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 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 организација 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 член 47 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 pajtim me nenin 75, paragrafi 1 të Ligjit të Informacioneve të Klasifikuara (*) (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 275/19), neni 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), e 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 nenit 47 të Rregullores për sigurinë dhe 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 ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ДИРЕКЦИЈАТА ЗА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

RREGULLORE PËR MASAT TEKNIKE DHE ORGANIZATIVE PËR SIGURIMIN E KONFIDENCIALITETIT DHE TË MBROJTJES SË PËRPUNIMIT TË TË DHËNAVE PERSONALE NË DREJTORINË E SIGURISË SË INFORMACIONEVE TË KLASIFIKUARA

I. Општи одредби

Член 1

Со овој правилник се пропишуваат техничките и организациските мерки што Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата) во својство на контролор ги применува за обезбедување тајност и заштита на обработката на личните податоци.

Член 2

Одредбите од овој правилник се применуваат за:
целосна или делумна автоматизирана обработка на личните податоци и рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Член 3

Дирекцијата ја евидентира и ја чува документацијата за софтверските програми за обработка на личните податоци и за сите нејзини промени.

Технички и организациски мерки

Член 4

(1) Дирекцијата применува технички и организациски мерки кои обезбедуваат тајност и заштита на обработката на личните податоци соодветно на природата, обемот, контекстот и целите на обработката, како и на ризиците при нивната обработка.

(2) Техничките и организациските мерки од ставот (1) на овој член се применуваат пропорционално на

I. Dispozitat e përgjithshme

Neni 1

Me këtë rregullore përcaktohet masat teknike dhe organizative që Drejtoria e Sigurisë së Informacioneve të Klasifikuara (në tekstin e mëtejmë: Drejtoria) në cilësinë e kontrollorit i zbaton për të siguruar konfidencialitetin dhe mbrojtjen e përpunimit të të dhënave personale.

Neni 2

Dispozitat e kësaj rregulloreje zbatohen për:
përpunimin e plotë ose të pjesshëm të automatizuar të të dhënave personale dhe përpunimin manual të të dhënave personale që janë pjesë e një përmbledhjeje ekzistuese të të dhënave personale ose që synojnë të jenë pjesë e përbmledhjes së të dhënave personale.

Neni 3

Drejtoria e evidenton dhe e ruan dokumentacionin për programet softuerike të përpunimit të të dhënave personale dhe për të gjitha ndryshimet e tij.

Masat dhe teknikat organizative

Neni 4

(1) Drejtoria zbaton masa teknike dhe organizative që sigurojnë fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale në përputhje me natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit, si dhe rreziqet gjatë përpunimit të tyre.

(2) Masat teknike dhe organizative sipas paragrafit (1) të këtij neni zbatohen proporcionalisht në aktivitetet për

активностите за обработка на личните податоци и се класифицирани во две нивоа:

- стандардно ниво и високо ниво.

Член 5

(1) Техничките и организациските мерки на стандардно ниво се применуваат задолжително на сите збирки на лични податоци.

(2) За документите што содржат: посебни категории на лични податоци, лични податоци што се обработуваат за полициски цели и лични податоци што се обработуваат заради заштита на државната безбедност и одбраната на Република Северна Македонија, за документите што се пренесуваат преку комуникациско-информациски мрежа, а содржат посебни категории на лични податоци и/или единствен матичен број на граѓанинот (ЕМБГ), задолжително се применуваат технички и организациски мерки на стандардно и на високо ниво.

СТАНДАРДНО НИВО

1. Технички мерки

Член 6

Дирекцијата применува соодветни технички мерки за обезбедување на тајност и заштита на обработката на личните податоци, и тоа:

единствено корисничко име и лозинка за секое овластено лице;

лозинка составена од комбинација од осум алфанумерички карактери – букви (мали и големи) и специјални знаци;

корисничко име и лозинка кое овозможува пристап на овластеното лице до информациските систем во

përpunimin e të dhënave personale dhe klasifikohen në dy nivele:

- niveli standard dhe niveli i lartë.

Neni 5

(1) Masat teknike dhe organizative në nivel standard zbatohen detyrimisht për të gjitha përmbledhjet e të dhënave personale.

(2) Për dokumentet që përmbajnë: kategori të veçanta të të dhënave personale, të dhëna personale që përpunohen për qëllime policore dhe të dhëna personale që përpunohen me qëllim të mbrojtjes së sigurisë shtetërore dhe mbrojtjes së Republikës së Maqedonisë së Veriut, për dokumentet që transmetohen nëpërmjet një rrjeti komunikimi-informativ, dhe të përmbajnë kategori të veçanta të të dhënave personale dhe/ose numrin e vetëm amë të qytetarit (NVAQ), në mënyrë obligative zbatohen masa teknike dhe organizative në nivel standard dhe nivel të lartë.

NIVELI STANDARD

Masat teknike

Neni 6

Drejtoria zbaton masat e duhura teknike për të garantuar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, edhe atë:

emri i përdoruesit dhe fjalëkalimi për çdo person të autorizuar;

fjalëkalim i përbërë nga kombinimi i tetë karaktereve alfanumerike - shkronja (të vogla dhe të mëdha) dhe karaktere speciale;

emri i përdoruesit dhe fjalëkalimi që mundëson qasjen e personit të autorizuar në sistemin informativ në tërësi, qasje në

целина, пристап до поединечни апликации и/или поединечни збирки на личните податоци потребни при извршување на работните задачи;

aplikacione individuale dhe/ose koleksione individuale të të dhënave personale të nevojshme në kryerjen e detyrave të punës;

најава во информацискиот систем во којшто се обработуваат, чуваат и управуваат податоците преку воспоставените системи преку квалификуван дигитален сертификат и единствено корисничко име и лозинка за секое овластено лице на дигиталниот сертификат;

hyrje në sistemin e informacionit në të cilin të dhënat përpunohen, ruhen dhe menaxhohen përmes sistemeve të krijuara përmes një certifikate digjitale të kualifikuar dhe emri i përdoruesit dhe fjalëkalimi për çdo person të autorizuar të certifikatës digjitale;

евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем и постапки за идентификација и проверка на авторизираниот пристап;

të dhënat e personave të autorizuar që kanë qasje të autorizuar në dokumente dhe në sistemin informativ dhe procedurat për identifikimin dhe verifikimin e qasjes së autorizuar;

правила на доверливост и интегритет при пријавување, доделување и чување на лозинки и автоматско менување по изминат период од три месеци;

rregullat e konfidencialitetit dhe integritetit gjatë regjistrimit, dhënia dhe ruajtja e fjalëkalimeve dhe ndryshimit automatik të tyre pas një periudhe prej tre muajsh;

автоматизирано одјавување од информацискиот систем по изминување на одреден период на неактивност (не подолг од 15 минути) и за повторно активирање на системот со одново внесување на корисничкото име и лозинката;

çregjistrim të automatizuar nga sistemi i informacionit pas një periudhe të caktuar pasiviteti (jo më shumë se 15 minuta) dhe riaktivizimi i sistemit duke rifutur emrin e përdoruesit dhe fjalëkalimin;

