Republika e Maqedonisë së Veriut

Agjencia për mbikëqyrje të financimit kapital të sigurimit pensional
Nr. 08-939/5
30.9.2021-viti
SHKUP

Rregullat për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes të përpunimit të të dhënave personale personale

Shkup, gusht, viti 2021

MAPAS
Agjencia për mbikëqyrje
të financimit kapital të
sigurimit pensional

Republika e Maqedonisë së Veriut

PËRMBAJTJA

MAPAS
Agjencia për mbikëqyrje të financimit kapital të sigurimit pensional

Republika e Maqedonisë së Veriut

Në bazë të nenit 36 të Ligjit për mbrojtjen e të dhënave personale ("Gazeta zyrtare e Republikës së Maqedonisë" numër 42/20), dhe në lidhje me nenin 6 paragrafët (1) dhe (2) të Rregullores për siguri në përpunimin e të dhënave personale ("Gazeta Zyrtare e Republikës së Maqedonisë" nr.122/2020), dhe nenit 8 paragrafi (1) pika o) të Statutit të Agjensisë për mbikëqyrjen e finansimit kapital të sigurimit pensional (Nr.01-385/3 nga 18.03.2013, nr. 02-13/5 të datës 22.01.2014, 02-1316/4 të datës 11.11.2014, 02- 83/3 të datës 30.01.2015, 02/1259/6 të datës 27.11.2018 dhe 02-464/6 të datës 29.03.2019) kryetare e Këshillit të ekspertëve në Agjensinë për mbikëqyrje të financimit kapital të sigurimit pensional, në ??.??. 2021 miratoi:

Rregullat për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes të përpunimit të të dhënave personale

I. Dispozitat e përgjithshme

Lënda e rregullimit

Neni 1

Këto rregulla përshkruajnë masat teknike dhe organizative që Agjencia për mbikëqyrje të financimit kapital të sigurimit pensional (në tekstin e mëtejmë: Agjencia) i zbaton në cilësinë e saj si kontrollues për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale.

Fjalorth

Neni 2

Disa shprehje të përdorura në këtë rregullore kanë këtë kuptim:

"**Konfidencialiteti**" është qasja në të dhënat personale vetëm nga personat që kanë autorizim për përpunimin e tyre nga kontrolluesi;

"**Integriteti**" është mbrojtja e saktësisë së të dhënave personale, duke garantuar që të dhënat personale të jenë të sakta, të plota dhe të përditësuara;

"**Disponueshmëria**" është qasja e papenguar dhe disponueshmëria e vazhdueshme (business continuity) e sistemit informativ në të cilin përpunohen të dhënat personale nga personat e autorizuar;

MAPAS
Agjencia për mbikëqyrje
të financimit kapital të
sigurimit pensional

"**Autentifikimi**" është një procedurë që mundëson konfirmimin e identitetit të personit të autorizuar që lajmërohet dhe qaset në sistemin e informacionit në të cilin përpunohen të dhënat personale;

"**Parevokueshmëria**" është sigurimi i vërtetimit të autenticitetit të identitetit të personit të autorizuar i cili lajmërohet në sistemin e informacionit me çrast personi i autorizuar nuk mund ta mohojë aktivitetin ose veprimin e ndërmarrë;

"**Rreziku i sigurisë**" është probabiliteti i ndodhjes së një ngjarjeje që mund të rezultojë në

kompromentim, veçanërisht shkatërrimi i rastësishëm apo i kundërligjshëm, humbja, ndryshimi, zbulimi i paautorizuar i të dhënave personale, ose qasja e paautorizuar në të dhënat e transferuara, të dhënat personale të ruajtura ose të përpunuara në mënyrë të ndryshme (në tekstin e mëposhtëm: rrezik);

"**Menaxhimi i rrezikut**" është identifikimi, vlerësimi dhe klasifikimi i tij, i cili përfshin zbatimin e koordinuar të resurseve të kontrolluesit për minimizimin, vëzhgimin dhe kontrollin e probabilitetit dhe seriozitetit që mund të lindë gjatë përpunimit të të dhënave personale, të cilat mund të shkaktojnë dëme materiale ose jo materiale në proceset me të cilat përpunohen të dhënat personale;

"**Sistemi i mbrojtjes së të dhënave personale**" është një grup politikash të dokumentuara, kode të praktikave, udhëzime, procedura dhe udhëzimet e punës të miratuara nga Agjencia, të cilat janë në funksionin e zbatimit të masave teknike dhe organizative për garantimin e sigurisë dhe përpunimin e të dhënave personale në përputhje me rregullat për mbrojtjen e të dhënave personale.

