Република Северна Македонија
Дирекција за безбедност
на класифицирани информации

Бр./Nr. _____
Скопје/Shkup, _____ година

Врз основа на член 75 став 1 од Законот за класифицирани информации(*) („Службен весник на Република Северна Македонија“ бр. 275/19), член 55 став 2 од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија“ бр. 58/00, 44/02, 82/08, 167/10, 51/11 и „Службен весник на Република Северна Македонија“ бр. 96/19, 110/19), а во врска со член 119 и 120 од Законот за заштита на личните податоци(*) („Службен весник на Република Северна Македонија“ бр. 42/20) и согласно член 21 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), директорот на Дирекцијата за безбедност на класифицирани информации донесе

Në mbështetje të nenit 75, paragrafi 1 të Ligjit të Informacioneve të Klasifikuara(*)(“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 275/19), nenit 55, paragrafi 2 të Ligjit të Organizimit dhe të Punës së Organeve të Administratës Shtetërore (“Gazeta Zyrtare e Republikës së Maqedonisë” nr. 58/00, 44/02, 82/08, 167/10, 51/11 dhe “Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 96/19, 110/19), a në lidhje me nenet 119 dhe 120 të Ligjit të Mbrojtjes së të Dhënave Personale (*) (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 42/20) dhe në mbështetje të nenit 21 të Rregullores së sigurisë për përpunimin e të dhënave personale (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 122/20), drejtori i Drejtorisë së Sigurisë së Informacioneve të Klasifikuara, miratoi

ПРАВИЛНИК ЗА НАЧИНОТ НА ПРЕВЕНИРАЊЕ И УПРАВУВАЊЕ СО ИНЦИДЕНТИ КОИ ЈА НАРУШУВААТ ДОВЕРЛИВОСТА, ИНТЕГРИТЕТОТ ИЛИ ДОСТАПНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

RREGULLORE PËR MËNYRËN E PARANDALIMIT DHE MENAXHIMIT TË INCIDENTEVE QË SHKELIN BESUESHMËRINË, INTEGRITETIN APO QASJEN TE TË DHËNAT PERSONALE

Член 1

Со овој правилник се пропишува

Neni 1

Kjo rregullore përcakton mënyrën e

начинот на превенирање и управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци во Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата).

parandalimit dhe menaxhimit të incidenteve që cenojnë besueshmërinë, integritetin ose disponueshmërinë e të dhënave personale në Drejtorinë e Sigurisë së Informacioneve të Klasifikuara (në tekstin e mëtejmë: Drejtoria).

Дефиниција

Член 2

Во смисла на овој правилник:

- „инцидент“ е секое нарушување на доверливоста, интегритетот или достапноста на личните податоци, вклучително и по информацискиот систем на којшто се обработуваат личните податоци;
- „управување со инциденти“ опфаќа пријавување, реакција, санирање и евиденција на инцидентите.

Definicioni

Neni 2

Në kuptim të kësaj rregulloreje:

- - "incident" është çdo shkelje e besueshmërisë, integritetit ose disponueshmërisë së të dhënave personale, duke përfshirë sistemin e informacionit në të cilin përpunohen të dhënat personale;
- "Menaxhimi i incidentit" përfshin raportimin, reagimin, korrigjimin dhe regjistrimin e incidenteve.

Превенирање на инциденти

Член 3

Дирекцијата ги презема следните мерки и контроли за превенирање на инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци:

- користење на непрекинато напојување за да се заштити опремата што се користи за обработка на личните податоци;
- едновремена употреба на повеќе уреди во низа за зачувување на личните податоци;
- заштита од пожар, експлозии,

Parandalimi i incidenteve

Neni 3

Drejtoria i ndërmerr këto masa dhe kontrollet e mëposhtme, për të parandaluar incidentet që cenojnë besueshmërinë, integritetin ose qasjen e të dhënave personale:

- përdorimi i furnizimit me energji të pandërprerë për të mbrojtur pajisjet e përdorura për përpunimin e të dhënave personale;
- përdorimi i njëkohshëm i pajisjeve të shumta në sekuencë për të ruajtur të dhënat personale;
- mbrojtje nga zjarri, shpërthimet,

прашина, вода, кражба, пречки во напојување со електрична енергија, електромагнетно зрачење во просторијата во којашто се сместени серверите;

pluhuri, uji, vjedhjet, ndërhyrjet në furnizimin me energji elektrike, rrezatimi elektromagnetik në dhomën ku ndodhen serverët;

