

**RREGULLORE PËR MASAT TEKNIKE DHE ORGANIZATIVE PËR
SIGURIMIN E FSHEHTËSISË, MBROJTJES DHE SIGURISË SË PËRPUNIMIT
TË TË DHËNAVE PERSONALE NË
IK Kinoteka e Republikës së Maqedonisë së Veriut**

Përmbajtja

Dispozitat e përgjithshme	3
Parimet themelore për përpunim të drejtë dhe të ligjshëm	3
Ligjshmëria e përpunimit	4
Sistemi i mbrojtjes së të dhënave personale	7
Siguria fizike	10
Lidhja me rrjet dhe komunikimi	11
Shërbimet e internetit	12
Sigurimi i serverëve dhe kompjuterëve personal ku bëhet përpunimi i të dhënave personale	13
Menaxhimi i përdoruesve	14
Menaxhimi i fjalëkalimeve	15
Sistemi i monitorimit dhe kontrollit	16
Plani i vazhdimësisë dhe kopjeve të sigurimit	17
Enkriptimi	19
Sigurimi i medimeve portative	19
Ballafaqimi me incidente	20
Menaxhimi i përpunuesve	20
Ruajtja e dokumentacionit-rregulli tavolina e pastër	21
Afatet për ruajtjen e të dhënave personale	22
Testimi (Niveli i lartë)	22
Kontrolli periodik	22
Dispozitat përmbyllëse	23

Në bazë të Ligjit për Mbrojtjen e të Dhënave Personale (Gazeta Zyrtare nr. nr. 42/20) dhe Rregulloren për sigurinë e përpunimit të të dhënave personale ("gaz. zyrtare nr. 122/2020) IK Kinoteka e Republikës së Maqedonisë së Veriut e miratoi

**RREGULLOREN PËR MASAT TEKNIKE DHE ORGANIZATIVE PËR SIGURIMIN E FSHEHTËSISË,
mbrojtje dhe siguri të përpunimit të të dhënave personale
IK Kinoteka e Republikës së Maqedonisë së Veriut**

Dispozitat e përgjithshme

Neni 1

Rregullorja për masat teknike dhe organizative për të siguruar fshehtësinë, mbrojtjen dhe sigurinë e përpunimit të të dhënave personale (në tekstin e mëtejshëm: Rregullorja) e IK Kinoteka e Republikës së Maqedonisë së Veriut (në tekstin e mëtejshëm: Kinoteka) përshkruan masat teknike dhe organizative për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale.

Neni 2

Rregullorja përcakton parimet dhe përcakton kornizën e masave dhe përgjegjësi në fushën e mbrojtjes së të dhënave personale në fazat e mbledhjes, ruajtjes, përpunimit, transferimit, arkivimit dhe shkatërrimit të tyre në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale (LPRDHP) dhe rregulloret përkatëse të Agjencisë për Mbrojtjen e të Dhënave Personale.

Neni 3

Rregullorja zbatohet dhe përdoret në të gjitha pjesët organizative të Kinotekës dhe vlen për të gjithë punonjësit, personat e punësuar, praktikantët dhe palët e jashtme/të treta.

Punonjësit me publikimin e kësaj Rregullore konsiderohen të njohur dhe të vetëdijshëm për detyrimet e përcaktuara në të.

Neni 4

Dispozitat e kësaj Rregullore zbatohen për:

- përpunim të plotë dhe të pjesshëm të automatizuar të të dhënave personale;
- përpunim tjetër të të dhënave personale që janë pjesë e një përmbledhje ekzistues të të dhënave personale ose kanë për qëllim të jenë pjesë e një përmbledhje të të dhënave personale.

Parimet themelore për përpunimin e drejtë dhe të ligjshëm

Neni 5

Në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale (Ligji për Mbrojtjen e të Dhënave Personale) dhe Rregulloren e Përgjithshme Evropiane të Mbrojtjes së të Dhënave (GENERAL DATA PROTECTION REGULATION GDPR), si vlerë themelore janë përcaktuar parimet e mëposhtme të mbrojtjes së të dhënave:

- Të dhënat personale mbledhen dhe përpunohen në baza ligjore, në mënyrë transparente (informim paraprak) dhe duke respektuar rregullat për përpunimin e të dhënave të ndjeshme (të dhënat personale

që zbulojnë origjinën racore ose etnike, përkatësinë politike, përkatësinë fetare ose filozofike, anëtarësimin në sindikata dhe përpunimin e të dhënave për gjendjen shëndetësore ose jetën seksuale).

- Të dhënat personale përpunohen në përputhje me ligjin, në masë të mjaftueshme dhe në mënyrë transparente në lidhje me subjektin e të dhënave personale ("ligjshmëria, drejtësia dhe transparenca"),
- Të dhënat personale grumbullohen për qëllime konkrete, të qarta dhe legjitime dhe nuk do të përpunohen në mënyrë që nuk përputhet me ato qëllime.
- Të dhënat personale janë adekuate, relevante dhe të kufizuara në atë që është e nevojshme në lidhje me qëllimet për të cilat ato përpunohen ("vëllimi minimal i të dhënave"),
- Të dhënat personale janë të sakta dhe kur është e nevojshme të përditësuara, duke marrë të gjitha masat e duhura për të fshirë ose korrigjuar menjëherë të dhënat që janë të pasakta ose jo të plota, duke marrë parasysh qëllimet për të cilat janë përpunuar ("saktësia"),
- Të dhënat personale janë të ruajtura në formë që lejon identifikimin e subjekteve të të dhënave personale, jo më gjatë se sa është e nevojshme për qëllimet për të cilat përpunohen të dhënat personale. Të dhënat personale mund të ruhen më gjatë se periudha e mbajtjes së tyre nëse ato përpunohen për qëllime statistikore, përgatitjen e raporteve, përmbushjen e detyrimeve ligjore të Kontrolluesit, si dhe duke zbatuar masat e duhura teknike dhe organizative në përputhje me këtë ligj, me qëllim mbrojtjen e të drejtave dhe lirive të subjektit të të dhënave personale ("kufizimi i periudhës së ruajtjes").
- Të dhënat personale janë të përpunuara në mënyrë që siguron nivel të përshtatshëm të sigurisë së të dhënave personale, duke përfshirë mbrojtjen nga përpunimi i paautorizuar ose i paligjshëm, si dhe humbjen, shkatërrimin ose dëmtimin aksidental të tyre, duke zbatuar masat e duhura teknike ose organizative ("integriteti dhe besueshmëria").
- Janë ndërmarrë masat e duhura teknike dhe organizative për të mbrojtur nga përpunimi i paautorizuar ose i paligjshëm i të dhënave personale dhe për të parandaluar humbjen aksidentale, shkatërrimin ose dëmtimin e të dhënave personale.
- Të dhënat personale nuk do të transferohen në vende ose territor jashtë Bashkimit Evropian ose Komunitetit Ekonomik Evropian, nëse ai vend ose territor nuk siguron një nivel adekuat të mbrojtjes së të drejtave dhe lirive të subjekteve në lidhje me përpunimin e të dhënave personale.

Neni 6

Për të arritur këto qëllime themelore, Kinoteka, si Kontrolluese, zhvillon dhe mirëmban sistem të kontrolleve të brendshme me masat e duhura organizative dhe teknike në përputhje me Ligjin për mbrojtjen e të dhënave personale, Rregulloret shoqëruese si dhe praktikrat dhe standardet përkatëse më të mira.