автоматизирано отфрлање на информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име и лозинка) и автоматизирано известување на корисникот дека треба да побара упатство од администраторот на системот;

refuzimi i automatizuar i sistemit të informacionit pas tri përpjekjeve të dështuara për hyrje (shënimi i emrit të përdoruesit dhe fjalëkalimit të gabuar) dhe njoftimi i automatizuar i përdoruesit se ai duhet të kërkojë udhëzime nga administratori i sistemit;

инсталирана хардверска/софтверска заштитна мрежна бариера (firewall) или рутер помеѓу информацискиот систем и интернет или која било друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;

mbrojtje e instaluar harduerike/softuerike (firewall) ose ruter ndërmjet sistemit të informacionit dhe internetit ose çdo forme tjetër të rrjetit të jashtëm, si masë mbrojtëse ndaj përpjekjeve të paautorizuara ose me qëllim të keq për të hyrë ose depërtuar në sistem;

ефективна и сигурна антивирусна заштита и антиспајвер заштита на информацискиот систем која постојано ќе се ажурира заради превентивна заштита од непознати и непланирани закани од нови вируси и шпионски софтвери (spyware);

mbrojtje efektive dhe të sigurt antivirus dhe mbrojtje antispajuer të sistemit informativ i cili do të përditësohet vazhdimisht për mbrojtje parandaluese kundër kërcënimeve të panjohura dhe të paplanifikuara nga viruset e reja dhe softuerëve spiunë (spyware);

ефективна и сигурна антиспам заштита која постојано ќе се ажурира заради превентивна заштита од спамови;

mbrojtje efektive dhe e sigurt antispam që do të përditësohet vazhdimisht për mbrojtje parandaluese kundër spameve;

приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување (UPS уред);

lidhja e sistemit të informacionit (kompjuterët dhe serverët) me rrjetin elektrik përmes një pajisjeje të furnizimit me energji të pandërprerë (pajisje UPS);

обезбедување на веб-страната на Дирекцијата со примена на технички мерки со кои се гарантира идентитетот на страната и интегритетот и доверливоста на информациите на страната;

sigurimin e faqes së internetit të Drejtorisë duke aplikuar masa teknike që garantojnë identitetin e faqes dhe integritetin dhe konfidencialitetin e informacionit në sajt;

редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;

softuer antivirus i përditësuar rregullisht dhe një politikë e përcaktuar për përditësime të rregullta të programeve softuerike;

зачувување на податоците на корисниците на серверите на Дирекцијата за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително користење на мерки за синхронизација или резервни дополнителни мерки за заштита врз основа на анализа на ризикот;

ruajtja e të dhënave të përdoruesve në serverët e Drejtorisë, të cilët rezervohen rregullisht, dhe në rast se të dhënat ruhen në nivel lokal, përdorimi i detyrueshëm i masave të sinkronizimit ose rezervimi i masave shtesë mbrojtëse bazuar në analizën e rrezikut;

ограничување на опцијата за приклучување на преносливите медиуми (USB, DVD, CD, надворешни хард дискови и слично) кон системите со примарна важност;

kufizimi i opsionit për lidhjen e medieve të bartshme (USB, DVD, CD, hard disk të jashtëm, etj.) me sistemet parësore;

исклучен автоматски режим на работа на преносливите медиуми (Disable Autorun for Removable Media);

regjim i çaktivizuar automatik për punën e medieve të lëvizshme (Disable Autorun for Removable Media);

алатките за далечинска администрација мора да бидат

нагодени на начин што претходно задолжително треба да обезбедат согласност од овластеното лице од Дирекцијата на работната станица на корисникот пред каква било интервенција на самата работна станица;

mjetet për administrim në distancë duhet patjetër duhet të vendosen në mënyrë të tillë që të sigurojnë fillimisht pëlqimin e personit të autorizuar nga Drejtoria e stacionit të punës së përdoruesit përpara çdo ndërhyrjeje në vetë stacionin e punës;

нагодување на информацискиот систем кое ќе обезбеди овластеното лице од Дирекцијата да врши далечинска администрација на работната станица на корисникот, како и приказ за тоа кога истата завршила (на пр. со прикажување на порака на екранот дека далечинската администрација завршила);

vendosja e sistemit të informacionit që do të sigurojë që personi i autorizuar nga Drejtoria të kryejë administrimin në distancë të stacionit të punës së përdoruesit, si dhe pasqyrë se kur ka përfunduar (p.sh. duke shfaqur mesazh në ekran që administrimi në distancë ka përfunduar);

забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;

ndalimi i punës me programe softuerike të shkarkuara që nuk vijnë nga burime të sigurta;

ограничување на употребата на софтверски програми што бараат администраторски права;

kufizimi i përdorimit të programeve softuerike që kërkojnë të drejta administratori;

бришење на податоците што се наоѓаат на работна станица која треба да се предаде;

fshirja e të dhënave të vendosura në një stacion pune që do të dorëzohet;

ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;

përditësimi i programeve softuerike kur identifikohen dhe korrigjohen mangësitë kritike;

инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно;

instalimi i përditësimeve të sistemit operativ me verifikim automatik sipas vlerësimit të rrezikut, të paktën një herë në javë;

подигнување на нивото на свесност во однос на тоа, на што овластените лица треба да се посветат и податоци за контакт на лицата што треба да ги контактираат во случај на инцидент или појава на необичен настан што влијае на информациите и комуникацијата на системите на Дирекцијата.

ngritjen e nivelit të ndërgjegjësimit në lidhje me atë që duhet t'i kushtojnë vëmendje personat e autorizuar dhe detajet e kontaktit të personave me të cilët duhet të kontaktojnë në rast incidenti ose ndodhjeje të një ngjarjeje të pazakontë që ndikon në informimin dhe komunikimin e sistemeve të Drejtorisë.

Обезбедување на преносливите медиуми

Член 7

Sigurimi i medieve bartëse

Neni 7

Дирекцијата применува соодветни технички мерки, согласно анализата на ризикот од нарушување на безбедноста на личните податоци во случај на кражба или друг начин на загуба на преносливите медиуми (мобилна опрема) на кои се врши обработка на личните податоци, и тоа:

подигање на свеста на овластените лица за специфичните ризици поврзани со користење на преносливите медиуми и преземање мерки за намалување на ризици и

употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на постојните услови и безбедносни гаранции.

Drejtoria zbaton masat e duhura teknike, sipas analizës së rrezikut të cenimit të sigurisë së të dhënave personale në rast vjedhjeje apo mënyrë tjetër të humbjes së medieve bartëse (pajisjeve mobile) në të cilat përpunohen të dhënat personale, edhe atë:

ndërgjegjësimi i personave të autorizuar për rreziqet specifike që lidhen me përdorimin e medieve bartëse dhe marrja e masave për reduktimin e rreziqeve dhe

përdorimi i shërbimeve të reve (cloud services) për krijimin e kopjeve rezervë vetëm pas analizës paraprake të kushteve ekzistuese dhe garancive të sigurisë.