"**Qasje e autorizuar**" është i autorizim, e cila i jepet personit të autorizuar për përpunimin e të dhënave personale, për përdorimin e pajisjeve të caktuara të komunikimit të informacionit ose për qasje në objektet e caktuara të punës së Agjencisë.

"**Incidenti**" është çdo anomali që prek ose mund të ndikojë në fshehtësinë dhe mbrojtjen e te dhenave personale.

"**Fjalëkalimi**" është informacion konfidencial i përbërë nga një grup karakteresh të cilat përdoren për kontrollimin e personit të autorizuar dhe operatorit.

"**Mediat**" janë një pajisje fizike që përdoret gjatë përpunimit të të dhënave personale në sistemin e informacionit, në të cilin të dhënat mund të regjistrohen ose nga të cilat mund kthehen sërish.

"**Kontrolli**" është një procedurë për kontrollin e identitetit të personit të autorizuar të sistemit të informacionit.

"**Kopja e sigurtë**" është një kopje e të dhënave personale që gjenden në dokumentet elektronike, të cilat

ruhen në një mediat për të mundësuar rikthimin e tyre.

"**Administrator i sistemit të informacionit**" është personi i autorizuar për planifikim dhe zbatim të masave teknike dhe organizative, si dhe për kontrollin e sigurimit të fshehtësisë dhe mbrojtjes të përpunimit të të dhënave personale, të cilat ruhen në sistemin e informacionit të Agjencisë.

"**Person i autorizuar**" është personi i punësuar ose i angazhuar në Agjenci, i cili ka qasje të autorizuar në të dhënat personale të cilat ruhen në sistemin e informacionit të Agjencisë, në dokumente dhe pajisje të komunikimit të informacionit.

"**Operatori**" është person fizik i autorizuar, i punësuar ose i angazhuar nga subjekte të jashtme i cili ka qasje në të dhënat personale të marra përmes sistemit të informacionit të Agjencisë, dokumentet dhe pajisjet për komunikim të informacionit.

"**Oficer për mbrojtjen e të dhënave personale**" është person i autorizuar i punësuar në Agjenci i cili kryen punë që kanë të bëjnë me mbrojtjen e të dhënave personale në dispozicion të Agjencisë, në pajtim me Ligjin për mbrojtjen e të dhënave personale.

"**Sistemi i informacioneve i Agjencisë**" është sistemi i përgjithshëm i Agjencisë i përbërë nga kompjuterët personal, serveri i bazës së të dhënave, serveri i aplikacioneve, serveri i ruajtjes së të dhënave, portali i internetit dhe aplikacionet dhe pajisjet e tjera që përdoren për përpunimin e të dhënave.

"**Infrastruktura e informacionit**" është e gjithë pajisja Agjencisë për komunikimin e informacionit, brenda së cilës mblidhen, përpunohen dhe ruhen të dhënat personale.

"**Portali i internetit**" është pjesë e sistemit të informacionit të Agjencisë, i cili lejon qasje të kufizuar të personit dhe operatorit të autorizuar nëpërmjet një formulari në internet në të dhënat për të cilat është i autorizuar t'i përpunojë.

"**Dokumenti**" është çdo regjistrim që përmban të dhëna personale dhe mund të jetë në formë elektronike ose në letër, i ruajtur në një media dhe në pajisjet e komunikimit të informacionit që përdoren për përpunimin e të dhënave, të dorëzuara me postë ose të transmetuara përmes një rrjeti të komunikimit elektronik.

"**Biskotat (cookie)**" është informacioni që krijohet dhe dërgohet nga serveri i uebit deri në shfletuesin e uebit, dhe i cili më pas dërgohet si informacion i pandryshuar nga shfletuesi i uebit sa herë që serveri i uebit që ka krijuar informacionin i qaset përsëri.

"**Stacioni i punës**" është çdo pajisje (desktop, laptop) që është i lidhur me një rrjet dhe është pjesë e pajisjes së kontrollorit dhe në të cilën përpunohen të dhënat personale në sistemin e informacionit.

Zbatimi

Neni 3

Agjencia zbaton masa teknike dhe organizative që sigurojnë fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, sipas natyrës së të dhënave që përpunohen dhe rreziku gjatë përpunimit të tyre.

Mirëmbajtja e sistemit të informacionit

Neni 4

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

Personat fizik ose juridik që mirëmbajnë sistemin e informacionit të Agjencisë janë të detyruar të zbatojnë rregullat për mbrojtjen e të dhënave personale dhe dokumentacionin e miratuar për masat teknike dhe organizative.

Dispozitat e paragrafit (2) të këtij neni zbatohen edhe nëse personat fizik ose juridik i përpunojnë të dhënat personale të kontrollorit.