Ligjshmëria e përpunimit

Neni 7

Në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale, Kinoteka respekton plotësisht ligjshmërinë e mbledhjes dhe përpunimit të të dhënave personale, duke përmbushur të paktën një nga kushtet e mëposhtme:

- subjekti i të dhënave personale ka dhënë pëlqimin e qartë dhe eksplisit për përpunimin e të dhënave të tija personale për një ose më shumë qëllime konkrete,

– përpunimi është i nevojshëm për të përmbushur një kontratë ku subjekti i të dhënave personale është palë kontraktuese ose për të ndërmarrë aktivitete me kërkesë të subjektit të të dhënave personale para hyrjes të tij/saj në kontratë,

- përpunimi është i nevojshëm për përmbushjen e një detyrimi ligjor të kontrolluesit, - përpunimi është i nevojshëm për mbrojtjen e interesave thelbësore të subjektit të të dhënave personale ose të një personi tjetër fizik,

– përpunimi është i nevojshëm për kryerjen e punëve me interes publik ose në ushtrimin e autoritetit publik të kontrolluesit të përcaktuar me ligj,

– përpunimi është i nevojshëm për qëllime të interesave legjitime të kontrolluesit ose të një pale të tretë, përveç kur këto interesa nuk mbizotërojnë mbi interesat ose të drejtat dhe liritë themelore të subjektit të të dhënave personale që kërkojnë mbrojtjen e të dhënave personale, në veçanti kur subjekti i të dhënave personale është fëmijë.

Neni 8

Kinoteka mbledh dhe përpunon NVAQ (Numrin e Vetëm Amë të Qytetarit) në kushtet e mëposhtme:

- nëse është marrë pëlqimi paraprak i subjektit të të dhënave personale;
- për ushtrimin e të drejtave ose detyrimeve të Kontrolluesit ose subjektit të të dhënave personale të përcaktuara me ligj;
- raste të tjera të përcaktuara me ligj;

Kinoteka do të marrë masat e nevojshme që NVAQ të mos jetë i dukshëm pa nevojë dhe i ekspozuar gjatë përpunimit, transmetimit dhe ruajtjes, në përputhje me udhëzimet e përpunimit të përfshira në Rregulloren për Regjistrimet e Përpunimit të Koleksioneve me Rrezik të Lartë.

Neni 9

Kinoteka si Kontrollor nuk do të mbledhë dhe përpunojë kategori të veçanta të të dhënave personale.

Me përjashtim, përpunimi i kategorive të veçanta të të dhënave personale do të kryhet nëse:

- është marrë pëlqim i qartë i subjektit të të dhënave personale për përpunimin e këtyre të dhënave, në rast se ligji parashikon që ndalimi i përpunimit të këtyre të dhënave nuk mund të hiqet me pëlqimin e subjektit të të dhënave personale;
- për përmbushjen e të drejtave dhe detyrimeve të veçanta në fushën e së drejtës së punës, brenda fushës së veprimit dhe mbrojtjes së përshtatshme të përcaktuar me ligj në atë fushë.
- kur është e nevojshme të mbrohet subjekti i të dhënave ose një person tjetër, nëse ky i fundit ka pengesa që e pengojnë atë të japë pëlqimin ose është i paaftë për punë dhe për të dhënë pëlqimin.
- përpunimi u referohet të dhënave që subjekti i të dhënave personale i ka bërë publike.

Neni 10

Kinoteka si Kontrollues respekton plotësisht të drejtat, liritë dhe interesat legjitime të subjektit në mbledhjen dhe përpunimin e të dhënave personale, në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale:

- ✓ e drejta e informimit transparencës (neni 16)
- ✓ e drejta e qasjes në të dhënat personale (neni 19),
- ✓ e drejta për korrigjim (neni 20),
- ✓ e drejta e fshirjes (neni 21),
- ✓ e drejta e kufizimit të përpunimit (neni 22),
- ✓ e drejta e bartjes (neni 23),
- ✓ e drejta e ankesës (neni 24) dhe
- ✓ e drejta për të mos iu nënshtruar një vendimi të bazuar vetëm në përpunimin e automatizuar, duke përfshirë profilizimin (neni 25).

Neni 11

Parimi i llogaridhënies dhe transparencës është parimi themelor i çdo sistemi të mbrojtjes së të dhënave personale.

Kinoteka në faqen e saj të internetit si Kontrollues ka krijuar një Politikë të Privatësisë dhe informacione kontakti në dispozicion të publikut me Kontrolluesin dhe Zyrtarin për Mbrojtjen e të Dhënave Personale me udhëzime të qarta për informim transparent dhe ushtrimin e të drejtave të subjekteve të të dhënave personale në përputhje me Ligjin për mbrojtjen e të dhënave personale.

Neni 12

Si Kontrollues në kohën e mbledhjes së të dhënave personale, i siguron subjektit të të dhënave personale informacionin e mëposhtëm:

- identitetin dhe detajet e kontaktit të kontrolluesit dhe detajet e përfaqësuesit të tij të autorizuar në Republikën e Maqedonisë së Veriut;
- të dhënat e kontaktit për Zyrtarin për Mbrojtjen e të Dhënave Personale;
- qëllimet e përpunimit për të cilat synohen të dhënat personale, si dhe bazën ligjore për përpunimin;
- interesat legjitime që i zbaton kontrolluesi ose një palë e tretë
- përdoruesit ose kategoritë e përdoruesve të të dhënave personale, nëse ka;
- kur është e zbatueshme, fakti që kontrolluesi synon të transferojë të dhënat personale në një vend të tretë ose organizatë ndërkombëtare, duke iu referuar masave mbrojtëse të përshtatshme ose të pranuar dhe mjeteve për të marrë një kopje të tyre ose informacione ku ato janë të kapshme.

Neni 13

Me kërkesë të subjektit të të dhënave personale, Kinoteka i paraqet kërkuarit informacion mbi masat dhe aktivitetet që ndërmerr dhe në bazë të neneve 19 deri në 25 të Ligjit për Mbrojtjen e të Dhënave Personale, pa vonesë të panevojshme brenda një muaji nga dita e marrjes së kërkesës.

Nëse është e nevojshme, ky afat mund të shtyhet me dy muaj të tjerë, duke marrë parasysh kompleksitetin dhe numrin e kërkesave. Kontrolluesi do të informojë subjektin e të dhënave personale për çdo zgjatje brenda një muaji nga data e marrjes së kërkesës, së bashku me arsyen e shtyrjes.

Neni 14

Kërkesat në lidhje me ushtrimin e të drejtave të tyre sipas nenit 19-25 mund të bëhen nga subjektet e të dhënave personale nëpërmjet:

- emailit të zyrtarit
- Nëpërmjet dorëzimit me postë me emërtimin e *Zyrtarit për Mbrojtjen e të Dhënave Personale*
- Nëpërmjet dorëzimit të drejtpërdrejtë në Arkiv në Zyrën Qendrore me emërtimin *për Zyrtarin për Mbrojtjen e të Dhënave Personale*

Sistemi i mbrojtjes së të dhënave personale

Neni 15

Siguria e të dhënave personale është një çështje shumë më e gjerë sesa zbatimi i thjeshtë i masave të duhura teknike dhe organizative. Siguria është parakusht për arritjen e pajtueshmërisë me të gjitha parimet e tjera të përpunimit të të dhënave personale.

Kinoteka ka krijuar një sistem masash organizative dhe teknike në përputhje me Rregulloren për Sigurinë e Agjencisë për Mbrojtjen e të Dhënave Personale.