Заштита на внатрешната мрежа

Mbrojtja e rrjetit të brendshëm

Член 8

Дирекцијата обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните можни функции потребни за обработката на личните податоци, а особено преку:

ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси;

во случај на далечински пристап, задолжително воспоставување на VPN конекција со задолжителна автентикација на овластеното лице;

обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително да се изврши преку VPN) и

ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен ѕид (firewall) и прокси сервери.

Neni 8

Drejtoria siguron mbrojtjen e rrjetit të saj të brendshëm duke mundësuar vetëm funksionet e nevojshme të mundshme që kërkohen për përpunimin e të dhënave personale, e në veçanti nëpërmjet:

kufizimit të qasjes në internet duke bllokuar shërbimet jo thelbësore;

në rastin e qasjes në distancë, vendosja e detyrueshme e një lidhjeje VPN me vërtetim të detyrueshëm të personit të autorizuar;

duke siguruar që asnjë nga panelet administrative për menaxhimin e përmbajtjes dhe cilësimet e sistemit nuk janë të qasshme drejtpërdrejt nëpërmjet internetit (mirëmbajtja në distancë duhet të kryhet nëpërmjet VPN) dhe

kufizimi i trafikut të rrjetit duke filtruar trafikun hyrës/dalës në pajisje me mur mbrojtës (firewall) dhe serverë proksi.

Обезбедување на серверите

Член 9

(1) Примената на техничките мерки за серверите на Дирекцијата на кои се централизира обработката на личните податоци задолжително опфаќа:
пристап до алатките и административните панели на серверите само за овластените лица од страна на директорот на Дирекцијата;
примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);
приемена на посебна политика за креирање и употреба на лозинките за администраторите на информацискиот систем;
инсталирање на сите важни ажурирања (updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (auto update) и
правење сигурносни копи (backup) и нивна редовна проверка.
(2) Во случај кога се врши администрирање на базите на податоци, се применуваат следните мерки:
употреба на персонализирани профили за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација и
заштита од напади преку инјектирање на SQL код (компјутерски јазик за комуникација со базата на податоци), скрипти и слично.

Обезбедување на веб-страната на Дирекцијата

Sigurimi i serverëve

Neni 9

(1) Aplikimi i masave teknike për serverët e Drejtorisë në të cilët është i centralizuar përpunimi i të dhënave personale duhet të përfshijë:
qasje në mjetet dhe panelet administrative të serverëve vetëm për personat e autorizuar nga ana e drejtorit të Drejtorisë;
zbatimi i autorizimeve me më pak privilegje për personat që nuk janë administratorë të sistemit të informacionit (operacione të zakonshme për përdoruesit standardë);
zbatim i politikës së veçantë për krijimin dhe përdorimin e fjalëkalimeve për administratorët e sistemit të informacionit;
instalimi i të gjitha përditësimeve të rëndësishme (updates) për sistemet operative dhe për aplikacionet në një interval kohor bazuar në analizën e rrezikut, por jo më shumë se përditësim javor duke e vendosur sistemin në përditësimin automatik (auto update) dhe
duke bërë kopje rezervë dhe duke i kontrolluar ato rregullisht.
(2) Në rast se administrohet baza e të dhënave, zbatohen masat e mëposhtme:
përdorimi i profileve të personalizuara për të hyrë në bazat e të dhënave dhe për të krijuar një emër përdoruesi të veçantë për çdo aplikacion dhe
mbrojtje kundër sulmeve përmes injektimit të kodit SQL (gjuhë kompjuterike për komunikim me bazën e të dhënave), skriptet dhe të ngjashme.

Sigurimi i faqes së internetit të Drejtorisë

Член 10

(1) За веб-страната на Дирекцијата се применуваат технички мерки со кои се гарантира идентитетот на страната и интегритетот и доверливоста на информациите што ги испраќа или ги собира преку веб-страната, и тоа особено преку следните мерки:

имплементација на криптографски протокол за сите страници на веб-страната, вклучително и на формуларите за собирање лични податоци или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавно достапни;

ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации и

пристап до алатките и административните интерфејси можат да имаат само овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни.

(2) Не треба да се применуваат практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна, неовластена обработка на личните податоци, а особено:

да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пр. идентификатори или лозинка);

користење на небезбедни услуги;

употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страни, пристап до електронска пошта и слично;

Neni 10

(1) Për faqen e internetit të Drejtorisë zbatohen masa teknike, të cilat garantojnë identitetin e faqes dhe integritetin dhe konfidencialitetin e informacioneve që i dërgon ose mbledh përmes faqes së internetit, veçanërisht përmes masave të mëposhtme:

zbatimin e protokollit kriptografik për të gjitha faqet e faqes së internetit, duke përfshirë formularët për mbledhjen e të dhënave personale ose për të mundësuar vërtetimin e përdoruesit dhe ato që shfaqin ose transmetojnë të dhëna personale që nuk janë të qasshme publikisht;

kufizimi i porteve të komunikimit në ato që janë rreptësisht të nevojshme për funksionimin e duhur të aplikacioneve të instaluara dhe

qasje në mjetet dhe ndërfaqet administrative mund të kenë vetëm persona të autorizuar me privilegje administratori, të cilët janë pjesë e ekipit përgjegjës për teknologjinë informatike dhe vetëm për aktivitetet administrative që janë të patjetërsueshme.

(2) Nuk duhet të zbatohen praktikat që e rrisin rrezikun e keqpërdorimit të mundshëm, të përpunimit të të dhënave të padëshiruar (të rastësishëm) ose të qëllimshëm, të paautorizuara personale, e në veçanti:

të mos transmetojë të dhëna personale nëpërmjet URL-ve pa aplikuar protokoll enkriptimi (p.sh. identifikues ose fjalëkalim);

përdorimi i shërbimeve të pasigurta;

përdorimi i serverëve që presin bazat e të dhënave ose serverët si stacione pune, veçanërisht jo për kërkimin e faqeve të internetit, qasjen në e-mail dhe të ngjashme;

поставување на базите на податоци на сервери кои се директно достапни преку интернет и
споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

vendosjen e bazave të të dhënave në serverë që janë të aksesueshëm drejtpërdrejt nëpërmjet internetit dhe
ndarjen dhe përdorimin e llogarive të përdoruesve ndërmjet dy ose më shumë personave të autorizuar.

Администратор на информациски систем

Член 11

(1) Администратор на информациски систем е стручно лице од комуникациско-информатичката област, вработено во Дирекцијата, кое се грижи за функционалност на информацискиот систем во смисла на обезбедување на интегритетот и сигурноста на податоците, на апликацијата за пристап до податоците и на техничката опрема која е во функција на информацискиот систем, како и за обезбедување тајност и заштита на обработката на личните податоци.

(2) Информацискиот систем на Дирекцијата е целокупниот систем составен од персонални компјутери, сервери и комуникациска опрема, опрема за обезбедување сигурност на податоците, базата на податоци, апликацискиот сервер и останатите апликации и опрема коишто се користат за обработка на податоци.

(3) Обврските и одговорностите на администраторот на информацискиот систем се пропишани во Правилникот за определување на обврските и на одговорностите на администраторот на информацискиот систем и на овластените лица за обработка на лични податоци.

