



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 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), nenin 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), dhe në lidhje me nenin 119 dhe 120 të Ligjit të Mbrojtjes së të Dhënave Personale (*) (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 42/20) dhe nenin 47 të Rregullores së sigurisë së përpunimit të të dhënave personale (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 122/20), drejtori i Drejtorisë së Sigurimit të Informacioneve të Klasifikuara miraton

**ПОЛИТИКА ЗА ВОСПОСТАВУВАЊЕ
СИСТЕМ ЗА
ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ**

**POLITIKËN E KRIJIMIT TË SISTEMIT
PËR MBROJTJEN E TË DHËNAVE
PERSONALE**

Цел и опсег

Qëllimi dhe fushëveprimi

Член 1

Neni 1

Со политиката за воспоставување систем за заштита на личните податоци

Me politikën e krijimit të sistemit për mbrojtjen e të dhënave personale

се востановуваат основите на системот за заштита на личните податоци и мерките што ќе се преземат при обработка на личните податоци, сè со цел заштита и безбедност на личните податоци кои се обработуваат како и оценка на нивната адекватност со видот и обемот на работните процеси што ги врши Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата).

vendosen bazat e sistemit të mbrojtjes së të dhënave personale dhe masat që do të ndërmerren gjatë përpunimit të të dhënave personale, të gjitha me qëllim mbrojtjen dhe sigurimin e të dhënave personale që përpunohen, si dhe vlerësimin e përshtatshmërisë së tyre me llojin dhe shtrirjen e proceseve të punës që kryen Drejtoria e Sigurisë së Informacioneve të Klasifikuara (në tekstin e mëtejme: drejtoria).

Принципи при обработка на личните податоци

Parimet gjatë përpunimit të të dhënave personale

Член 2

Neni 2

Принципи (начела) врз кои се заснова обработката на личните податоци во Дирекцијата се:

Parimet (principet) sipas të cilave bazohet përpunimi i të dhënave personale në drejtori janë:

- законитост,
- транспарентност,
- ограничување на целта,
- принцип на обработка на минимален обем на податоци,
- принцип на точност,
- принцип на ограничување на рокот на чување,
- принцип на интегритет и доверливост,
- принцип на законитост на обработката на личните податоци и
- согласност.

- ligjshmëria,
- transparenca,
- kufizimi i qëllimit,
- parimet e përpunimit të vëllimit minimal të të dhënave,
- parimet e saktësisë,
- parimet e kufizimit të afatit të ruajtjes,
- parimet e integritetit dhe besueshmërisë,
- parimet e ligjshmërisë së përpunimit të të dhënave personale dhe
- Pajtuueshmëria.

Технички и организациски мерки заради безбедност на личните податоци и спречување пристап до истите од страна на трети лица

Masat teknike dhe organizative për sigurimin e të dhënave personale nga ana e personave të tretë

Член 3

Neni 3

(1) Безбедноста на личните податоци е предуслов за постигнување усогласеност со сите други принципи на обработка на личните податоци.

(2) Дирекцијата и обработувачот, користејќи пристап базиран на анализа на ризици, презема соодветни технички и организациски мерки за да обезбеди ниво на безбедност на податоците коешто ќе биде соодветно на нивото на ризикот. Ризиците може да бидат случајни и предизвикани од невнимание, но и умислени, намерни активности, па така и мерките што ги презема контролорот се движат од заштита против комплексни технолошки закани, како што се злонамерни софтвери и DOS-напади, па сè до мерки против невнимание на вработени лица.

(3) Освен ризиците, при избор на соодветни технички и организациски мерки контролорот ги зема предвид и најновите технолошки достигнувања, трошоците за спроведување, природата, обемот и контекстот и целите на обработката.

(4) Согласно Правилникот за безбедност на обработката на личните податоци, на сите документи во Дирекцијата задолжително се применуваат технички и организациски мерки за обезбедување тајност, приватност и заштита на личните податоци, класифицирани во следните нивоа:

- стандардно, и
- високо ниво.

(5) Дирекцијата во својство на контролор е одговорна за примена на потребното ниво на мерки за безбедност на обработка на личните податоци со цел да обезбеди соодветно ниво на безбедност на личните податоци,

(1) Siguria e të dhënave personale është parakusht për arritjen e pajtueshmërisë me të gjitha parimet e tjera në përpunimin e të dhënave personale.

(2) Drejtoria dhe përpunuesi, duke shfrytëzuar qasje të bazuar në analizën e rreziqeve, ndërmarrin masat e duhura teknike dhe organizative për të siguruar nivelin e sigurisë së të dhënave të përshtatshme me nivelin e rrezikut. Rreziqet mund të jenë aksidentale dhe të shkaktuara nga pakujdesia, por edhe të menduara, aktivitete të qëllimshme, kështu që masat e ndërmarra nga kontrolluesi lëvizin nga mbrojtja kundër kërcënimeve komplekse teknologjike, si softuerët me qëllime të këqija dhe sulmet DOS, deri te masat kundër pakujdesisë së personave të punësuar.

(3) Përveç rreziqeve gjatë zgjedhjes së masave të duhura teknike dhe organizative, kontrolluesi i merr parasysh arritjet teknologjike më të reja, shpenzimet për realizimin, natyrën, vëllimin dhe kontekstin dhe qëllimet e përpunimit.