Siguria e të dhënave personale sigurohet përmes përbushjes së attributeve të mëposhtme:

- Fshehtësia (ang. Confidentiality):** Të dhënat janë në dispozicion vetëm për ata që kanë qasje të autorizuar në to;
- **Integriteti (ang. Integrity):** Mbrojtja e saktësisë dhe konsistencës së informacionit dhe metodave të përpunimit;
- Disponueshmëria (ang. Availability):** Përdoruesit e autorizuar kanë qasje në informacionin dhe mjetet e tjera shoqëruese të nevojshme për paraqitjen e tij, kur për të ka nevojë biznesi;
- **Padiskutueshmëria (Ing. Non-Repudiation):** Vërtetim dhe pakundërshtueshmëri e aktiviteteve që lidhen me qasjen dhe përdorimin e të dhënave;
- **Llogaridhënia (ang. Accountability):** Aktivitetet që lidhen me përdorimin dhe qasjen në të dhëna mund të shënohen dhe regjistrohen në mënyrë unike.

Neni 16

Sipas arritjeve më të fundit teknologjike, kostove të zbatimit dhe natyrës, fushëveprimit, kontekstit dhe qëllimeve të përpunimit, si dhe rreziqeve me shkallë të ndryshme probabiliteti dhe serioziteti për të drejtat dhe liritë e personave fizikë, Kinoteka krijon një sistem për mbrojtjen e të dhënave personale duke zbatuar masat e duhura teknike dhe organizative për të siguruar një nivel sigurie të përshtatshëm për rrezikun.

sistemi për mbrojtjen e të dhënave personale mbulon fushat e mëposhtme:

- Vlerësimi i nivelit të rrezikut të mbuluar në Metodologjinë e Vlerësimit të Ndikimit, në përputhje me nenin 39 të Ligjit për Mbrojtjen e të Dhënave Personale.

Në përcaktimin dhe vlerësimin e rrezikut (menaxhimi i rrezikut), merr parasysh rreziqet që lidhen me përpunimin, veçanërisht nga shkatërrimi aksidental ose i paligjshëm, humbja, ndryshimi, zbulimi i

paautorizuar i të dhënave personale ose qasja e paautorizuar në të dhënat personale të transmetuara, të ruajtura ose të përpunuara ndryshe.

- Zbatimi i një sistemi të përshtatshëm të kontrolleve që ndahen në
 - Kontrollët fizike, që shërbejnë për të siguruar sigurinë fizike adekuate të informacionit dhe mjeteve informative (serverët, pajisjet e rrjetit).

Shembuj të kontrolleve fizike janë përdorimi i pajisjeve të furnizimit me energji elektrike të pandërprerë. Ups), shërbimi i rojës, sensorë dhe alarme, dhe masa të ngjashme për të kontrolluar qasjen fizike dhe për të mbrojtur burimet dhe pasuritë që përdoren për përpunimin, transferimin dhe ruajtjen e të dhënave personale.

– Kontrollët teknike, janë kontrollë që janë të integruara në mjetet e informacionit, gjegjësisht softueri i aplikimit, pajisjet e rrjetit dhe komunikimit dhe pajisjet shoqëruese. Kontrollët teknike ndryshe quhen edhe kontrollë logjike.

– Kontrollët administrative, duke përfshirë përcaktimin e procedurave dhe udhëzimeve, për autorizimin e përdoruesve (punonjësve, palëve të treta) që kanë qasje në sistemin e informacionit, duke u lejuar atyre autorizimin e nevojshëm për të kryer proceset e tyre të biznesit dhe duke pasur një pasqyrë të qartë të aktiviteteve në drejtim të sigurimit të një sistemi informacioni më të besueshëm.

- Zbatimi i parimit të mbrojtjes së të dhënave personale by design ose by default, në përputhje me nenin 10, III. Niveli standard, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Sipas këtij parimi, masat e duhura teknike dhe organizative janë përfshirë në procesin e përpunimit të të dhënave personale në momentin e përcaktimit të mjeteve të përpunimit. Ky parim zbatohet edhe për aktivitetet rrjedhëse dhe mjetet e përpunimit, për të siguruar kontrolluesi se në mënyrë efektive përballet me jetëgjatësinë e të dhënave personale që përpunon.

Neni 17

Duke marrë parasysh natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit, si dhe rreziqet me probabilitet dhe ashpërsi të ndryshme për të drejtat dhe liritë e personave fizikë, kontrolluesi është i detyruar të zbatojë një nivel të përshtatshëm masash teknike dhe organizative që do të jenë proporcionale me aktivitetet e përpunimit të të dhënave personale.

Masat teknike dhe organizative mund të klasifikohen në dy nivele:

- -standarde dhe
- I lartë

Neni 18

Kinoteka zbaton nivelet e mëposhtme të masave teknike dhe organizative të nivelit standard, në përputhje me nenin 10, III. Niveli standard, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

- Siguria fizike e kompjuterit dhe pajisjeve të tjera të përdorura për përpunimin e të dhënave personale
- Metodot e duhura të autentifikimit dhe regjistrimit të përdoruesve që hyjnë në sistemin kompjuterik;
- Politikat dhe rregullat adekuate për menaxhimin e fjalëkalimeve;

- Çlajmërim i automatizuar i sistemit të informacionit pas kalimit të një periudhe të caktuar prej 15 minutash joaktiviteti dhe për riaktivizimin e sistemit kërkohet shënimi i sërishëm i emrit të përdoruesit dhe fjalëkalimi;
- Pengesë e instaluar e rrjetit mbrojtës të harduerit/softuerit (ang. Firewall”) dhe ruterin midis sistemit të informacionit dhe internetit ose çdo forme tjetër të rrjetit të jashtëm, si masë mbrojtëse kundër përpjekjeve të paautorizuara ose qëllimkëqia për të hyrë ose thyer sistemin;
- mbrojtje e besueshme anti-virus dhe anti-spyware e sistemit të informacionit, i cili do të përditësohet vazhdimisht për parandalimin e kërcënimeve të panjohura dhe të paplanifikuara nga viruset dhe spyware të reja;
- Mbrojtje efektive dhe e besueshme anti-spam e sistemit të postës elektronike , i cili azhurnohet vazhdimisht për mbrojtje parandaluese kundër spam dhe kodeve të tjera të këqija;
- Lidhja e kompjuterit dhe pajisjeve të tjera me një rrjet energjie përmes një pajisjeje për furnizim të pandërprerë me energji elektrike;
- Sigurimi i një vendi të përshtatshëm për ruajtjen e kopjeve (backup) të të dhënave personale në një formë të mbrojtur;
- Sigurimi i një lokacioni për rikuperim nga fatkeqësi (disasret recovery location), ku bëhet përsëritje e të dhënave nga serverët e lokacionit primar dhe që janë përfshirë file server, e-mail server, web server etj.
- Proces për zbulimin dhe menaxhimin efektiv me incidente të sigurisë;
- Menaxhimi i mediave portative;

Neni 19

Kinoteka zbaton nivelet e mëposhtme të masave teknike dhe organizative të nivelit të lartë, në përputhje me pjesën IV. Niveli i lartë nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

- Menaxhimi i fjalëkalimeve – në lidhje me mbrojtjen dhe keqpërdorimin e sistemit të ruajtjes dhe përdorimit të fjalëkalimeve (password hashing), në përputhje me nenin 38, IV. Niveli i lartë, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.
- Menaxhimi i mediave portative - përmes përdorimit të metodave të përshtatshme të mbrojtjes (kriptimit) që sigurojnë që të dhënat nuk do të jenë të lexueshme nga persona të paautorizuar, siç është përdorimi i një mjeti për moskriptimin e disqeve në kompjuterë portativë (notebook), në përputhje me nenin 40, IV. Niveli i lartë, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.
- Testimi i sistemit të informacionit - futja e praktikës për testimin e rregullt të pavarur dhe profesional (siç është hakimi etik) të mekanizmave dhe kontroleve për mbrojtjen e të dhënave dhe kërcënimit kibernetik, në përputhje me nenin 41, IV. Niveli i lartë, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.
- Transmetimi i të dhënave personale përmes rrjetit të komunikimit elektronik duke përdorur metodat e duhura të enkriptimit dhe mbrojtjes, në përputhje me nenin 44, IV. Niveli i lartë, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Neni 20

Për të gjitha përmbledhjet, Kinoteka duhet të zbatojë masa teknike dhe organizative që klasifikohen në nivel standard.