(4) Офицерот за безбедност на личните податоци задолжително врши периодична контрола над работата на администраторот на информацискиот

Administratori i Sistemit të Informacionit

Neni 11

(1) Administratori i sistemit të informacionit është ekspert i fushës së komunikimit dhe informacionit, i punësuar nga Drejtoria, i cili kujdeset për funksionalitetin e sistemit të informacionit në drejtim të garantimit të integritetit dhe besueshmërisë së të dhënave, aplikacionit për qasje në të dhëna dhe pajisje teknike që janë në funksion të sistemit të informacionit, si dhe për sigurimin e konfidencialitetit dhe mbrojtjen e përpunimit të të dhënave personale.

(2) Sistemi informativ i Drejtorisë është i gjithë sistemi i përbërë nga kompjuterët personalë, serverët dhe pajisjet e komunikimit, pajisjet e sigurisë së të dhënave, baza e të dhënave, serveri i aplikacionit dhe aplikacionet dhe pajisjet tjera që përdoren për përpunimin e të dhënave.

(3) Obligimet dhe përgjegjësitë e administratorit të sistemit informativ janë të përcaktuara me Rregulloren për përcaktimin e obligimeve dhe përgjegjësive të administratorit të sistemit informativ dhe personave të autorizuar për përpunimin e të dhënave personale.

(4) Zyrtari për sigurinë e të dhënave personale duhet të kryejë kontroll periodik mbi punën e administratorit të sistemit informativ dhe të përgatisë

систем и изготвува извештај за извршената контрола. Во него треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

raport për kontrollin e kryer. Ai duhet të përmbajë parregullsitë e konstatuara dhe masat e propozuara për heqjen e këtyre parregullsive.

Обврските и одговорности на овластените лица

Член 12

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем за обработка на личните податоци, Дирекцијата ги пропишува во Правилникот за определување на обврските и на одговорностите на администраторот на информацискиот систем и на овластените лица за обработка на лични податоци.

(2) Дирекцијата задолжително ги информира овластените лица од ставот (1) на овој член за документацијата за технички и организациски мерки коишто се однесуваат на нивните обврски и одговорности.

Detyrimet dhe përgjegjësitë e personave të autorizuar

Neni 12

(1) Drejtoria i përcakton obligimet dhe përgjegjësitë e çdo personi të autorizuar që ka qasje në të dhënat personale dhe në sistemin informativ për përpunimin e të dhënave personale në Rregulloren për përcaktimin e obligimeve dhe përgjegjësive të administratorit të sistemit të informacioneve dhe personave të autorizuar për përpunimin e të dhënave personale.

(2) Drejtoria detyrimisht i njofton personat e autorizuar sipas paragrafit (1) të këtij neni për dokumentacionin për masat teknike dhe organizative që kanë të bëjnë me obligimet dhe përgjegjësitë e tyre.

Идентификација и проверка

Член 13

(1) Дирекцијата задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите и до информацискиот систем, како и воспоставува постапки за идентификација и проверка на авторизираниот пристап.

(2) Евиденцијата од ставот (1) на овој член се ажурира континуирано. Податоците за поранешен вработен на Дирекцијата којшто имал авторизиран пристап до документите и до информацискиот систем се чуваат до 5 години од престанокот на неговиот работен однос во Дирекцијата.

Identifikimi dhe kontrollit

Neni 13

(1) Drejtoria mban evidencë obligative për personat e autorizuar të cilët kanë qasje të autorizuar në dokumente dhe në sistemin informativ, si dhe përcakton procedura për identifikimin dhe verifikimin e qasjes së autorizuar.

(2) Procesverbali sipas paragrafit (1) të këtij neni përditësohet vazhdimisht. Të dhënat për ish-punonjës të Drejtorisë që ka pasur qasje të autorizuar në dokumente dhe në sistemin informativ ruhen deri në 5 vjet nga përfundimi i marrëdhënies së punës së tij në Drejtori.

(3) Кога проверката се врши врз основа на корисничко име и лозинка, Дирекцијата секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.

(4) Лозинките треба автоматски да се менуваат по изминатиот временски период што не може да биде подолг од три месеци.

(5) Со цел да обезбеди идентификување на некој неовластен пристап или злоупотреба на личните податоци, како и да го утврди потеклото на таквите инциденти, Дирекцијата воспоставува и води евиденција за секој пристап до информацискиот систем (logs).

(6) Евиденцијата од ставот (5) на овој член ги содржи особено следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

(7) Евиденцијата од ставот (5) на овој член по правило се чува најмалку пет години.

(8) Офицерот за заштита на личните податоци врши периодична контрола на податоците од ставовите (3) и (4) на овој член, во соработка со администраторот на информацискиот систем и изготвува извештај за извршената проверка и за констатираните неправилности.

(3) Kur kontrolli kryhet në bazë të emrit të përdoruesit dhe fjalëkalimit, Drejtoria gjithmonë zbaton rregullat që garantojnë konfidencialitetin dhe integritetin e tyre gjatë regjistrimit, caktimit dhe ruajtjes së tyre.

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

(5) Për të siguruar identifikimin e çdo qasjeje të paautorizuar ose keqpërdorim të të dhënave personale, si dhe për të përcaktuar origjinën e incidenteve të tilla, Drejtoria themelon dhe mban evidencë për çdo qasje në sistemin informativ (regjistrat).

(6) Procesverbali sipas paragrafit (5) të këtij neni përmban në veçanti këto të dhëna: emrin dhe mbiemrin e personit të autorizuar, vendin e punës nga ku i qaset sistemit informativ, datën dhe kohën e qasjes, të dhënat personale të aksesuara, llojin e akses me operacionet e ndërmarra gjatë përpunimit të të dhënave, një regjistrim autorizimi për çdo akses, një rekord për çdo akses të paautorizuar dhe një rekord për refuzimin e automatizuar nga sistemi i informacionit.

(7) Evidenca, sipas paragrafit (5) të këtij neni, si rregull, mbahet së paku pesë vjet.

(8) Zyrtari për mbrojtjen e të dhënave personale kryen kontroll periodik të të dhënave nga paragrafët (3) dhe (4) të këtij neni, në bashkëpunim me administratorin e sistemit informativ dhe përgatit raport për kontrollin e kryer dhe për parregullsitë e konstatuara. .

Контрола на пристап

Член 14

(1) Овластените лица задолжително имаат авторизиран пристап само до личните податоци и комуникациско-информацискатаопрема кои се неопходни за извршување на нивните работни задачи.

(2) Дирекцијата воспоставува механизми за да се оневозможи пристап на овластени лица до личните податоци и комуникациско-информацискатаопрема со права различни од тие што се авторизирани.

(3) Администраторот на информацискиот систем, согласно неговите овластувања пропишани во Правилникот за определување на обврските и на одговорностите на администраторот на информацискиот систем и на овластените лица за обработка на лични податоци, може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и комуникациско-информацискатаопрема само врз основа на налог даден од страна на директорот на Дирекцијата и во согласност со критериумите што се утврдени од страна на Дирекцијата.