- во случај на прекин на напојување со електрична енергија, системот треба да биде обезбеден со уред за непрекинато напојување (UPS) како секундарен механизам;
- në rast të ndërprerjes së energjisë elektrike, sistemi duhet të pajiset me një furnizim me energji të pandërprerë (UPS) si mekanizëm dytësor;
- инсталирање на алармни уреди против упад и нивна периодична проверка;
- instalimi i pajisjeve të alarmit kundër ndërhyrjeve dhe inspektimi periodik i tyre;
- обезбеден пристап до просториите во коишто се чуваат безбедносните клучеви и шифрите за аларм;
- qasje e sigurt në ambientet ku mbahen çelësat e sigurisë dhe kodet e alarmit;
- контрола за пристап до сервер-собата;
- kontrolli i qasjes në dhomën e serverit;
- ажуриран список на лица или категории на лица кои се овластени да влезат во просториите каде што се чува опрема на којашто се врши обработка на лични податоци;
- një listë të përditësuar të personave ose kategorive të personave që janë të autorizuar të hyjnë në ambientet ku mbahen pajisjet në të cilat përpunohen të dhënat personale;
- воспоставување на правила и методи за контрола на пристапот на посетителите во Дирекцијата и тоа минимум со придружба од едно лице на посетителите надвор од утврдена локација за прием на странки;
- vendosja e rregullave dhe metodave për kontrollin e hyrjes së vizitorëve në Drejtori dhe së paku i shoqëruar nga një person për vizitorët jashtë një lokacioni të caktuar për pritjen e palëve;
- одржување на сервер-собата (климатизација, инсталација на UPS уред, итн.);
- mirëmbajtjen e dhomës së serverit (ajri i kondicionuar, instalimi i një pajisjeje UPS, etj.);
- применување на политиката за „чист екран и чисто биро“;
- aplikimi i politikës "ekran i pastër dhe tavolinë e pastër";
- чување на документите во хартиена форма на начин што ќе оневозможи пристап до истите од страна на неовластено лице (на пр. во ормари за чување документи со клуч до кои пристап има
- ruajtja e dokumenteve në formë letre në një mënyrë që do të parandalojë qasjen në to nga një person i paautorizuar (p.sh. në dollapët e ruajtjes së dokumenteve me çelës, tek i cili ka qasje personi

овластеното лице за обработка на податоците).

i autorizuar për përpunimin e të dhënave).

Пријавување на инцидент

Член 4

(1) Секое овластено лице е должно веднаш да го пријави инцидентот кај офицерот а заштита на личните податоци.

(2) Во случај на инцидент поврзан со информацискиот систем на кој што се врши обработка на лични податоци, корисникот кој го забележал инцидентот е должен веднаш да го пријави инцидентот кај администраторот на информацискиот систем.

(3) Пријавување на инцидентот од ставот (2) на овој член се врши во електронска и/или во писмена форма, пришто се наведуваат следните податоци за инцидентот:

- време на настанување на инцидентот;
- траење и престанување на инцидентот;
- место во информацискиот систем каде што се појавил инцидентот;
- податок или проценка на обемот, односно опсегот на инцидентот;
- име и презиме на овластеното лице коешто го пријавува инцидентот;
- име и презиме на овластените лица до коишто е поднесена пријавата за инцидентот.

(4) Во функција на побрзо преземање мерки за управување со настанатиот инцидент, се препорачува овластеното лице што го пријавува инцидентот, покрај пријавата во електронска и/или во писмена форма, и телефонски да го извести администраторот на

Raportimi i incidentit

Neni 4

(1) Çdo person i autorizuar është i obliguar që menjëherë t'ia raportojë incidentin zyrtarit për mbrojtjen e të dhënave personale

2) Në rast incidenti në lidhje me sistemin e informacionit mbi të cilin përpunohen të dhënat personale, përdoruesi që ka vërejtur incidentin është i detyruar të raportojë menjëherë incidentin tek administratori i sistemit të informacionit.

Raportimi i incidentit nga paragrafi (2) i këtij neni bëhet në formë elektronike dhe/ose me shkrim, me këto të dhëna për incidentin:

- koha e ndodhjes së incidentit;
- kohëzgjatja dhe përfundimi i incidentit;
- vend në sistemin e informacionit ku ka ndodhur incidenti;
- të dhënat ose vlerësimi i shtrirjes, domethënë fushëveprimit të incidentit;
- emri dhe mbiemri i personit të autorizuar që raporton incidentin;
- emri dhe mbiemri i personave të autorizuar të cilëve u është dorëzuar raporti për incidentin.