Neni 21

Për përmbledhjet që përmbajnë: kategori të veçanta të të dhënave personale, të dhënat personale që përpunohen me qëllim mbrojtjen e sigurisë dhe interesave të shtetit, janë të detyrueshme masat teknike dhe organizative që klasifikohen në nivel standard dhe nivelit të lartë.

Për përmbledhjet që përmbajnë numrin amë të qytetarit, është e detyrueshme të zbatohen masa teknike dhe organizative që klasifikohen në nivel standard dhe nivelit të lartë.

Siguria fizike

Neni 22

Kinoteka ofron kushte të përshtatshme për mbrojtjen fizike të sistemeve kompjuterike të përdorura për përpunimin, ruajtjen ose shpërndarjen e të dhënave personale.

Kontrollet e sigurisë fizike në kuptim të kësaj Rregulloreje nënkuptojnë masat e duhura për të kufizuar dhe kontrolluar qasjen fizike dhe përdorim të informacionit dhe mjeteve të informacionit, për mbrojtje nga ndikimet dhe dëmtimet e jashtme si zjarri, përmytja, lagështia, energjia elektrike, vandalizmi dhe sabotimi.

Neni 23

Kinoteka përcakton perimetrin e sigurisë fizike ose zonat e sigurisë për të mbrojtur fizikisht mjetet informative në përputhje me nenin 26, Siguria fizike e Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Qasja fizike kontrollohet në mënyrë të përshtatshme dhe lejohet vetëm për personat e autorizuar – punonjësit dhe/ose palët e treta.

Punonjësve u jepet qasje në ambiente në përputhje me pozicionet e tyre të punës dhe përgjegjësitë që lidhen me përmbushjen e detyrave të tyre të punës.

Neni 24

Salla e Sistemit është një kategori e veçantë e zonës së sigurisë me shkallën më të lartë të kufizimit për hyrje dhe mbrojtje.

Rregullat në lidhje me dhomën e sistemit, në përputhje me nenin 26, Siguria fizike e Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë për Mbrojtjen e të Dhënave Personale janë si më poshtë:

- të bëhet testim i rregullt i sistemeve për monitorimin dhe ruajtjen e kushteve optimale të punës në sallë;
- inspektim i rregullt të kondicionerëve dhe pajisjeve të mbrojtjes nga zjarri në sistemin e sallës;

- qasja fizike në sallën e sistemit kontrollohet dhe mundësohet në mënyrë të përshtatshme vetëm për punonjësit e autorizuar. Të jashtëm – palët e treta mund të hyjnë në sallën e sistemit vetëm në prani të një punonjësi të autorizuar të përshtatshëm.
- vendosja e një mekanizmi të përshtatshëm për regjistrimin e hyrjeve, gjegjësisht hyrjeve revizore për qasje në zonat e sigurisë.
- Furnizimi me energji elektrike - Pajisjet harduerike dhe pajisjet tjera sigurohen nga një dështim në furnizimin e rregullt me energji elektrike ose ndryshime të pakontrolluara në tension, përmes mekanizmave të duhur që do të sigurojnë vazhdimësi në punë sipas specifikimeve të prodhuesit të pajisjeve në rast të dështimit të furnizimit të rregullt me energji elektrike.

Rrjetëzimi dhe komunikimi

Neni 25

Kinoteka zbaton kontrollet e duhura në rrjetin kompjuterik dhe komunikimet elektronike në përputhje me nenin 7, paragrafi (3) Menaxhimi i rrezikut nga Rregullorja për sigurinë e përpunimit të të dhënave personale të Agjencisë së Mbrojtjes së të Dhënave Personale si më poshtë:

- Pengesë e instaluar e rrjetit mbrojtës të harduerit/softuerit (ang. Firewall”) dhe ruterin midis sistemit të informacionit dhe internetit ose çdo forme tjetër të rrjetit të jashtëm, si masë mbrojtëse kundër përpjekjeve të paautorizuara ose qëllimkëqija për të hyrë ose thyer sistemin;
- komunikimet dhe shërbimet rrjetit janë konfiguruar me një nivel të përshtatshëm kufizimesh në kontrollin e qasjes;
- komunikimet dhe shërbimet e rrjetit menaxhohen nga personeli i autorizuar në mënyrë që të mos rrezikojnë sigurinë dhe efikasitetin e proceseve;
- qasja në distancë në rrjet dhe burime lejohet vetëm për përdoruesit e autorizuar përmes një procesi autentifikimi, kufizimeve në të drejtat e qasjes dhe një niveli adekuat të sigurisë gjatë transferimit të të dhënave;
- kapaciteti i rrjetit dhe fuqia e qarkullimit të linjave të komunikimit janë projektuar në një mënyrë që mundësojnë kryerjen efikase dhe pa pengesë të proceseve;
- është krijuar një sistem i përshtatshëm i gjurmës së revizionit për evidentim, monitorim dhe raportimin e ngjarjeve të sigurisë në lidhje me përdorimin e komunikimeve dhe shërbimeve të rrjetit.

Neni 26

Lidhja pa tela është e mbrojtur nga përgjimi ose ndryshimi i paautorizuar.

Kinoteka përcakton rregullat për vendosjen e lidhjes pa tel, në përputhje me nenin 7, paragrafi (3) Menaxhimi i rrezikut të Rregullores për sigurinë e përpunimit të të dhënave personale të Agjencisë së Mbrojtjes së të Dhënave Personale si më poshtë:

- vendosjen e enkriptimit të përshtatshëm të të dhënave të transmetuara përmes komunikimit pa tel;
- ngritjen e mekanizmave të përshtatshëm të vërtetimit të përdoruesit (si për shembull Wi-Fi Protected Access II);
- ndalimin e transmetimit (broadcasting) të *identifikuesit të vetëm të lidhjes në rrjet (Service set identifier SSID)*;

- praktika e mbylljes së komunikimit pa tel (access point) jashtë orarit të punës dhe gjatë fundjavave dhe festave;
- kufizimin e llojit të komunikimit dhe rrjedhën e lejuar të të dhënave (personal firewall).