Transferimi i të dhënave personale në vendet e treta

Neni 5

Agjencia, në rast të mirëmbajtjes së harduerit dhe/ose softuerit ose aktiviteteve të tjera të sistemit të informacionit, mund t'i transferojë të dhënat personale vendeve të treta vetëm në përputhje me kushtet e përcaktuara në rregulloret për mbrojtjen e të dhënave personale.

Përpunimi i të dhënave personale

Neni 6

Në Agjenci, këto rregulla 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 synohet të jenë pjesë e një koleksioni të të dhënave personale

Niveli i lartë i masave të sigurisë për përpunimin e të dhënave personale

Neni 7

Agjencia zbaton masa teknike dhe organizative që sigurojnë fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, sipas natyrës së të dhënave që përpunohen dhe rreziku gjatë përpunimit të tyre.

Masat teknike dhe organizative nga paragrafi 1 i këtij neni klasifikohen në tre nivele:

a) standarde dhe

b) niveli i lartë.

II. Niveli i lartë i masave për sigurinë e përpunimit të të dhënave personale

Neni 8

Masat teknike dhe organizative të klasifikuara në nivel standard duhet të zbatohen për të gjitha dokumentet.

Për dokumentet që përmbajnë të dhëna personale në lidhje me: veprat penale, sanksionet e shqiptuara dhe masat e kontrollit duhet të zbatohen masat teknike dhe organizative të klasifikuara në nivel standard dhe të lartë.

Për dokumentet që përmbajnë: kategori të veçanta të të dhënave personale dhe të dhëna personale në lidhje me anëtarët e fondeve pensionale, duhet të zbatohen masat teknike dhe organizative të klasifikuara në nivel standard dhe të lartë.

Masat teknike dhe organizative që klasifikohen në nivel standard duhet të zbatohen në dokumentet që përmbajnë numrin e identifikimit të qytetarit.

Për dokumentet të cilat transferohen nëpërmjet një rrjeti të komunikimit elektronik, dhe përmbajnë kategori të veçanta të të dhënave personale dhe/ose numrin amë të qytetarit, duhet të zbatohen masat teknike dhe organizative të klasifikuara në nivel standard dhe të lartë.

Masat teknike

Neni 9

Agjencia zbaton masat e duhura teknike për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, të cilat ruhen në sistemin e informacionit, gjatë qasjes në

portalin e internetit nga personi i autorizuar, dhe atë:

- Krijimi i një emri unik i përdoruesit për çdo person të autorizuar në portalin e internetit të

Agjencisë;

- Fjalëkalimi i krijuar nga personi i autorizuar, i përbërë nga një kombinim prej të paktën tetë karaktereve alfanumerike (nga të cilat të paktën një shkronjë e madhe) dhe shenja speciale;

- Ndryshimi automatik i fjalëkalimeve çdo tre muaj;

- Qasje e kufizuar për çdo emër përdoruesi dhe fjalëkalim në pjesë të caktuara të sistemit të informacionit;

- Emri i përdoruesit dhe fjalëkalimi i cili mundëson qasjen e personit të autorizuar në sistemin e informacionit në tërësi, qasjet në aplikacione individuale dhe/ose koleksione individuale të të dhënave personale të nevojshme për kryerjen e detyrave të punës;

- Pseudonimizimi dhe kriptimi i të dhënave personale;

- Vendosja e çlajmërimit të automatizuar nga sistemi pas një periudhe të caktuar të pasivitetit (jo më shumë se 15 minuta) dhe rifutja e emrit të përdoruesit dhe fjalëkalimit gjatë aktivizimit të sistemit;

- Refuzim i automatizuar nga sistemi i informacionit pas tre përpjekjeve të dështuara për lajmërim (futja e emrit të përdoruesit ose fjalëkalimit të gabuar) dhe njoftimi i automatizuar i personit të autorizuar se duhet të kërkojë udhëzime nga administratori i sistemit të informacionit (në tekstin e mëposhtëm: administrator);

- Një pengesë e instaluar e rrjetit mbrojtës harduerik/softuerik ('firewall') ose ruter ndërmjet sistemit të informacionit dhe rrjetit të internetit ose formës tjetër të rrjetit të jashtëm, si një mbrojtje kundër përpjekjeve të paautorizuara ose përpjekjeve me qëllim të keq për të hyrë ose për lajmërim të paautorizuar në sistem;

- Instalimi i mbrojtjes efektive anti-virus dhe anti-spajver të sistemit të informacionit që do të përditësohet vazhdimisht dhe

- Lidhja e sistemit të informacionit në rrjetin elektrik përmes një pajisjeje të furnizimit me energji të pandërprerë.

- Sigurimi i faqes së internetit të Agjencisë duke aplikuar masa teknike që garantojnë identitetin e saktë të faqes, si dhe konfidencialitetin e informacionit në faqe.

