragrafi (4) i këtij neni veçanërisht përmban: se personat do të respektojnë parimet e mbrojtjes së të dhënave personale para qasjes së tyre në të dhënat personale; do të përpunojnë të dhënat personale në përputhje me udhëzimet e marra nga Kontrollori, përveç nëse rregullohet ndryshe me ligj, dhe do t'i mbajnë konfidenciale të dhënat personale, si dhe masat për mbrojtjen e tyre.
(6) Deklarata nga paragrafi (4) i këtij neni duhet të ruhet në dosjet e personave që janë të punësuar ose të angazhuar te Kontrolluesi.
(7) NPRRSH është e detyruar të informojë dhe edukojë vazhdimisht udhëheqësinë dhe personat e autorizuar për detyrimet dhe përgjegjësitë e menjëhershme për mbrojtjen e të dhënave personale.

Qasja në dokumente

Neni 26

(1) Qasja në dokumente duhet të jetë e kufizuar për personat e autorizuar në NPRRSH.
(2) Për qasje në dokumente bëhet identifikimi i personave të autorizuar dhe për kategoritë e të dhënave personale në të cilat bëhet qasja dhe mbahet evidencë e qasjeve.
(3) Qasja e personave të paautorizuar në dokumente duhet të shoqërohet nga një person i cili është i autorizuar për qasje në dokumente.

Rregulla "tavolinë e pastër"

Neni 27

NPRRSH zbaton detyrimisht rregullën e “tavolinës së pastër” gjatë përpunimit të të dhënave personale të përfshira në dokumente për mbrojtjen e tyre gjatë gjithë procesit të përpunimit nga qasja e personave të paautorizuar.

Ruajtja e dokumenteve

Neni 28

Ruajtja e dokumenteve duhet të bëhet në atë mënyrë që të zbatohen mekanizmat e duhur për të parandaluar çdo hapje të paautorizuar.

Shkatërrimi i dokumenteve

Neni 29

(1) Shkatërrimi i dokumenteve bëhet me copëtim ose në një mënyrë tjetër, ku ato nuk mund të përdoren më.
(2) Në rastin e paragrafit (1) të këtij neni, komisioni përpilon një procesverbal që përmban të gjitha të dhënat për identifikimin e plotë të dokumentit si dhe për kategoritë e të dhënave personale që gjenden në të njëjtin.

Mënyra e ruajtjes së dokumenteve

Neni 30

Dollapët (vitrinat), kartotekat e dosjeve ose pajisje të tjera për ruajtjen e dokumenteve duhet të vendosen në hapësira të mbyllura me mekanizma të përshtatshme mbrojtëse. Hapësirat duhet të jenë të mbyllura edhe për periudhën kur dokumentet nuk përpunohen nga personat e autorizuar.

NIVEL I LARTË

1. Masat teknike

Menaxhimi i fjalëkalimeve

Neni 31

NPRRSH përdor dhe siguron që fjalëkalime të ndryshme për çdo shërbim, ose program softuerik të ruhen siç duhet, ashtu që përshkruan një Politikë të menaxhimit të fjalëkalimeve.

Menaxhimi me mediat portative

Neni 32

(1) NPRRSH-ja krijon sistem për regjistrimin e mediumeve të cilat pranohen me qëllim të mundësimit të identifikimit të drejtpërdrejtë ose të tërthortë të llojit të mediumit të pranuar, datës dhe kohës së pranimit, dërguesit, numrit të mediumeve të cilat janë të pranuara, llojit të dokumentit të regjistruar në medium, mënyrës së dërgimit të mediumit, emri dhe mbiemri i personit të autorizuar për pranimin e mediumit.

(2) Për mediat e transferuara jashtë ambienteve të punës së kontrolluesit, duhet të ndërmerren masat e nevojshme për parandalimin e përpunimit të paautorizuar të të dhënave personale të regjistruara në to.

Testimi i sistemit të informacionit

Neni 33

(1) NPRRSH-ja kryen testimin e detyrueshëm të sistemit të informacionit para zbatimit të tij ose pas ndryshimeve të bëra me qëllim verifikimin nëse sistemi siguron sigurinë e të dhënave personale në përputhje me rregullativat për mbrojtjen e të dhënave personale.
(2) Testimi i përmendur në paragrafin (1) të këtij neni do të kryhet përmes përpunimit të dokumenteve që përmbajnë të dhëna imagjinare personale.

Transmetimi i medias

Neni 34

Media mund të transferohet jashtë ambienteve të punës vetëm nëse të dhënat personale janë të koduara ose të mbrojtura me metoda të përshtatshme që sigurojnë që të dhënat nuk do të jenë të lexueshme, ku vetëm administratori i sistemit të informacionit mund t 'i dekriptojë ato ose një person i autorizuar prej tij.

Transferimi i të dhënave personale përmes një rrjeti të komunikimit elektronik

Neni 35

Të dhënat personale mund të transmetohen përmes rrjetit të komunikimit elektronik vetëm nëse ato janë të koduara ose nëse mbrohen në mënyrë specifike me metoda të përshtatshme që sigurojnë që të dhënat nuk do të jenë të lexueshme gjatë transmetimit.

2. Masat organizative

Kopjimi ose shumëzimi i dokumenteve

Neni 36

Kopjimi ose shumëzimi i dokumenteve mund të kryhet vetëm nga persona të autorizuar të caktuar me autorizim paraprak me shkrim nga ana e Drejtorit të NPRRSH-së dhe në përputhje me procedurat që duhet të përcaktojnë masat dhe mënyrën e kopjimit dhe shumëzimit të dokumenteve.

(2) Shkatërrimi i kopjeve ose dokumenteve të shumëzuara duhet të kryhet në një mënyrë që e bën të pamundur ripërtrirjen e mëtutjeshme të të dhënave personale të përmbajtura.

Transferimi i dokumenteve

Neni 37

Në rast të transferimit fizik të dokumenteve, kontrollori merr detyrimisht masa për t'i mbrojtur ato nga qasja ose përdorimi i paautorizuar i të dhënave personale që gjenden në dokumentet që transferohen.

V. DISPOZITAT KALIMTARE DHE PËRFUNDIMTARE

Ndërprerja e vlefshmërisë

Neni 38

Në ditën e hyrjes në fuqi të këtyre Rregullave, ndërpritet të vlejë Rregullorja për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale në Ndërmarrjen Publike për Rrugë Shtetërore me nr. 02-7926/15 të datës 17.10.2014.

Neni 39

Kjo rregullore hyn në fuqi në ditën e miratimit të tij dhe e njëjta publikohet në UEB faqen e NPRRSH.

Zëvendëskryetar i Bordit Drejtues

Bllazhena Pejovska