Kontrolli i qasjes

Neni 14

(1) Personat e autorizuar duhet të kenë qasje të autorizuar vetëm në të dhënat personale dhe pajisjet komunikuese-informative që janë të nevojshme për kryerjen e detyrave të tyre të punës.

(2) Drejtoria themelon mekanizma për të penguar qasjen e personave të autorizuar në të dhënat personale dhe pajisjet komunikuese-informative me të drejta të ndryshme nga ato të autorizuara.

(3) Administratori i sistemit informativ, në pajtim me kompetencat e tij të përcaktuara me Rregulloren për përcaktimin e obligimeve dhe përgjegjësive të administratorit të sistemit informativ dhe personave të autorizuar për përpunimin e të dhënave personale, mund të lejojë, ndryshojë ose revokojë qasjen e autorizuar. ndaj të dhënave personale dhe pajisjeve komunikuese-informative vetëm në bazë të urdhrit të dhënë nga drejtori i Drejtorisë dhe në përputhje me kriteret e përcaktuara nga Drejtoria.

Превенирање, реакција и санирање на инциденти (обезбедување континуитет)

Член 15

(1) Начинот на превенирање и управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци, директорот на Дирекцијата ги пропишува во Правилникот за начинот на превенирање и управување со

Parandalimi, reagimi dhe korrigjimi i incidenteve (duke siguruar vazhdimësi)

Neni 15

(1) Mënyrën e parandalimit dhe menaxhimit të incidenteve që cenojnë konfidencialitetin, integritetin ose qasshmërinë e të dhënave personale e përcakton drejtori i Drejtorisë me Rregulloren për mënyrën e parandalimit dhe menaxhimit të incidenteve që cenojnë

инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци.

(2) Управувањето со инциденти опфаќа мерки и постапки за пријавување, реакција, санирање и евиденција на инцидентите, вклучувајќи и повторно внесување, односно враќање на личните податоци во системот во случај на нивно оштетување или уништување.

konfidencialitetin, integritetin ose qasshmërinë e të dhënave personale.

(2) Menaxhimi i incidentit përfshin masat dhe procedurat për raportimin, reagimin, korrigjimin dhe regjistrimin e incidenteve, duke përfshirë rifutjen, pra kthimin e të dhënave personale në sistem në rast të dëmtimit ose shkatërrimit të tyre.

Правење на сигурносна копија, архивирање, чување и начин за повторно враќање на зачуваните сигурносни копии

Член 16

(1) Дирекцијата, врз основа на анализа на ризиците, прави сигурносни копии на личните податоци на редовни временски интервали со цел да се намали ефектот во случај на нивно непосакувано губење или оштетување.

(2) Начинот на правење на сигурносна копија, архивирање и чување, како и начинот за повторно враќање на зачуваните лични податоци што се предмет на автоматизирана (софтверска) обработка во Дирекцијата, директорот на Дирекцијата ги пропишува во Правилникот за начинот на правење на сигурносна копија, архивирање и чување, како и за начинот на повторно враќање на зачуваните лични податоци.

Bërja e kopjes së sigurisë, arkivimi, ruajtja dhe mënyra e kthimit të kopjeve të ruajtura të sigurisë

Neni 16

(1) Drejtoria, në bazë të analizës së rrezikut, bën kopje të sigurisë të të dhënave personale në intervale të rregullta kohore për të zvogëluar efektin në rast të humbjes ose dëmtimit të padëshiruar të tyre.

(2) Mënyra e bërjes së kopjes së sigurt, arkivimit dhe ruajtjes, si dhe mënyra e marrjes së të dhënave të ruajtura personale që i nënshtrohen përpunimit të automatizuar (softverik) në Drejtori, e përcakton drejtori i Drejtorisë me Rregulloren për metodën e bërjes së kopjes së sigurisë, arkivimit dhe ruajtjes, si dhe metodën e marrjes së të dhënave personale të ruajtura.

Управување со медиуми

Член 17

(1) Дирекцијата ги евидентира преносливите медиуми со кои се ракува во Дирекцијата за складирање лични податоци.

(2) Пристап до медиумите од ставот (1) на овој член треба да се имаат само овластени лица.

Menaxhimi i medieve

Neni 17

(1) Drejtoria i evidenton mediet bartëse të cilat përdoren në Drejtori me qëllim deponimin e të dhënave personale.

(2) Qasje në medie sipas paragrafit (1) të këtij neni duhet të kenë vetëm personat e autorizuar.

(3) Пренесувањето на медумите надвор од работните простории се врши само со претходно писмено овластување од страна на директорот н Дирекцијата.

(4) За пренесените медуми надвор од работните простории на Дирекцијата се преземаат мерки за да се спречи неовластено обработување на личните податоси што се снимени на нив.

(5) Управувањето со медиумите, односно начинот на бришење, чистење и уништување на медиуми што се користат за обработка на лични податоци во Дирекцијата, директорот на Дирекцијата го пропишува во Правилникот за начинот на уништување на документите со лични податоци по истекот на рокот за нивно чување и за начинот на бришење, чистење и уништување на медиуми што се користат за обработка на личните податоци.

(3) Bartja e mjediumeve jashtë hapësirave të punës bëhet vetëm me autorizim paraprak me shkrim nga drejtori i Drejtorisë.

(4) Për mediet e bartura jashtë hapësirave të punës së Drejtorisë ndërmerren masa për të parandaluar përpunimin e paautorizuar të të dhënave personale të regjistruara në to.

(5) Menaxhimi i medieve, gjegjësisht mënyra e fshirjes, pastrimit dhe asgjësimit të medieve që përdoren për përpunimin e të dhënave personale në Drejtori, e përcakton drejtori i Drejtorisë me Rregulloren për mënyrën e asgjësimit të dokumenteve me të dhëna personale pas skadimit të afatit për ruajtjen e tyre dhe mënyrën e fshirjes, pastrimit dhe shkatërrimit të medieve të përdorura për përpunimin e të dhënave personale.

Физичка безбедност на информацискиот систем

Член 18

(1) Серверите на кои се инсталиранин софтверски програми за обработка на личните податоци се физички лоцирани, хостирани и администрирани од страна на Дирекцијата.

(2) Дирекцијата обезбедува зајакнато ниво на безбедност во однос на просториите во коишто се сместени и се чуваат серверите и мрежната опрема преку коишто се врши обработката на личните податоци, и тоа:

пристап до просторијата во којашто се сместени серверите имаат само лица со посебно овластување за тоа од страна на директорот на Дирекцијата;

Siguria fizike e sistemit të informacionit

Neni 18

(1) Serverët në të cilët janë instaluar programet softuerike për përpunimin e të dhënave personale janë fizikisht të detektuara, të vendosura dhe të administruar nga Drejtoria.