Neni 27

Kinoteka në përputhje me nenin 12, Sigurimi i pajisjeve mbi të cilat kryhet përpunimi i të dhënave personale nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale, zbaton kontrollet e duhura të qasjes në distancë, si më poshtë:

- të gjithë punonjësit që përdorin kompjuterë portativë, gjegjësisht laptopë, tableta ose pajisje të tjera smart, janë përgjegjës për mbrojtjen e të dhënave të biznesit që mund të jenë në to, si dhe vetë mbrojtjen fizike, mbrojtjen nga qasja e paautorizuar, mbrojtja e sigurisë dhe mbrojtja kundër viruseve.
- pajisjet e lëvizshme dhe portative të përdorura dhe që kanë informacione të ndjeshme dhe/ose kritike të biznesit nuk duhet të lihen pa mbikëqyrje dhe kur është e mundur të kyçen fizikisht.
- qasja në distancë në sistemet kompjuterike dhe informacion është e kufizuar përkohësisht duke ndërprerë automatikisht seancën pasi të ketë kaluar një periudhë e caktuar kohore, sa herë që të jetë e mundur dhe e realizueshme.

Shërbime interneti

Neni 28

Posta elektronike (në tekstin e mëtejme: e-mail) përdoret për nevojat afariste të Kinotekës në përputhje me procedurat e brendshme si dhe legjislacionin.

Kinoteka përcakton rregullat për përdorimin e postës elektronike në përputhje me nenin 30, Masat organizative për sigurinë e të dhënave personale (standardi minimal) të Rregullores për sigurinë e përpunimit të të dhënave personale të Agjencisë për Mbrojtjen e të Dhënave Personale si më poshtë:

- vetëm personat e autorizuar nga njësia organizative e TI-së, gjegjësisht personat e autorizuar prej tyre (furnizuesit e jashtëm) janë përgjegjës për konfigurimin dhe vendosjen e sistemit të postës elektronike;
- përdoruesit e postës elektronike nuk duhet të paraqiten rrejshëm dhe të marrin identitetin e dikujt tjetër gjatë komunikimit;
- përdoruesit duhet të përdorin bashkëngjitjet në email me kujdes maksimal dhe një përmbajtje e tillë mund t'i nënshtrohet filtrimit të brendshëm nga sistemi i postës elektronike.

Për shembull, transmetimi i llojeve të caktuara të skedarëve (exe, .bat, .pif, .mpeg, .mp3,.....) është i ndaluar përmes sistemit të postës elektronike;

- është e nevojshme të përcaktohet një periudhë e ruajtjes së postës elektronike për të përmbushur nevojat juridike dhe afariste dhe të gjithë përdoruesit e atij shërbimi duhet t'i përmbahen periudhës së ruajtjes;
- Nuk duhet të abuzohet me shërbimin e-posta për shqetësim dhe propagimin e materialeve dhe përmbajtjeve joetike;

Neni 29

Interneti dhe shërbimet e internetit përdoren për nevojat afariste të Kinotekës në përputhje me procedurat e brendshme si dhe legjislacionit.

Kinoteka përcakton rregullat për përdorimin e postës elektronike në përputhje me nenin 30, Masat organizative për sigurinë e të dhënave personale (standardi minimal) të Rregullores për sigurinë e përpunimit të të dhënave personale të Agjencisë për Mbrojtjen e të Dhënave Personale si më poshtë:

- Qasja në internet duhet të vendoset përmes kufizimeve të duhura të qasjes, duke përmbushur rregullin e privilegjit më të vogël;
- Qasja në internet duhet të sigurohet nga ndërhyrjet e jashtme qëllimkëqija duke vepruar dhe konfiguruar qasjen kufizuese në përmbajtjen e internetit përmes firewall
- Qasja në internet dhe përdorimi i shërbimeve të internetit (rrjetet sociale, komunikimet e shpejta - chat) nuk duhet të rrezikojnë në asnjë mënyrë funksionimin dhe kryerjen efikase dhe të sigurt të operacioneve afariste;
- Qasja dhe përdorimi i shërbimeve të internetit i nënshtrohet kontrollit dhe monitorimit të rregullt;
- Kërkuesit duhet të përdoren në mënyrë të sigurt me ndihmën e mjeteve dhe funksionaliteteve të integruara të sigurisë;
- Punonjësit duhet të njihen me rregullat për përdorimin e sigurt të internetit dhe shërbimeve të internetit.

Neni 30

Kinoteka zbaton masa teknike që do të garantojnë identitetin e saktë të faqes (pharming prevention), si dhe konfidencialitetin e informacioneve që dërgon ose mbledh përmes faqes së internetit, në përputhje me nenin 19, Sigurimi i faqes së internetit të kontrolluesit nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale përmes masave të mëposhtme:

- Zbatimin e protokollit kriptografik (TLS / SSL) në të gjitha faqet e internetit të kontrolluesit;
- Përdorimi i detyrueshëm i protokollit kriptografik (TLS) për të gjitha faqet e internetit, duke përfshirë edhe formularët për mbledhjen e të dhënave personale ose mundësimin e vërtetimit të përdoruesit dhe ato të cilave u shfaqen ose transmetohen të dhënat personale që nuk janë publike;
- kufizimin e portave të komunikimit në ato që janë rreptësisht të nevojshme për funksionimin e duhur të aplikacioneve të instaluar. Nëse serveri i vebit 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;
- siguria që vetëm personat e autorizuar do të kenë qasje në mjetet dhe ndërfaqet administrative, në veçanti duke kufizuar përdorimin që të jetë në dispozicion vetëm për personat e autorizuar me privilegje administratori që janë pjesë e ekipit përgjegjës për teknologjinë informative dhe vetëm për aktivitetet administrative që janë të domosdoshme; dhe
- gjatë përdorimit të cookies, sigurohet pëlqimi paraprak i përdoruesit të internetit pas njoftimit të përdoruesit.

Sigurimi i serverëve dhe kompjuterëve personale në të cilët kryhet përpunimi i të dhënave personale

Neni 31

Kinoteka zbaton masat e duhura teknike për të siguruar mbrojtjen e serverëve dhe pajisjeve, në përputhje me nenin 12, Sigurimi i pajisjeve mbi të cilat kryhet përpunimi i të dhënave personale nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale si më poshtë:

- softueri antivirus i përditësuar rregullisht dhe politika e përcaktuar për përditësimet e rregullta të programeve softuerike;
- programe softuerike të konfiguruar në mënyrë që përditësimet e sigurisë të kryhen automatikisht;
- mbrojtje e besueshme anti-virus dhe anti-spyware e sistemit informativ, i cili do të përditësohet vazhdimisht për parandalimin e kërcënimeve të panjohura dhe të paplanifikuara nga viruset dhe spyware të reja;
- mbrojtje efektive dhe e besueshme anti spam, e cila përditësohet vazhdimisht për mbrojtje parandaluese nga spamet;
- kufizimin e mundësisë për të lidhur media portative (USB, disqe të jashtëm, etj.) në sistemet me rëndësi primare;
- regjim automatik i çaktivizimit të punës për mediumet portative (Disable autorun for removable media);
- Çlajmërim i automatizuar i sistemit informativ pas kalimit të një periudhe të caktuar prej 15 minutash joaktiviteti dhe për riaktivizimin e sistemit kërkohet shënimi i sërishëm i emrit të përdoruesit dhe fjalëkalimi;

Menaxhimi i përdoruesve

Neni 32

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.

Kinoteka ka krijuar mekanizma për të parandaluar personat e autorizuar që të kenë qasje në të dhënat personale dhe pajisjet e komunikimit informativ me të drejta të tjera nga ato të autorizuar.

Neni 33

Qasja në sisteme siguron minimum privilegjesh për të përmbushur detyrat dhe detyrimet e punës së punonjësve, personave të punësuar dhe/ose personave të tjerë të autorizuar në përputhje me pozicionin e tyre të punës dhe kërkesave afariste. (parimi "need to know").