Neni 10

Agjencia duhet të sigurojë masa teknike për fshehtësinë dhe mbrojtjen e të dhënave personale, të cilat ruhen në sistemin informativ të Agjencisë, gjatë qasjes në portalin e internetit nga subjektet e jashtme (shoqëritë pensionale, Fondi për sigurim pensional dhe invalidor në Maqedoni dhe rojet e pasurisë së fondeve pensionale) dhe atë:

- Krijimi i një emri të vetëm të përdoruesit;

- Fjalëkalimi i krijuar nga secili operator i portalit të internetit. Fjalëkalimi përbëhet nga

një kombinim prej të paktën tetë karakteresh alfanumerike (nga të cilat të paktën një është shkronjë e madhe) dhe shenja speciale;

- Ndryshimi automatik i fjalëkalimeve çdo tre muaj;

- Qasje e kufizuar për çdo emër të përdoruesit dhe fjalëkalim deri në pjesë të caktuara të sistemit të informacionit;

- Vendosaja e një çlajmërimi automatik nga sistemi pasi të ketë kaluar një periudhë e caktuar kohore e joaktivitetit (jo më shumë se 15 minuta) dhe shënimi i sërishëm i emrit të përdoruesit dhe fjalëkalimit gjatë aktivizimit të sistemit;

- Refuzim i automatizuar nga sistemi i informacionit pas tre përpjekjeve të dështuara për lajmërim (shënimi i gabuar i emrit të përdoruesit ose fjalëkalimit) dhe njoftimi i automatizuar i operatorit se ai duhet të kërkojë një udhëzim nga administratori;

- Krijimi i mbrojtjes efektive dhe të besueshme kundër viruseve dhe mbrojtjes anti-spajver të sistemit të informacionit, me vëzhgim dhe përditësim të vazhdueshëm me qëllim të parandalimit të kërcënimeve të panjohura dhe të paplanifikuara nga viruse dhe spajverë të rinj;

- Barriera e instaluar e rrjetit mbrojtës harduerik/softuerik ("firewall") ose ruteri i instaluar midis sistemit të informacionit dhe internetit ose çdo forme tjetër e rrjetit të jashtëm, si masë mbrojtëse ndaj përpjekjeve të paautorizuara ose me qëllim të keq për të hyrë ose depërtuar në sistem;

- Mbrojtje efektive dhe e besueshme kundër spamit; e cila do të përditësohet vazhdimisht për mbrojtje parandaluese kundër spamit dhe

- Lidhja e sistemit të informacionit (kompjuterët dhe serverët) me një rrjet energjetik përmes furnizimit të pandërprerë me energji.

- Masat nga paragrafi 1 i këtij neni zbatohen nga administratori dhe kontrollohen periodikisht në sistemin e informacioneve të Agjencisë.

- Subjekti i jashtëm duhet të njoftojë Agjencinë për ndryshimin e operatorit në mënyrë që t'i caktohet një emër i ri i përdoruesit dhe fjalëkalimi i ri. Emri i përdoruesit dhe fjalëkalimi i mëparshëm fshihen.

- Njoftimi nga paragrafi 3 i këtij neni bëhet edhe gjatë çdo ndryshimi tjetër të operatorit që ka ndikim në nivelin ose shtrirjen e qasjes së lejuar në të dhënat personale të marra përmes sistemit informativ të Agjencisë.

Masat organizative

Neni 11

Agjencia zbaton masat e duhura organizative për mbrojtjen e konfidencialitetit dhe përpunimit

të shtojcave personalë, dhe atë:

- qasja ose identifikimi i kufizuar për të hyrë në të dhënat personale;

- shkatërrimi i dokumenteve pas skadimit të afatit për ruajtjen e tyre në përputhje me rregullat për materialet e arkivës;

- vendosja e masave për sigurimin fizik të ambienteve të punës dhe pajisjeve të komunikimit të informacionit ku mblidhen, përpunohen dhe ruhen të dhënat personale dhe

- respektimi i udhëzimeve teknike gjatë instalimit dhe përdorimit të informacionit-pajisjet e komunikimit mbi të cilat përpunohen të dhënat personale Personi i punësuar që kryen punë për burimet njerëzore në Agjenci, me pëlqim paraprak nga ana e Kryetarit të Agjencisë, njofton administratorin e sistemit të informacionit për punësimin apo angazhimin e çdo personi të autorizuar me të drejtë të qasjes në sistemin e informacionit, për t'u caktuar një emër për përdoruesin dhe fjalëkalim, si dhe për pushimin e punësimit ose angazhimit në mënyrë që emri i përdoruesit dhe fjalëkalimi të fshihen, respektivisht të bllokohen për qasje të mëtutjeshme. Personi i punësuar që kryen punë për burimet njerëzore në Agjenci i raporton administratorit me shkrim.