(2) Drejtoria siguron nivel të përforcuar të sigurisë në lidhje me ambientet në të cilat ndodhen dhe mbahen serverët dhe pajisjet e rrjetit përmes të cilave përpunohen të dhënat personale, përkatësisht:

qasja në dhomën ku ndodhen serverët është e disponueshme vetëm për personat me autorizim të veçantë për këtë nga drejtori i Drejtorisë;

во просторијата во којашто се сместени серверите се применуваат мерки и контроли за заштита од кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење;
доколку е потребен пристап на друго лице до просторијата и личните податоци што се зачувани на серверите, тогаш тоа лице ќе биде придружувано и ќе биде под надзор на лицето овластено од директорот на Дирекцијата;
водење ажуриран список на лица или категории на лица кои се овластени да влегуваат во просториите каде е сместена и се чува комуникациско-информациска опрема на која се врши обработка на лични податоци;
водење евиденција на пристап до просториите во коишто се сместени и се чуваат серверите кои содржат лични податоци;
одржување на просториите во коишто се сместени и се чуваат серверите (климатизација, UPS уред и слично).

(3) По исклучок од ставот (1) на овој член, серверите на кои се инсталиранин софтверски програми за обработка на личните податоци се физички лоцирани, хостирани и администрирани надвор од просториите на Дирекцијата.

(4) Во случајот од ставот (3) на овој член, меѓусебните права и обврски на Дирекцијата и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, се уредуваат со договор во писмена форма кој задолжително содржи мерки за безбедност на личните податоци согласно со прописите за заштита на личните податоци.

në hapësirën ku ndodhen serverët zbatohen masa dhe kontrolle për mbrojtjen nga vjedhja, zjarri, shpërthimet, tymi, uji, pluhuri, vibrimet, ndikimet kimike, ndërhyrjet në furnizimin me energji elektrike dhe rrezatimi elektromagnetik;
nëse një person tjetër ka nevojë për qasje në dhomë dhe në të dhënat personale të ruajtura në serverë, atëherë ai person do të shoqërohet dhe do të jetë nën mbikëqyrjen e personit të autorizuar nga drejtori i Drejtorisë;
mbajtjen e një liste të përditësuar të personave ose kategorive të personave që janë të autorizuar të hyjnë në ambientet ku ndodhen dhe mbahen pajisjet e komunikimit dhe informacionit në të cilat përpunohen të dhënat personale;
mbajtjen e shënimeve për aksesin në ambientet ku ndodhen dhe mbahen serverët që përmbajnë të dhëna personale;

mirëmbajtjen e ambienteve ku ndodhen dhe mbahen serverët (klimatizim, pajisje UPS, etj.).

(3) Me përjashtim të paragrafit (1) të këtij neni, serverët në të cilët janë instaluar programet softuerike për përpunimin e të dhënave personale, fizikisht gjenden, strehohen dhe administrohen jashtë hapësirave të Drejtorisë.

(4) Në rastin sipas paragrafit (3) të këtij neni, të drejtat dhe detyrimet e ndërsjella të Drejtorisë dhe personit juridik, përkatësisht personit fizik në të cilin serverët janë fizikisht të vendosur, hostuar dhe administruar, rregullohen me marrëveshje. në formë të shkruar që duhet të përmbajë masa sigurie të të dhënave personale në përputhje me rregulloret për mbrojtjen e të dhënave personale.

Контрола на информацискиот систем и на комуникациско-информацискатa опрема

Член 19

(1) Офицерот за заштита на личните податоци врши периодични контроли заради следење на усогласеноста на работењето на Дирекцијата со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

(2) Информацискиот систем и комуникациско-информацискатa опрема на Дирекцијата подлежат на годишна внатрешна контрола со цел да се провери дали постапките и упатствата, односно техничките и организациските мерки содржани во политиките и правилниците за безбедност на личните податоци, се применуваат и се во согласност со прописите за заштита на личните податоци.

Kontrolli i sistemit të informacionit dhe pajisjeve komunikuese-informative

Neni 19

(1) Zyrtari për mbrojtjen e të dhënave personale kryen kontrolle periodike me qëllim të monitorimit të harmonizimit së punës së Drejtorisë me rregulloret për mbrojtjen e të dhënave personale dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

(2) Sistemi informativ dhe pajisjet komunikuese-informative të Drejtorisë i nënshtrohen një kontrolli të brendshëm vjetor për të kontrolluar nëse procedurat dhe udhëzimet, përkatësisht masat teknike dhe organizative që përmbajnë politikat dhe rregulloret për sigurinë e të dhënave personale, zbatohen dhe janë në përputhje me rregulloret për mbrojtjen e të dhënave personale.

Управување со обработувачи

Член 20

(1) Дирекцијата обезбедува заштита на личните податоци во електронска форма при нивната размена со надворешни субјекти, преку примена на мерки за идентификација при размена.

(2) Меѓусебните права и обврски на Дирекцијата и обработувачот се уредуваат со договор. Пред склучување на договорот, Дирекцијата е должна да побара од обработувачот (давател на услугата) да му ја презентира својата безбедносна политика во однос на информацискиот систем и комуникациско-информацискатa опрема на која ќе се врши обработката на личните податоци во име на Дирекцијата.

Menaxhimi i përpunuesve

Neni 20

(1) Drejtoria siguron mbrojtjen e të dhënave personale në formë elektronike gjatë shkëmbimit të tyre me subjekte të jashtme, përmes aplikimit të masave për identifikim gjatë shkëmbimit.

(2) Të drejtat dhe detyrimet e ndërsjella të Drejtorisë dhe përpunuesit rregullohen me marrëveshje. Përpara lidhjes së kontratës, Drejtoria është e detyruar të kërkojë nga përpunuesi (ofruesi i shërbimit) të paraqesë politikën e tij të sigurisë në lidhje me sistemin e informacionit dhe pajisjet e komunikimit-informacionit mbi të cilat do të kryhet përpunimi i të dhënave personale në emër të Drejtorisë.

(3) Безбедносната политика од ставот (2) на овој член треба да содржи податоци со кои ќе се гарантира безбедноста на личните податоци, и тоа:

дали и како се врши криптирање на податоците според нивната чувствителност;

дали и како се врши криптирање на преносот на податоци;

постоење на процедури што гарантираат дека никој нема да има неовластен пристап до податоците;

гаранции во однос на следење на пристапот до информацискиот систем (логови);

управување со правата на пристап;

автентикација и

други мерки за безбедност на обработката на личните податоци.

(4) Договорот од ставот (2) на овој член треба да содржи одредби особено за:

предметот, должината и целта на обработката на личните податоци;

обврските за обработувачот во однос на преземање на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци;

обврските во однос на тајноста на доверените лични податоци;

минималните стандарди за автентикација на овластените лица;

условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;

правилата за известување на Дирекцијата и управување со инциденти во случај на нарушување на безбедноста на личните податоци;

обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на Дирекцијата и

(3) Politika e sigurisë sipas paragrafit (2) të këtij neni duhet të përmbajë të dhëna që garantojnë sigurinë e të dhënave personale, përkatësisht:

nëse dhe si kodohen të dhënat sipas ndjeshmërisë së tyre;

nëse dhe si është i koduar transmetimi i të dhënave;

ekzistenca e procedurave që garantojnë se askush nuk do të ketë akses të paautorizuar në të dhëna;

garanci në lidhje me aksesin monitorues në sistemin e informacionit (logo);

menaxhimi i të drejtave të qasjes;

vërtetimi dhe

masa të tjera për sigurinë e përpunimit të të dhënave personale.