Të drejtat e qasjes janë hartuar sipas rregullit të segregimit (ndarjes) së detyrave, aty ku është e mundur.

Kërkesat afariste për qasje dhe niveli o privilegjeve përcaktohen, dokumentohen dhe autorizohen në mënyrë përkatëse.

Kinoteka ka krijuar proces për regjistrimin dhe kontrollin e të drejtave të qasjes në sistemet e informacionit. Procesi mbulon të gjitha fazat nga regjistrimi fillestar i përdoruesve të rinj, deri në fshirjen përfundimtare të përdoruesve që nuk kanë më nevojë afariste për qasje.

Administratori i sistemit të informacionit autorizohet nga Kinoteka si kontrollues, ndan, ndryshon ose revokon privilegjet e qasjes së autorizuar në të dhënat personale dhe pajisjet e komunikimit të informacionit vetëm në përputhje me rregulloret ligjore dhe të brendshme.

Neni 34

Kinoteka ka krijuar proces të përshtatshëm për identifikimin dhe vërtetimin e përdoruesve të sistemit të informacionit, në përputhje me nenin 11, 1. Masat teknike Autentifikimi i personave të autorizuar nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Identifikimi (ang. Identification) është procesi i caktimit të një identifikuesi unik (emri i përdoruesit) për t'u identifikuar në sisteme.

Autentifikimi (ang. Authentication) është procesi i konfirmimit të identitetit të përdoruesit (subjektit) dhe të drejtave të tyre të qasjes në sisteme.

Në varësi të kriticitetit të sistemit të informacionit, mund të përdoren një ose më shumë mënyra autentifikimi, siç janë:

- ✓ me përdorimin e një rrokje (vargu) të shenjave të njohura vetëm nga përdoruesi (siç është përdorimi i fjalëkalimit);
- ✓ me përdorimin e një pajisjeje që është në pronësi vetëm të përdoruesit (për shembull, kartë elektronike);
- ✓ duke përdorur karakteristika biometrike që janë unike për përdoruesin (skanimi i syve, gjurmët e gishtërinjve).

Neni 35

Kinoteka zbaton rregullat për regjistrimin e përdoruesve, gjegjësisht, procedurë për lejimin dhe revokimin e qasjes në sistemet e informacionit në të gjitha nivelet (sistemi operativ, bazat e të dhënave dhe aplikacionet) në përputhje me nenin 18, paragrafi (1) Sigurimi i serverëve, të Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale si më poshtë:

- duke përdorur një identifikues unik (emrin e përdoruesit) me të cilin përdoruesit do të lidhen në mënyrë unike;
- përdorimi i emrave grupor të përdoruesve ose profileve gjenerike (të vendosura) të përdoruesve (p.sh. operator/administrator) duhet të shmanget dhe të zbatohet vetëm në situata të jashtëzakonshme;
- krijimin e të drejtave të qasjes dhe nivelin e privilegjit sipas nevojave afariste dhe në përputhje me autorizimet;
- sigurimi i rregullave që do të parandalojnë qasjen individuale nga komprometimi i kontrollit të ndarjes së duhur të detyrave;
- krijimin e një gjurme të përshtatshme revizore për qasjen dhe përdorimin e sistemeve;
- procedurat për ndryshimin ose anulimin e qasjes gjatë ndryshimit të pozicionit të punës ose largimit.

Menaxhimi i fjalëkalimeve

Neni 36

Kinoteka përcakton rregullat e duhura për zgjedhjen dhe përdorimin e fjalëkalimeve në nivel përdoruesi dhe sistemi për qasje në sistemin e informacionit. Fjalëkalimet janë mënyra më e zakonshme për të siguruar vërtetimin e përdoruesve, gjegjësisht konfirmimin dhe vërtetimin e identitetit të përdoruesve gjatë qasjes në sistemet ose shërbimet informative.

Kinoteka përcakton rregullat për sistem efektiv dhe të besueshëm të menaxhimit të fjalëkalimeve në përputhje me nenin 11, paragrafi (2), 1. Masat teknike Autentifikimi i personave të autorizuar nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale si në vijim:

- përdorimi i profileve individuale të përdoruesve dhe fjalëkalimeve për të ruajtur përgjegjësinë(accountability);
- ndryshimi i fjalëkalimeve të paracaktuara (default passwords) për sistemet (serverat, pajisjet e rrjetit, bazat e të dhënave, sistemet operative, etj.);
- fjalëkalimi duhet të përbëhet nga një kombinim i të paktën tetë shkronjave alfanumerike (shkronja të vogla dhe të mëdha), simboleve, numrave dhe shenjave të pikësimit;
- fjalëkalimet duhet të ndryshohen automatikisht pas një periudhe të caktuar kohore bazuar në analizën e rrezikut, e cila nuk mund të jetë më e gjatë se tre muaj.
- të sigurojë mekanizëm për mbylljen e përdoruesit pas një numri të caktuar të hyrjeve të pasuksesshme, por jo më shumë se pesë përpjekje të njëpasnjëshme të pasuksesshme
- të sigurojë mekanizëm për ruajtjen e historikut të fjalëkalimeve të përdorura të përdoruesve;
- mbrojtja nga përdorimi i sërishëm i fjalëkalimeve të njëjta për një periudhë të caktuar kohe;
- maskimi i fjalëkalimeve në ekran gjatë futjes së tyre;
- zbatimin e mekanizmave të sigurisë për ruajtjen dhe transferimin e fjalëkalimeve (encrypted or hashed).
- fjalëkalimet fillestare duhet të ndryshohen menjëherë pas hyrjes së parë.

Neni 37

Qasja në krijimin e rregullave për menaxhimin e fjalëkalimeve është në përputhje me kritikizmin e profileve të përdoruesve, gjegjësisht nivelin e privilegjit, siç janë administratorët e sistemit, profilet shërbyese ose sisteme të përdoruesve, etj., në përputhje me nenin 18, Sigurimi i serverëve nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë për Mbrojtjen e të Dhënave Personale.

Neni 38

Kinoteka ka rregulla të veçanta për krijimin dhe përdorimin e fjalëkalimeve për administratorët e sistemit të informacionit, në përputhje me nenin 38, Masat e Larta, Menaxhimi i Fjalëkalimeve nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale si më poshtë:

- fjalëkalimi duhet të përbëhet nga një kombinim i të paktën tetë shkronjave alfanumerike (shkronja të vogla dhe të mëdha), simboleve, numrave dhe shenjave të pikësimit;
- fjalëkalimet duhet të ndryshohen automatikisht pas një periudhe të caktuar kohore bazuar në analizën e rrezikut, e cila nuk mund të jetë më e gjatë se një muaj.

Sistemi i monitorimit dhe kontrollit

Neni 39

Kinoteka ka vendosur gjurmët e revizionit në pjesët kritike të sistemit të informacionit në disa nivele – sistemi operativ, aplikacionet, baza e të dhënave dhe komunikimi në rrjet, pajisjet periferike (Ups), përmes regjistrimit (event recording) në përputhje me nenin 15, Sigurimi i të dhënave për çdo qasje (logs) të Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale për parametrat e mëposhtëm:

- emrin e përdoruesit;
- data dhe koha e hyrjes dhe daljes nga sistemi;
- identifikuesi i terminalit ose nëse është e mundur, vendndodhja;
- regjistrimet e përpjekjeve të suksesshme dhe të refuzuara për hyrje;
- regjistrimet e të dhënave të suksesshme dhe të refuzuara dhe përpjekjet e tjera për qasje.