Neni 12

Agjencia duhet të sigurojë masa për mbrojtjen e të dhënave personale gjatë përpunimit të automatizuar, të cilat përfshijnë leximin ose përpunimin e të dhënave personale në të cilat qasen subjektet e jashtme (shoqëritë pensionale, Fondi i sigurimit pensional dhe invalidor të Maqedonisë së Veriut dhe rojet e pasurisë së fondeve pensionale) dhe atë:

- Respektimi i konfidencialitetit dhe sigurisë së plotë të fjalëkalimeve dhe formave të tjera të identifikimit, të lëshuara zyrtarisht nga Agjencia për qasje në sistemin e informacionit që përmban të dhëna personale;

- Shkatërrimi elektronik i dokumenteve që përmbajnë të dhëna personale pas skadimit të periudhës së ruajtjes;

- Heqja e medias që është bartës i të dhënave personale (kompakt disk, disketë, kompjuter i lëvizshëm dhe media të tjera për transferimin e të dhënave) jashtë ambienteve të punës duhet të bëhet me leje dhe kontroll të veçantë për të parandaluar humbjen ose përdorimin e paligjshëm të tyre;

- Sigurimi i sigurisë fizike të ambienteve dhe pajisjeve të punës ku ruhen dhe përpunohen të dhënat personale; dhe

- Respektimi i udhëzimeve të përdorimit për përdorimin e një aplikacioni softuerik përmes të cilit qaset në sistemin e informacionit të Agjencisë, i cili përmban të dhëna personale, dhe mënyrën e shkarkimit të të dhënave personale prej tij.

Siguria fizike e sistemit të informacionit

Neni 13

Agjencia duhet të sigurojë sigurinë fizike të sistemit të informacionit. Serverët në të cilat janë instaluar programet softuerike për përpunimin e të dhënave personale, duhet të lokalizohen dhe administrohen fizikisht nga Agjencia.

Vetëm personat me autorizim të veçantë nga Agjencia mund të kenë qasje fizike në hapësirën ku ndodhen serverët.

Nëse një person tjetër ka nevojë për qasje në hapësirë dhe të dhënat personale të ruajtura në serverë, atëherë ai person duhet të shoqërohet dhe të mbikëqyret nga personi nga paragrafi 3 i këtij neni.

Hapësira ku ndodhen serverët është e mbrojtur nga rreziqet e mjedisit nëpërmjet zbatimit të masave dhe kontrolleve që reduktojnë rrezikun e kërcënimeve të mundshme duke përfshirë vjedhjen, zjarrin, shpërthimet, tymin; ujin, pluhurin, dridhjet, ndikimet kimike, pengesat në furnizimin me energji elektrike dhe rrezatimi elektromagnetik.

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 hostohen dhe të administrohen jashtë hapësirave të Agjencisë.

Në rastin e paragrafit 5 të këtij neni, të drejtat dhe detyrimet e ndërsjella të Agjencisë dhe personit juridik, gjegjësisht të personit fizik ku serverët vendosen fizikisht, hostohen dhe administrohen, duhet të rregullohen me kontratë në formë të shkruar, e cila domosdo do të përmbajë masa teknike dhe organizative për të garantuar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale.

Oficeri për mbrojtjen e të dhënave personale

Neni 8

Kryetari i Këshillit të ekspertëve të Agjencisë emëron një oficer për mbrojtjen e të dhënave personale i cili kryen këto detyra:

- merr pjesë në miratimin e vendimeve në lidhje me përpunimin e të dhënave personale, si dhe realizimin e të drejtave të subjekteve të të dhënave personale;

- ndjek pajtueshmërinë e veprimtarisë së Agjencisë me rregullat që kanë të bëjnë me përpunimin e të dhënave personale, me këtë rregullore dhe me dokumentacionin për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale;

- koordinon kontrollin e procedurave dhe udhëzimeve të përcaktuara në këtë rregullore dhe në dokumentacionin për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale dhe

- rekomandon trajnimin e të punësuarve në lidhje me mbrojtjen e të dhënave personale.

Informimi për mbrojtjen e të dhënave personale

Neni 9

Personat të cilët janë të punësuar ose të angazhuar në Agjenci, para se të fillojnë me punën e tyre, njihen me rregullullat për mbrojtjen e të dhënave personale, si dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

Për personat të cilët janë të angazhuar për kryerjen e punëve në Agjenci në kontratën për angazhimin e tyre, theksohen detyrimet dhe përgjegjësitë për mbrojtjen e të dhënave personale.

Agjencia para fillimit të drejtëpërdrejtë të punës së personave të autorizuar, në mënyrë shtesë informon për detyrimet dhe përgjegjësitë e drejtëpërdrejta për mbrojtjen e të dhënave personale.