(4) Kontrata sipas paragrafit (2) të këtij neni duhet të përmbajë dispozita veçanërisht për:

subjektin, kohëzgjatjen dhe qëllimin e përpunimit të të dhënave personale;

detyrimet për përpunuesin në lidhje me marrjen e masave teknike dhe organizative për të garantuar sigurinë e përpunimit të të dhënave personale;

detyrimet në lidhje me konfidencialitetin e të dhënave personale të besuara;

standardet minimale për vërtetimin e personave të autorizuar;

kushtet për kthimin e të dhënave dhe/ose shkatërrimin e tyre pas skadimit ose zgjidhjes së kontratës;

rregullat për raportimin në Drejtori dhe menaxhimin e incidentit në rast të shkeljes së sigurisë së të dhënave personale;

detyrimet që përpunuesi të veprojë vetëm në përputhje me udhëzimet e marra nga Drejtoria dhe

другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

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

2. Организациски мерки

2. Masat organizative

Член 21

(1) Дирекцијата применува соодветни организациски мерки кои обзбедуваат тајност и заштита на обработката на личните податоци, и тоа:

ограничен пристап или идентификација за пристап до личните податоци;

уништување на документи по истекот на рокот за нивно чување;

мерки за физичка сигурност на работните простории и на комуниникациско-информациската опрема на која се обработуваат личните податоци;

почитување на техничките упатства при инсталирање и користење комуниникациско-информациска опрема на која се обработуваат личните податоци.

(2) Вработеното лице во организационата единица за човечки ресурси во Дирекцијата, преку раководното лице во институцијата го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му биде избришано корисничкото име и лозинката, односно заклучена за понатамошен пристап. Известувањето се врши писмено.

Neni 21

(1) Drejtoria zbaton masat e duhura organizative që sigurojnë fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale, përkatësisht:

akses ose identifikim i kufizuar për të hyrë në të dhënat personale;

shkatërrimi i dokumenteve pas skadimit të afatit të ruajtjes së tyre;

masat për sigurimin fizik të ambienteve të punës dhe pajisjeve komunikuese-informative në të cilat përpunohen të dhënat personale;

pajtueshmërinë me udhëzimet teknike gjatë instalimit dhe përdorimit të pajisjeve komunikuese-informative mbi të cilat përpunohen të dhënat personale.

(2) Punonjësi në njësinë organizative për burime njerëzore në Drejtori, nëpërmjet personit drejtues në institucion, e njofton administratorin e sistemit informativ për punësimin ose angazhimin e çdo personi të autorizuar me të drejtë aksesi në sistemin informativ me qëllim t'i caktohet një emër përdoruesi dhe fjalëkalimi, si dhe për përfundimin e punësimit ose punësimin në mënyrë që emri i përdoruesit dhe fjalëkalimi i tij të fshihen, përkatësisht të kyçen për qasje të mëtejshme. Njoftimi bëhet me shkrim.

(3) Известувањето од ставот (2) на овој член се врши и при кои било други промени во работниот статус или статусот на ангажирањето на овластеното лице што има влијание врз нивото на дозволениот пристап до информацискиот систем.

(3) Njoftimi sipas paragrafit (2) të këtij neni bëhet edhe në rast të ndonjë ndryshimi tjetër në gjendjen e punës ose statusin e punësimit të personit të autorizuar që ka ndikim në nivelin e qasjes së lejuar në sistemin informativ.

Информирање и едуцирање за заштитата на личните податоци

Informimi dhe edukimi për mbrojtjen e të dhënave personale

Член 22

Neni 22

(1) Лицето коешто се вработува или се ангажира во Дирекцијата, пред започнување со работа се запознава со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(1) Personi i cili është i punësuar ose i angazhuar në Drejtori, para fillimit të punës, njihet me rregulloret për mbrojtjen e të dhënave personale, si dhe me dokumentacionin e miratuar për masat teknike dhe organizative.

(2) За лицето кое се ангажира за извршување работа во Дирекцијата во договорот за неговото ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(2) Për personin që punësohet për kryerjen e punëve në Drejtori, detyrimet dhe përgjegjësitë për mbrojtjen e të dhënave personale janë të përcaktuara në kontratën për punësimin e tij.

(3) Пред непосредното започнување со работа на овластеното лице, раководно лице од организационата единица за човечки ресурси дополнително го информира за непосредните обврски и одговорности за заштита на личните податоци.

(3) Para se personi i autorizuar të fillojë menjëherë me punë, menaxheri i njësisë organizative për burime njerëzore e informon atë për obligimet dhe përgjegjësitë imediate për mbrojtjen e të dhënave personale.

(4) Лицето кое се вработува или се ангажира во Дирекцијата, пред започнување со работа своерачно потпишува Изјава за тајност и заштита на обработката на личните податоци.

(4) Personi i cili është i punësuar ose i angazhuar në Drejtori, para fillimit të punës, personalisht nënshkruan Deklaratë për konfidencialitetin dhe mbrojtjen e përpunimit të të dhënave personale.

(5) Изјавата од ставот (4) на овој член особено го содржи следното:
дека лицето ќе ги почитува начелата за заштита на личните податоци пред нивниот пристап до личните податоци;
ќе врши обработка на личните податоци согласно упатствата добиени

(5) Deklarata sipas paragrafit (4) të këtij neni veçanërisht përmban:
se personi do të respektojë parimet e mbrojtjes së të dhënave personale përpara aksesit të tij në të dhënat personale;
do të përpunojë të dhënat personale në përputhje me udhëzimet e marra nga

од Дирекцијата, освен ако со закон поинаку не е уредено;
личните податоци ќе ги чуваат како доверливи и
ќе ги применуваат пропишаните мерки за заштита на личните податоци.
(6) Изјавата од ставот (4) на овој член задолжително се чува во досието на лицето коешто се вработува или се ангажира во Дирекцијата.
(7) Дирекцијата врши континуирано информирање и едуцирање на раководството и на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Drejtoria, përveç nëse rregullohet ndryshe me ligj;
do të mbajë konfidenciale të dhënat personale dhe
do të zbatojë masat e parapara për mbrojtjen e të dhënave personale.
(6) Deklarata sipas paragrafit (4) të këtij neni duhet të ruhet në dosjen e personit i cili është i punësuar ose i angazhuar në Drejtori.
(7) Drejtoria vazhdimisht informon dhe edukon menaxhmentin dhe personat e autorizuar për obligimet dhe përgjegjësitë imediate për mbrojtjen e të dhënave personale.

Пристап до документите

Член 23

(1) Пристапот до документите треба да биде ограничен само за овластени лица во Дирекцијата.
(2) За пристапување до документите се врши идентификација на овластените лица и за категориите на личните податоци до кои се пристапува се води евиденција на пристапи.
(3) Пристапувањето на неовластените лица до документи треба да биде во придружба на лице кое е овластено за пристапување до документите.

Qasja te dokumentet

Neni 23

(1) Qasja te dokumentet duhet të kufizohet vetëm për personat e autorizuar në Drejtori.
(2) Për qasje në dokumente, bëhet identifikimi i personave të autorizuar dhe për kategoritë e të dhënave personale në të cilat aksesohen, mbahet evidencë e qasjeve.