(4) Për marrjen e masave për menaxhimin më të shpejtë të incidentit, rekomandohet që personi i autorizuar që raporton incidentin, përveç raportit në formë elektronike dhe/ose me shkrim, ta njoftojë edhe administratorin e sistemit informativ nëpërmjet telefonit, në lidhje

информацискиот систем за поднесената пријава за инцидент.

me raportin e paraqitur të incidentit.

Реакција во случај на пријавен инцидент

Член 5

(1) По приемот на пријавата за инцидентот, администраторот на информацискиот систем го известува директорот на Дирекцијата и веднаш започнува со санирање на инцидентот, врши проценка на причините за појавување на инцидентот, како и утврдување на тоа дали и кои мерки треба да се преземат за евентуално дополнително санирање и за спречување на негово повторување во иднина.

(2) Доколку се работи за инцидент што се повторува, администраторот на информацискиот систем е должен да преземе мерки кои ќе гарантираат трајно отстранување на ризикот за настанување на инцидентот.

(3) Во случај на инцидент за којшто е потребна стручна помош од надворешни лица, администраторот на информацискиот систем во координација со офицерот за заштита на личните податоци, ги презема сите мерки за заштита личните податоци и информациите што се обработуваат на информацискиот систем.

Reagimi në rast të ndonjë incidenti të raportuar

Neni 5

(1) Pas marrjes së raportit për incidentin, administratori i sistemit informativ, e njofton drejtorin e Drejtorisë dhe menjëherë fillon me sanimin e incidentit, vlerëson arsyet e ndodhjes së incidentit, si dhe përcakton nëse dhe cilat masa duhen marrë. për riparime të mundshme shtesë dhe për të parandaluar përsëritjen e tij në të ardhmen.

2) Nëse bëhet fjalë për incident të përsëritur, administratori i sistemit të informacionit është i detyruar të marrë masa që garantojnë heqjen e përhershme të rrezikut të ndodhjes së incidentit.

(3) Në rast incidenti që kërkon ndihmë profesionale nga të huajt, administratori i sistemit informativ, në koordinim me zyrtarin për mbrojtjen e të dhënave personale, ndërmerr të gjitha masat për mbrojtjen e të dhënave personale dhe informacionit të përpunuar në sistemin informativ.

Санирање на инциденти

Член 6

(1) Инцидентот може да го санира само стручно лице овластено за таа цел од страна на директорот на Дирекцијата.

(2) По спроведената постапка за санирање на инцидентот, овластеното

Sanimi i incidenteve

Neni 6

(1) Incidentin mund ta sanojë vetëm eksperti, i autorizuar për atë qëllim nga ana e drejtorit të Drejtorisë.

(2) Pas kryerjes së procedurës për sanimin e incidentit, personi i autorizuar nga

лице од ставот (1) на овој член изготвува извештај за реакција по пријавениот инцидент.

(3) Во случај кога заради санација е потребно овластеното лице да пристапи до персоналните компјутери или серверот, тогаш датотеките во кои се чуваат и обработуваат личните податоци не треба да бидат достапни за него.

(4) Доколку при санацијата на инцидентот се јави потреба од влегување во датотеките со лични податоци, тогаш корисникот на чиешто работно место настанал инцидентот го внесува своето корисничко име и лозинка без притоа да дозволи овластеното лице за санирање да ја забележи/открие лозинката.

(5) Во случај на откривање на лозинката, по завршување на постапката за санација на инцидентот, лозинката се уништува и на корисникот му се овозможува креирање на нова лозинка.

(6) Во случај ако при санација на инцидентот овластеното лице сепак дојде во контакт со личните податоци, тоаш тоа лице задолжително ја потполнува и потпишува Изјавата за тајност и заштита на обработката на личните податоци.

(7) За време на санацијата на инцидентот, покрај овластеното лице за санирање задолжително е присуството на корисникот на персоналниот компјутер, а во случај на инцидент на серверот, задолжително е присуството на администраторот на информацискиот систем кој има право на пристап до серверот.

(8) Ако за време на санацијата на инцидентот дојде до оштетување или уништување на личните податоци, тогаш овластеното лице за санација тоа го констатира во извештајот од ставот (2) на

paragrafi (1) i këtij neni, përgatit raport për reagim pas incidentit të raportuar.