Personat që janë të punësuar ose të angazhuar në Agjenci, para fillimit të punës, nënshkruajnë deklaratën për fshehtësi dhe mbrojtje të përpunimit të të dhënave personale, e cila i bashkangjitet këtij vendimi.

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 Agjencia, përveç nëse rregullohet ndryshe me ligj, dhe do t'i mbajnë konfidenciale të dhënat personale, si dhe masat për mbrojtjen e tyre.

Deklarata nga paragrafi (4) i këtij neni duhet të ruhet në dosjet e personave që janë të punësuar ose të angazhuar në Agjenci.

Agjencia duhet të informojë vazhdimisht personat e autorizuar për detyrimet dhe përgjegjësitë e drejtëpërdrejta për mbrojtjen e të dhënave personale.

Detyrimet dhe përgjegjësitë e administratorit të sistemit të informacionit

Neni 10

Agjencia përkufizon dhe përcakton detyrimet dhe përgjegjësitë e administratorit të sistemit të informacionit në Rregullat për përcaktimin e detyrimeve dhe përgjegjësive të administratorit të sistemit të informacionit dhe personave të autorizuar.

Oficeri për mbrojtjen e të dhënave personale në Agjenci duhet të kryejë kontroll periodik mbi punën e administratorit të sistemit të informacionit dhe të përgatisë raport për kontrollin e kryer.

Raporti nga paragrafi (2) i këtij neni duhet të përmbajë parregullsitë e konstatuara, nëse janë konstatuar të tilla, si dhe masat e propozuara për largimin e atyre parregullsive.

Detyrimet dhe përgjegjësitë e personave të autorizuar

Neni 11

Detyrimet dhe përgjegjësitë e secilit person të autorizuar i cili ka qasje në të dhëna personale dhe në sistemin e informacionit, Agjencia i përkufizon dhe përcakton në Rregullat për përcaktimin e detyrimeve dhe përgjegjësive të administratorit në sistemin e informacionit dhe të personave të autorizuar.

Agjencia detyrimisht i njofton personat e autorizuar nga paragrafi (1) i këtij neni me dokumentacionin për masat teknike dhe organizative lidhur me ushtrimin e detyrimeve dhe përgjegjësive të tyre.

Identifikimi dhe kontrollimi

Neni 12

Agjencia detyrimisht mban shënime për personat e autorizuar që kanë qasje të autorizuar në dokumente dhe sistemin e informacionit, si dhe vendos procedurat për identifikimin dhe kontrollimin e qasjes të autorizuar.

Kur kontrollimi kryhet në bazë të emrit të përdoruesit dhe fjalëkalimit, Agjencia zbaton gjithmonë rregullat që garantojnë konfidencialitetin dhe integritetin e tyre gjatë lajmërimit, caktimit dhe ruajtjes së të njëjtave.

Fjalëkalimet duhet të ndryshohen automatikisht pas një periudhe kohore që nuk mund të jetë më e gjatë se tre muaj.

Të dhënat e personave të autorizuar që kanë qasje të autorizuar në dokumente dhe

në sistemin e informacionit

Neni 13

Agjencia mban shënime për punonjësit që kanë qasje të autorizuar në dokumente dhe në sistemin e informacionit, i cili përmban:

- Emrin dhe mbiemrin e të punësuarit;
- Stacionin e punës dhe emrin e përdoruesit për të gjithë të punësuarit kur qasen në sistem, së bashku me nivelin e qasjes të autorizuar, datën dhe orën e qasjes dhe të dhënat personale në të cilat është qasur;
- Llojin e qasjes me operacionet e ndërmarra gjatë përpunimit të të dhënave;
- Regjistrim të autorizimit për çdo qasje;
- Regjistrim për çdo qasje të paautorizuar;
- Regjistrimi i refuzimit të automatizuar nga sistemi i informacionit dhe
- Identifikimi i një sistemi nga i cili bëhet një përpjekje e jashtme për qasje në funksionet operacionale ose të dhënat personale pa nivelin e kërkuar të autorizimit.

Kontrolli i qasjes

Neni 14

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.

Agjencia vendos mekanizma për të parandaluar personat e autorizuar nga qasja në të dhënave personale dhe në informacione dhe pajisjeve të komunikimit me të drejta të ndryshme nga ato për të cilat ata janë të autorizuar.

Administratori i sistemit të informacionit i cili është i autorizuar sipas Rregullave për përcaktimin e detyrimeve dhe përgjegjësive të administratorit të sistemit të informacionit dhe personave të autorizuar mund të japë, ndryshojë ose marrë qasjen e autorizuar në të dhënat personale dhe pajisjet e informacionit dhe komunikimit vetëm në bazë të i një urdhri nga ana e Kryetarit dhe në përputhje me kriteret e përcaktuara nga Agjencia.