(3) Qasja e personave të paautorizuar në dokumente duhet të shoqërohet nga personi i cili është i autorizuar për qasje në dokumente.

Правило „чисто биро“
Член 24

Дирекцијата задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Rregulli i "tavolinës së pastër"

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

Чување на документи

Ruajtja e dokumenteve

Член 25

(1) Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секој неовластен пристап.

(2) Ормарите, картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од страна на овластените лица.

Neni 25

(1) Ruajtja e dokumenteve duhet të bëhet në atë mënyrë që të zbatohen mekanizmat e duhur për të parandaluar çdo qasje të paautorizuar.

(2) Dollapët, kabinetet ose pajisjet e tjera për ruajtjen e dokumenteve duhet të vendosen në dhoma të mbyllura me mekanizma të përshtatshëm mbrojtës. Lokalet duhet të jenë të kyçura edhe për periudhën kur dokumentet nuk përpunohen nga personat e autorizuar.

Уништување на документи

Член 26

(1) Уништувањето на документите се врши на начин што оневозможува нивно обновување и повторна употреба.

(2) Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

Asgjësimi i dokumenteve

Neni 26

(1) Asgjësimi i dokumenteve bëhet në atë mënyrë që e bën të pamundur rikthimin dhe ripërdorimin e tyre.

(2) Në rastin sipas paragrafit (1) të këtij neni, komisioni përgatit raport, i cili përmban të gjitha të dhënat për identifikimin e plotë të dokumentit si dhe kategoritë e të dhënave personale që gjenden në të.

ВИСОКО НИВО

1. Технички мерки

NIVELI I LARTË

1. Masat teknike

Управување со лозинки

Член 27

За секоја услуга или софтверска програма, Дирекцијата користи различни лозинки составени од комбинација од осум алфанумерички карактери – букви (мали и големи) и специјални знаци, и обезбедува нивно соодветно чување и заштита од неовластено откривање, при што пропишува Политика за креирање и

Menaxhimi i fjalëkalimeve

Neni 27

Për çdo shërbim ose program softuerik, Drejtoria përdor fjalëkalime të ndryshme të përbërë nga një kombinim i tetë karaktereve alfanumerike - shkronja (të vogla dhe të mëdha) dhe karaktere speciale, dhe siguron ruajtjen dhe mbrojtjen e duhur të tyre nga zbulimi i paautorizuar, ndërkohë që përshkruan Politikë për krijimin dhe përdorimin e fjalëkalimeve për administratorët.

употреба на лозинки за администратори.

Управување со преносливи медиуми

Член 28

(1) Дирекцијата воспоставува систем за евидентирање на медиумите кои се примаат со цел да се овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум на примање, испраќач, број на медиуми што се примени, вид на документ што е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.

(2) За пренесените медиуми надвор од работните простории на Дирекцијата, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Menaxhimi i medieve bartëse

Neni 28

(1) Drejtoria themelon sistem për regjistrimin e medieve të pranuara për të mundësuar identifikimin e drejtpërdrejtë ose të tërthortë të llojit të medies së pranuar, datës së pranimit, dërguesit, numrit të mediave të pranuara, llojit të dokumentit të regjistruar në medie, mënyrës së dërgimi i medies, emrit dhe mbiemrit të personit të autorizuar për marrjen e medies.

(2) Për mediet që transmetohen jashtë hapësirave të punës së Drejtorisë, duhet të ndërmerren masat e nevojshme për të parandaluar përpunimin e paautorizuar të të dhënave personale të regjistruara në to.

Тестирање на информацискиот систем

Член 29

(1) Дирекцијата задолжително врши тестирање на информацискиот систем пред негово имплементирање или по извршените промени со цел да се провери дали системот обезбедува безбедност на личните податоци согласно со прописите за заштита на личните податоци.

(2) Тестирањето од ставот (1) на овој член се врши преку обработка на документи што содржат имагинарни лични податоци.

Testimi i sistemit të informacionit

Neni 29

(1) Drejtoria duhet të bëjë testimin e sistemit informativ para zbatimit të tij ose pas ndryshimeve për të kontrolluar nëse sistemi siguron sigurinë e të dhënave personale në përputhje me rregulloret për mbrojtjen e të dhënave personale.

(2) Testimi sipas paragrafit (1) të këtij neni bëhet përmes përpunimit të dokumenteve që përmbajnë të dhëna personale imagjinare.

Пренесување на медиуми

Член 30

Медиумите можат да се пренесуваат надвор од работните

Bartja e medieve

Neni 30

Media mund të bartet jashtë ambienteve të punës së Drejtorisë vetëm

простории на Дирекцијата само ако личните податоци се криптирани или ако се заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем, или лице овластено од него, може да ги декриптира.

nëse të dhënat personale janë të koduara ose nëse mbrohet me metoda të përshtatshme që garantojnë se të dhënat nuk mund të lexohen, ku vetëm administratori i sistemit të informacionit ose personi i autorizuar nga ai mund t'i deshifrojë ato.

Пренесување на личните податоци преку мрежа за електронски комуникации

Член 31

Личните податоци можат да се пренесуваат преку мрежа за електронски комуникации само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.

Bartja e të dhënave personale nëpërmjet rrjetit të komunikimeve elektronike

Neni 31

Të dhënat personale mund të barten përmes rrjetit të komunikimit elektronik vetëm nëse janë të koduara ose nëse janë të mbrojtura në mënyrë specifike me metoda të përshtatshme që sigurojnë që të dhënat të mos lexohen gjatë bartjes.

2. Организациски мерки

2. Masat organizative

Копирање и умножување на документите

Член 32

(1) Копирањето и умножувањето на документите може да се врши единствено со контрола на овластените лица определени со претходно писмено овластување од страна на директорот на Дирекцијата и согласно процедурата во која задолжително се утврдуваат мерките и начинот на копирање и умножување на документите.

(2) Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе се оневозможи понатамошно обновување на содржаните лични податоци.

Kopjimi dhe dublikimi i dokumenteve

Neni 32

(1) Kopjimi dhe dublimi i dokumenteve mund të bëhet vetëm nën kontrollin e personave të autorizuar të përcaktuar me autorizim paraprak me shkrim nga drejtori i Drejtorisë dhe në pajtim me procedurën në të cilën përcaktohen masat dhe mënyra e kopjimit dhe dublimit të dokumenteve.

(2) Shkatërrimi i kopjeve ose dokumenteve të dubluara duhet të bëhet në atë mënyrë që do të parandalojë rikuperimin e mëtejshëm të të dhënave personale të përmbajtura.

Пренесување на документите

Член 33

Bartja e dokumenteve

Neni 33

Во случај на физички пренос на документите, Дирекцијата задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите што се пренесуваат.

Në rast të bartjes fizike të dokumenteve, Drejtoria ndërmerr detyrimisht masa për t'i mbrojtur ato nga qasja ose trajtimi i paautorizuar i të dhënave personale që gjenden në dokumentet që transferohen.

Влегување во сила

Hyrja në fuqi

Член 34

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

Neni 34

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

Директор/Drejtori

Стојан Славески