Kinoteka ka krijuar mekanizëm për mbrojtjen e integritetit të gjurmës së revizionit, gjegjësisht ndryshimin e gjithë jetëgjatësisë së saj.

Neni 40

Ngjarjet e hyrjeve i nënshtrohen monitorimit dhe kontrollit të vazhdueshëm nga personat përkatës të TI-së – administratorët në baza të rregullta.

Zyrtari për Mbrojtjen e të Dhënave Personale kontrollon të dhënat nga hyrjet nga aspekti i qasjes së paautorizuar të përdoruesve, të paktën një herë në muaj dhe përgatit raport për kontrollin e kryer dhe parregullsitë e konstatuara.

Plani i vazhdimësisë dhe kopjet e sigurimit

Neni 41

Kinoteka zhvillon dhe mban plan të përshtatshëm për vazhdimësinë në punë së bashku me procedurat dhe skenarët e duhur për kopjet e sigurisë dhe restaurimit në mënyrë që proceset dhe të dhënat afariste (përfshirë edhe të dhënat personale) të ruhen dhe të rikthehen në një kornizë të pranueshme kohore në mënyrë që të minimizohen dëmet e shkaktuara gjatë ndonjë ndërprerje të madhe ose fatkeqësie.

Masat dhe aktivitetet e përfshira në kuadër të Planit të Vazhdimësisë në punë bazohen në vlerësim të rreziqeve dhe ndikimit të tyre në proceset afariste, në përputhje me nenin 22, Kopjet e sigurisë dhe rivendosja e të dhënave personale të ruajtura (duke siguruar vazhdimësinë) të Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Kinoteka bën kopje të sigurisë së të dhënave personale në intervale të rregullta kohore, në mënyrë që të zvogëlojë efektin në rast të humbjes ose dëmtimit të tyre të padëshiruar.

Neni 42

Për efikasitet maksimal, Plani i Vazhdimësisë dhe udhëzimet përkatëse të kopjeve të sigurimit (backup) dhe renovimit IT përqendrohen në parimet e mëposhtme:

- mbrojtjen e jetës dhe shëndetit të punonjësve gjatë ndonjë fatkeqësie;
- mbrojtjen dhe rikuperimin e të dhënave dhe informacioneve pas ndodhjes së fatkeqësisë, nëpërmjet kopjeve të sigurisë të të dhënave personale dhe të tjera në intervale të rregullta kohore, me qëllim uljen e efektit në rast të humbjes ose dëmtimit të tyre të padëshiruar.
- mbrojtjen e linjave të komunikimit dhe mjeteve nga sistemi i informacionit.

Neni 43

Kopjet e sigurisë ruhen jashtë dhomës në të cilën ndodhen serverët dhe janë të mbrojtura fizikisht dhe kriptografikisht, me qëllim parandalimin e çdo modifikimi dhe abuzimi nga persona të paautorizuar, në përputhje me nenin 22, paragrafi (5) Kopjet e sigurisë dhe kthimi i sërishëm i të dhënave personale të

ruajtura (duke siguruar vazhdimësinë) të Rregullores për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Neni 44

Plani i Vazhdimësisë së punës së bashku me mekanizmat adekuat për rekonstruktiv inspektohen dhe testohen periodikisht, dhe të paktën një herë në vit bazuar në skenarë të përcaktuar më parë për të siguruar që janë në përputhje me aktivitetet afariste dhe se janë të përditësuara.

Menaxhmenti i lartë informohet rregullisht për nivelin e rreziqeve, gjegjësisht efikasitetin e procesit për sigurimin e vazhdimësisë së punës dhe të dhënave, përmes testimit të rregullt dhe raporteve përkatëse.

Administratorët e IT-së kontrollojnë rregullisht funksionalitetin e kopjeve të sigurisë për të kryer rekonstruktivimin e të dhënave personale.

Enkriptimi

Neni 45

Kodimi (Enkriptimi) është një teknikë për mbrojtjen e informacioneve të ndjeshëm ose kritike për të siguruar konfidencialitetin, integritetin dhe përvokueshmërinë e tyre në qasje dhe përdorim, në përputhje me nenin 17, Mbrojtja e rrjetit të brendshëm të Rregullores për sigurinë e përpunimit të të dhënave personale të Agjencisë për Mbrojtjen e të Dhënave Personale.

Niveli i duhur i kodimit duke përfshirë llojin dhe cilësinë e algoritmit, si dhe gjatësinë e çelësave mbrojtës që do të përdoren, duhet të bazohet në një analizë dhe vlerësim të rreziqeve ndaj kritikitetit të informacionit.

Informacionet e ndjeshme dhe konfidenciale ruhen dhe transmetohet të koduara kudo që kjo është e mundur. Ndalohet dërgimi i informacioneve të ndjeshme dhe të klasifikuara me shkallën më të lartë të konfidencialitetit, siç është NAVQ përmes shërbimeve të komunikimit elektronik si e-mail, komunikimeve të shpejta etj, nëse ato nuk janë të mbrojtura nga leximi dhe ndryshimi i paautorizuar.

Këto teknika dhe mekanizma duhet të kenë mundësinë e zbatimit të mekanizmave të përshtatshëm për deshifrimin e informacioneve nga personat e autorizuar në procedurë të përcaktuar saktë.

Sigurimi i medimeve portative

Neni 46

Mediumet portative në të cilat kryhet përpunimi i të dhënave personale, kontrolluesi siguron që ato të ruhen në një vend në të cilin kanë qasje vetëm personat e autorizuar të përcaktuar prej tij.

Transferimi i medimeve jashtë ambienteve të punës bëhet vetëm me autorizim paraprak me shkrim nga kontrolluesi.

Pas transferimit të të dhënave personale nga mediumet ose pas skadimit të periudhës së caktuar të ruajtjes, mediumi duhet të shkatërrohet, fshihet ose pastrohet nga të dhënat personale të regjistruara në të.

Neni 47

Shkatërrimi i mediumit kryhet në mënyrë që do të sigurojë që të dhënat që janë regjistruar në të nuk mund të rekonstruktohen (për shembull: duke ndarë mekanikisht pjesët e tij përbërëse).

Fshirja ose pastrimi i mediumit duhet të bëhet në mënyrë që parandalon ripërtëritjen e mëtutjeshëm të të dhënave personale të regjistruara.

Neni 48

Mediumet mund të transmetohet jashtë ambienteve të punës nëse të dhënat personale janë të koduara ose të mbrojtura me metoda të përshtatshme që garantojnë që të dhënat nuk do të jenë të lexueshme, dhe vetëm administratori i sistemit të informacionit mund t'i deshifrojë ato ose një person i autorizuar prej tij.

Neni 49

Të dhënat personale (p.sh. NVAQ) mund të transmetohen përmes rrjeti komunikimi elektronik vetëm nëse ato janë të koduara ose nëse mbrohen në mënyrë të posaçme që sigurojnë që të dhënat nuk do të jenë të lexueshme gjatë transmetimit.

Ballafaqimi me incidente

Neni 50

Sipas përcaktimit ligjor, cenimi i sigurisë së të dhënave personale është një ngjarje që çon në shkatërrim aksidental ose të paligjshëm, humbje, ndryshim, zbulim të paautorizuar ose qasje në të dhënat personale që transferohen, ruhen ose përpunohen në mënyrë tjetër.