Kontrolli i sistemit të informacionit dhe infrastrukturës së informacionit

Neni 15

Sistemi i informacionit dhe infrastruktura e informacionit e Agjencisë i nënshtrohet kontrollin e brendshëm dhe të jashtëm për të kontrolluar nëse procedurat dhe udhëzimet e përfshira në dokumentacionin për masat teknike dhe organizative zbatohen dhe janë në përputhje me rregulloret për mbrojtjen e të dhënave personale.

Agjencia kryen kontroll të jashtëm të sistemit të informacionit dhe infrastrukturës të TI çdo tre vjet, dhe kontroll të brendshëm çdo vit.

Kontrolli i jashtëm nga paragrafi (1) i këtij neni kryhet përmes përpunimit të dokumenteve nga ana e një palë të tretë të pavarur.

Në raportin nga kontrolli i kryer nga paragrafi (1) i këtij neni detyrimisht duhet të ketë një mendim për masën në të cilën procedurat dhe udhëzimet që përmban dokumentacioni për masat teknike dhe organizative zbatohen dhe janë në përputhje me rregulloret për mbrojtjen e të dhënave personale, për të theksuar mangësitë e konstatuara, si dhe ato masa të propozuara të nevojshme korrigjuese ose plotësuese për heqjen e tyre.

Raporti nga paragrafi (4) i këtij neni duhet të përmbajë të dhënat dhe faktet në bazë të së cilave është përgatitur mendimi dhe janë propozuar masat për heqjen e mangësive të konstatuara.

Raportin nga paragrafi (4) i këtij neni e analizon oficeri për mbrojtjen e të dhënave personale, i cili i parashtron kontrolluesit propozime për ndërmarrjen e masave të nevojshme korrigjuese ose masave shtesë, për të hequr mangësitë e konstatuara.

Menaxhimi me mediat

Neni 16

Transferimi i mediave jashtë ambienteve të punës kryhet vetëm me autorizim paraprak me hkrim nga Kryetari i Agjencisë.

Për mediat e transmetuara jashtë ambienteve të punës së Agjencisë, ndërmerren masat e nevojshme për të parandaluar përpunimin e paautorizuar të të dhënave personale të regjistruara në to.

Shkatërrimi, fshirja ose pastrimi i medias

Neni 17

Pas transferimit të të dhënave personale nga media ose pas skadimit të periudhës së caktuar për ruajtje, media duhet të shkatërrohet, fshihet ose pastrohet nga çdo e dhënë personale e regjistruar në të.

Shkatërrimi i medias kryhet duke e ndarë mekanikisht në pjesë përbërëse, në mënyrë që të mos përdoret më.

Fshirja ose pastrimi i medias duhet të bëhet në një mënyrë që parandalon ripërtrirjen e mëtutjeshme të të dhënave personale të regjistruara.

Për rastet e parashikuara në paragrafët (2) dhe (3) të këtij neni, komisioni harton një raport, i cili përmban të gjitha të dhënat për identifikimin e plotë të medias, si dhe për kategoritë e të dhënave personale të regjistruara në të njëjtln.

Identifikimi dhe kontrollimi

Neni 18

Agjencia duhet të krijojë mekanizma që do të mundësojnë identifikimin e qartë të çdo personi të autorizuar që ka hyrë në sistemin e informacionit dhe mundësinë e kontrollit të autorizimit për çdo person të autorizuar.

Kontrolli i qasjes fizike

Neni 19

Në dokumentacionin për masat teknike dhe organizative, Agjencia ka përcaktuar kritere për personat e autorizuar që mund të kenë qasje në ambientet ku ndodhet sistemi i informacionit.

Evidentimi i incidenteve

Neni 20

Në rregullat për raportimin, reagimin dhe sanimin e incidenteve. Agjencia përcakton procedurat që zbatohen për rikthimin e të dhënave personale dhe mënyrën e evidentimit të personave të autorizuar që kanë kryer operacionet për kthimin e të dhënave personale, kategoritë e të dhënave personale që janë kthyer dhe që janë futur manualisht gjatë kthimit.

Për rikthimin e të dhënave personale, Agjencia lëshon autorizim me shkrim për administratorin e sistemit të informacionit.

Kopjet e sigurta

Neni 21

Agjencia duhet të kryejë regjistrimin e rregullt të kopjes të sigurtë dhe arkivimin e të dhënave në sistem, për të shmangur humbjen ose shkatërrimin e tyre.

Kopjet e sigurta duhet të bëhen çdo ditë pune dhe në fund të javës së punës, dhe nëse është e nevojshme, çdo ditë pune të fundit të muajit.