(3) Në rast se me qëllim të sanimit është e nevojshme që personi i autorizuar të ketë qasje në kompjuterët personalë ose në server, atëherë dosjet në të cilat ruhen dhe përpunohen të dhënat personale nuk duhet të jenë të aksesueshme për të.

(4) Nëse gjatë sanimit të incidentit ka nevojë për qasje në dosjet me të dhëna personale, atëherë përdoruesi në vendin e punës të të cilit ka ndodhur incidenti e shënon emrin e përdoruesit dhe fjalëkalimin e tij pa lejuar që personi i autorizuar për riparim të shënojë/zbulojë fjalëkalimin.

(5) Në rast se fjalëkalimi zbulohet, pas përfundimit të procedurës së korrigjimit të incidentit, fjalëkalimi shkatërrohet dhe përdoruesi lejohet të krijojë një fjalëkalim të ri.

(6) Në rast se gjatë korrigjimit të incidentit, personi i autorizuar ende vjen në kontakt me të dhënat personale, ai person duhet të plotësojë dhe nënshkruajë Deklaratën për fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale.

(7) Gjatë sanimit të incidentit, përveç personit të autorizuar për riparim, është e detyrueshme prania e shfrytëzuesit të kompjuterit personal, ndërsa në rast të incidentit në server është e detyrueshme prania e administratorit të sistemit informativ, që ka të drejtë qasjeje në server.

(8) Nëse gjatë sanimit të incidentit ndodh dëmtimi ose asgjësimi i të dhënave personale, atëherë personi i autorizuar për sanim këtë e konstaton në raportin nga paragrafi (2) i këtij neni. Raporti i

овој член. Извештајот се доставува до администраторот на информацискиот систем кој врз основа на извештајот, а по претходно добиено овластување од директорот на Дирекцијата, пристапува кон повторно внесување, односно враќање на личните податоци во системот.

dorëzohet administratorit të sistemit të informacionit, i cili në bazë të raportit dhe pasi ka marrë paraprakisht autorizimin nga drejtori i Drejtorisë, procedon me rifutjen, pra kthimin e të dhënave personale në sistem.

Евиденција на инциденти

Член 7

(1) Администраторот на информацискиот систем води евиденција на инцидентите.

(2) Евиденцијата од ставот (1) на овој член ги содржи следните податоци:

- датум кога настанал инцидентот;
- име и презиме на лицето коешто го пријавило инцидентот;
- вид на инцидент;
- мерки што се преземени за санација на инцидентот;
- име и презиме на лицето коешто го санирало инцидентот;
- датум на санирање на инцидентот.

(3) При повторно внесување, односно враќање на личните податоци во системот, задолжително и во електронска форма се врши евидентирање на овластените лица коишто ја извршиле операцијата за враќање на податоците, категориите на личните податоци кои биде вратени и кои биле рачно внесени при враќањето.

(4) Евиденцијата од ставот (1) на овој член по правило се чува најмалку пет години, односно најмногу до 10 години по замена на оперативниот систем на информацискиот систем.

Evidentimi i incidenteve

Neni 7

(1) Administratori i sistemit informativ mban evidencë për incidentet.

(2) Procesverbali nga paragrafi (1) i këtij neni, i përmban këto të dhëna:

- datën kur ka ndodhur ngjarja;
- emri dhe mbiemri i personit që ka raportuar incidentin;
- lloji i incidentit;
- masat e marra për sanimin e incidentit;
- emri dhe mbiemri i personit që ka riparuar incidentin;
- data e riparimit të incidentit.

(3) Me rastin e futjes, përkatësisht kthimit të të dhënave personale në sistem, personat e autorizuar që kanë kryer operacionin e kthimit të të dhënave, kategoritë e të dhënave personale që janë kthyer dhe që janë futur manualisht gjatë kthimit, duhet të regjistrohen në formë elektronike.

(4) Evidenca nga paragrafi (1) i këtij neni, si rregull, ruhet së paku pesë vjet, përkatësisht deri në 10 vjet pas ndërrimit të sistemit operativ të sistemit informativ.

Влегување во сила

Hyrja në fuqi

Член 8

Овој правилник влегува во сила на денот на неговото донесување и се објавува на веб-страната на Дирекцијата.

Neni 8

Kjo rregullore hyn në fuqi ditën e miratimit dhe publikohet në faqen e internetit të Drejtorisë.

Директор/ Drejtori

Стојан Славески