Kinoteka ka krijuar një Rregullore për mënyrën e raportimit të shkeljes së sigurisë së të dhënave personale të përpunuara.

Neni 51

Nëse një ngjarje klasifikohet si shkelje e të dhënave personale që paraqet rrezik për të drejtat dhe liritë e subjekteve të të dhënave personale, kontrolluesi duhet të njoftojë Agjencinë për Mbrojtjen e të Dhënave Personale brenda 72 orëve.

Menaxhimi i përpunuesve

Neni 52

Të drejtat dhe detyrimet e ndërsjella të kontrolluesit dhe kompanive të jashtme që sipas Ligjit për Mbrojtjen e të Dhënave Personale karakterizohen si përpunues, rregullohen me marrëveshje të përshtatshme.

Kinoteka si Kontrollues para lidhjes së kontratës është i detyruar të kërkojë nga përpunuesi (ofruesi i shërbimit), të paraqesë politikën e tij të sigurisë në lidhje me sistemin e informacionit dhe infrastrukturën e informacionit mbi të cilën do të kryhet përpunimi i të dhënave personale në emër të Kontrolluesit. Është e një rëndësie të veçantë në kontratën e outsourcing që parashikon përpunimin e të dhënave personale të shënohen detyrimet dhe distinkcioni i saktë midis roleve të kontrolluesit (klientit) dhe përpunuesit (furnizuesit), që rrjedhin nga Ligji për Mbrojtjen e të Dhënave Personale.

Kontrata duhet të përfshijë dispozitën që furnizuesi do të përpunojë të dhënat personale vetëm sipas udhëzimeve të dokumentuara të marra nga klienti dhe duke zbatuar masat e duhura teknike dhe organizative.

Neni 53

Si minimum, Marrëveshjet me Përpunuesit duhet të përfshijnë elementët e mëposhtëm:

- detyrimet për përpunuesin të marrë masa teknike dhe organizative për të garantuar sigurinë e përpunimit të të dhënave personale. Pas çka, përpunuesi duhet të marrë parasysh natyrën e ndjeshme të të dhënave personale duke aplikuar zgjidhje moderne teknologjike dhe detyrime që duhet të sigurojnë mbrojtjen dhe konfidencialitetin e përpunimit;

- kushtet për kthimin e të dhënave dhe/ose shkatërrimin e tyre pas skadimit ose përfundimit të kontratës;

– rregullat për menaxhimin dhe njoftimin e kontrolluesit në rast të incidenteve, gjegjësisht në rast të shkeljes së të dhënave personale;

– detyrimet që përpunuesi të veprojë vetëm në përputhje me udhëzimet e marra nga kontrolluesi;

– të gjithë punonjësit dhe punonjësit e përpunuesit dhe nënkontraktorët e tyre që përpunojnë të dhënat personale, para fillimit të punës së tyre duhet të nënshkruajnë Deklaratën e Konfidencialitetit dhe Fshehtësisë.

Kinoteka si kontrollues duhet të informohet për të gjithë nënkontraktorët që janë të angazhuar dhe ata duhet të kenë nivelin minimum të masave të siguruar nga përpunuesi.

Ruajtja e dokumenteve – rregulli i tavolinës së pastër

Neni 54

Kinoteka promovon dhe zbaton rregullin “tavolina e pastër” gjatë përpunimit të të dhënave personale që përmbahen në dokumentet për mbrojtjen e tyre gjatë gjithë procesit të përpunimit nga qasja e personave të paautorizuar, në përputhje me nenin 33, rregulli “tavolina e pastër” të Rregullores për sigurinë e përpunimit të të dhënave personale të Agjencisë së Mbrojtjes së të Dhënave Personale.

Neni 55

Dokumentacioni që përdoret në Kinotekë është vendosur në dhoma dhe dollapë të veçantë me mekanizma të përshtatshëm mbrojtës. Hapësirat duhet të jenë të mbyllura edhe në periudhën kur dokumentet nuk përpunohen nga personat e autorizuar. Kur karakteristikat fizike të hapësirave nuk lejojnë zbatimin e masave, Kontrolluesi duhet të zbatojë masa të tjera për të parandaluar çdo qasje të paautorizuar në dokumente.

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

Neni 56

Shkatërrimi i dokumenteve bëhet duke i copëtuar ose në ndonjë mënyrë tjetër, në mënyrë që ato të mos mund të përdoren përsëri.

Afatet për ruajtjen e të dhënave personale

Neni 57

Të dhënat personale ruhen vetëm për kohën sa është e nevojshme për të arritur qëllimin për të cilin janë mbledhur dhe përpunuar. ndërsa respektohen edhe afatet e përcaktuara në përputhje me ligjet dhe aktet e brendshme që rregullojnë fushën përkatëse, si dhe ligjin për punën arkivore.

Testimi (niveli i lartë)

Neni 58

Kinoteka kryen testimin e sistemit informativ para zbatimit të tij ose pas ndryshimeve të bëra për të kontrolluar nëse sistemi ofron siguri të të dhënave personale në përputhje me rregulloret për mbrojtjen e të dhënave personale, në përputhje me nenin 41, IV. Niveli i lartë, nga Rregullorja për Sigurinë e Përpunimit të të Dhënave Personale të Agjencisë për Mbrojtjen e të Dhënave Personale Fushëveprimi, frekuenca dhe objekti i testimit të rezistencës së sistemeve përcaktohen në varësi të nivelit të rrezikut nga kërcënimet nga hapësira digjitale.

Kontrolli periodik

Neni 59

Masat për sigurimin e fshehtësisë dhe mbrojtjen e të dhënave personale i nënshtrohen kontrollit me qëllim të verifikimit nëse procedurat dhe udhëzimet të përfshira në dokumentacionin e masave teknike dhe organizative zbatohen dhe janë në përputhje me rregulloret për mbrojtjen e të dhënave personale.

Neni 60

Kontrolli i brendshëm bëhet në baza vjetore ose sipas nevojës në rast të ndryshimeve të rëndësishme organizative dhe teknike, kërkesave të menaxhmentit dhe në përputhje me kërkesat ligjore dhe rregullatore.

Kontrollin e brendshëm e kryen Zyrtari për Mbrojtjen e të Dhënave Personale për çka ai përgatit një raport të përshtatshëm për shkallën e pajtueshmërisë me Ligjin për Mbrojtjen e të Dhënave Personale.

Neni 61

Kinoteka bën vlerësim periodik të rezultateve të arritura të sistemit të video mbikëqyrjes çdo dy vjet. Procesi i analizës dhe kontrollit të video mbikëqyrjes përfshihet në Rregulloren përkatëse për video mbikëqyrje.

Neni 62

Zyrtari për Mbrojtjen e të Dhënave Personale të paktën njëherë në muaj kryen kontroll periodik të qasjes së paautorizuar në sisteme dhe punën e administratorit të sistemit të informacionit dhe përgatit një raport për kontrollin e kryer dhe parregullsitë e konstatuara.

Dispozitat përfundimtare

Kjo Rregullore hyn në fuqi ditën e miratimit të saj.

Rregullorja i nënshtrohet kontrolleve dhe përditësimeve të rregullta në përputhje me ndryshimet në strukturën organizative, infrastrukturën teknike ose kërkesat e reja ligjore dhe /ose rregullatore.

Nr. _____

Data:

IK Kinoteka e Republikës së Maqedonisë së Veriut
-Kryetari i Bordit Drejtues

Tomislav Osmanli