Kopjet e sigurta duhet të bëhen në një mënyrë që do të garantojë mundësinë e përhershme të rindërtimit të të dhënave personale në gjendjen në të cilën ishin para se të humbisnin ose shkatërroheshin.

Kopjet e sigurta që ruhen në një vend tjetër të largët nga vendi ku ndodhet sistemi i informacionit duhet të mbrohen në mënyrë fizike dhe kriptografike, në mënyrë që të parandalohet çdo modifikim.

Oficeri për mbrojtjen e të dhënave personale dhe administratori kontrollojnë zbatimin e masave nga ky nen.

Kopjet e sigurta duhet të bëhen në fund të javës së punës në një mënyrë që do të garantojë një mundësi të përhershme për të rindërtuar të dhënat personale në gjendjen në të cilën ishin përpara se të humbisnin ose shkatërroheshin.

Qasja në dokumente

Neni 22

Qasja në dokumente është kufizuar vetëm për personat e autorizuar të Agjencisë.

Për qasjen në dokumente, duhet të krijohen mekanizma për identifikimin e personave të autorizuar dhe për kategoritë e të dhënave personale në të cilat qasen ato persona.

Nëse nevojitet qasja e një personi tjetër në dokumente, për këtë qëllim janë vendosur procedurat përkatëse me dokumentacionin për masat teknike dhe organizative.

Rregulla e "tavolinës së pastër"

Neni 23

Agjencia zbaton detyrimisht rregullën e "tavolinës së pastër" gjatë përpunimit të të dhënave personale të përfshira në dokumentet për mbrojtjen e tyre gjatë gjithë procesit të përpunimit nga qasja e personave të paautorizuar.

Mënyra e ruajtjes së dokumenteve

Neni 24

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

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

Kur karakteristikat fizike të hapësirave nuk lejojnë zbatimin e masave nga paragrafi 2 i këtij neni, Agjencia duhet të zbatojë masa të tjera për të parandaluar çdo qasje të paautorizuar në dokumente.

Shkatërrimi i dokumenteve

Neni 25

Shkatërrimi i dokumenteve bëhet me copëtim ose në një mënyrë tjetër, ku ato nuk mund të përdoren më.

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.

Kopjimi ose shumëzimi i dokumenteve

Neni 26

Kopjimi ose shumëzimi i dokumenteve mund të bëhet vetëm nën kontrollin e personave të autorizuar të Agjencisë, dhe asgjësimi i kopjeve ose dokumenteve të shumëzuara duhet të bëhet në atë mënyrë që të parandalojë ripërtrirjen e mëtejshme të të dhënave personale të përmbajtura.

III. Niveli i lartë i masave për siguri të përpunimit të të dhënave personale

Neni 27

Një nivel i lartë i masave teknike dhe organizative për sigurinë e përpunimit të të dhënave personale përfshin këto lloje masash: transferim të kriptuar të dokumenteve, kopjim ose shumëzim i dokumenteve pas autorizimit paraprak dhe mbrojtje gjatë transferimit fizik të dokumenteve.

Neni 28

Agjencia duhet të sigurojë mbrojtjen e të dhënave personale gjatë shkëmbimit të tyre me subjekte të jashtme përmes mediave dhe rrjetit të komunikimit elektronik, duke mundësuar një lidhje të kriptuar të shkëmbimit, rregulla strikte për identifikimin gjatë shkëmbimit (fjalëkalime të vështira për t'u thyer) dhe nënshkrimin elektronik të dokumenteve të shkëmbimit. Dokumentet e kriptuara mund të dekriptohen vetëm nga administratori ose një person i autorizuar prej tij.

Masat mbrojtëse nga paragrafi 1 i këtij neni Agjencia mund t'i bartë te subjektet e jashtme me nënshkrimin e kontratës.

Neni 29

Kopjimi ose shumëzimi i dokumenteve që përmbajnë të dhëna personale mund të bëhet vetëm me autorizim paraprak me shkrim nga Kryetari i këshillit të ekspertëve të Agjencisë.

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

Neni 32

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

IV. Dispozitat kalimtare dhe përfundimtare

Me datën e miratimit të këtyre Rregullave, pushon të vlejë Rregullorja për masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjen e përpunimit të të dhënave personale nr.01-528/9 datë 27.4.2015

Këto rregulla hyjnë në fuqi në ditën e miratimit të tyre dhe të njëjtat do të shpallen në tabelën e shpalljeve të Agjencisë.

Përgatiti: Emilija Ramova
16.8.2021 E. Ramova

Kryetar i Këshillit të ekspertëve
Maksud Ali

MAPAS
Agjencia për mbikëqyrje
të financimit kapital të
sigurimit pensional