(4) Në pajtim me Rregulloren e sigurisë së përpunimit të të dhënave personale, të gjitha dokumentet në drejtori domosdoshmërisht zbatohen masat teknike dhe organizative për sigurimin e fshehtësisë, privatësisë dhe mbrojtjen e të dhënave personale, të klasifikuara në këto nivele:

- standarde, dhe
- niveli i lartë.

(5) Drejtoria në cilësinë e kontrolluesit është përgjegjës për zbatimin e nivelit të nevojshëm të masave për siguri të përpunimit të të dhënave personale me qëllim që të sigurojë nivelin përkatës të sigurisë së

вклучувајќи заштита од неовластена или незаконска обработка, како и заштита од нивно случајно губење, уништување или оштетување.

(6) За документите што содржат матичен број на граѓанинот задолжително се применуваат техничките и организациските мерки кои се класифицираат на стандардно ниво, а кои опфаќаат автентикација на овластени лица, обезбедување опрема на која се врши обработка на личните податоци, сегрегација на должности и одговорности, контрола на пристап до информацискиот систем, обезбедување евиденција за секој пристап (logs), заштита на внатрешната мрежа, обезбедување на веб-страницата, обезбедување континуитет во работењето, начин на архивирање и чување на податоците, физичка безбедност, управување со обработувачи, информирање и едуцирање за заштитата на личните податоци, пристап до документите, правило „чисто биро“, чување документи, начин на чување на документите и слично.

(7) За документите кои се пренесуваат преку комуникациско-информциски системи, а содржат матичен број на граѓанинот задолжително се применуваат техничките и организациските мерки кои се класифицираат на стандардно и високо ниво, а кои опфаќаат управување со лозинки, сертификација за заштита на личните податоци, управување со преносливи медиуми, пренесување на медиуми, копирање и умножување документи, пренесување документи и слично.

(8) Во Дирекцијата, личните податоци кои се чуваат во хартиена

тë dhënave personale, duke përfshirë mbrojtjen nga përpunimi i paautorizuar ose i paligjshëm, si dhe mbrojtjen kundër humbjes, shkatërrimit apo dëmtimit aksidental të tyre.

(6) Për dokumentet të cilat e përmbajnë numrin amzë të qytetarit, domosdoshmërisht zbatohen masat teknike dhe organizative që klasifikohen sipas nivelit standard dhe të cilat përfshijnë autenticitetin e personave të autorizuar, sigurimin e pajisjeve me të cilat përpunohen të dhënat personale, ndarjen e detyrave dhe përgjegjësi, kontrollin e qasjes në sistemin e informacionit, sigurimin e evidencës për çdo qasje (logs), mbrojtjen e rrjetit të brendshëm, sigurimin e ueb-faqes, sigurimin e vazhdimësisë në punë, mënyrën e arkivimit dhe ruajtjes së të dhënave, sigurimin fizik, menaxhimin e përpunuesve, informacionin dhe edukimin për mbrojtjen e të dhënave personale, qasje deri te dokumentet, rregulli “tavolinë e pastër”, ruajtja e dokumenteve, mënyra e ruajtjes së dokumenteve etj.

(7) Për dokumentet të cilat barten nëpërmjet sistemit të komunikimit dhe atij informativ dhe përmbajnë numrin amzë të qytetarit, domosdoshmërisht zbatohen masat teknike dhe organizative që klasifikohen në nivelin standard dhe të lartë, të cilat përfshijnë menaxhimin e fjalëkalimeve, certifikimin e mbrojtjes së të dhënave personale, menaxhimin me media lëvizëse, transferimin e mediave, kopjimin dhe shumëfishimin e dokumenteve, bartjen e dokumenteve etj.

(8) Në drejtori, të dhënat personale të cilat ruhen në formë të letrës, ruhen

форма, се чуваат во ормари за чување документи со клуч до кои пристап има овластеното лице за обработка на податоците, кое има пристап и до одредени работни простории на Дирекцијата. Чувањето на документите се врши на начин што ќе овозможи попречување на секое неовластено отворање.

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

(10) Во Дирекцијата, личните податоци кои се обработуваат и чуваат во комуникациско-информациски систем, односно во електронска форма, се заштитуваат со тоа што најавата во комуникациско-информацискиот систем се врши преку единствен идентификатор кој се поврзува само со едно лице, односно со овластеното лице за обработка на личните податоци (на пр. лозинка за најава во системот, автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолг од 15 минути), редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми, инсталирање на ажурирања на оперативните системи со автоматска верификација согласно процената на ризик, а најмалку еднаш неделно и слично).

(11) Со оглед на фактот што Дирекцијата има своја веб-страница, не применува практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена

нë dollapë dokumentesh të mbyllura me çelës, te të cilat qasje ka vetëm personi i autorizuar për përpunimin e të dhënave, i cili ka qasje edhe deri te hapësirat e caktuara të punës në drejtori. Ruajtja e dokumenteve bëhet në atë mënyrë që të parandalojë çdo hapje të paautorizuar.

(9) Drejtoria domosdoshmërisht e zbaton rregullin “tavolinë e pastër” gjatë përpunimit të të dhënave personale të përfshira në dokumentet për mbrojtjen e tyre nga qasja e personave të paautorizuar gjatë kohës së tërë procesit të përpunimit.

(10) Në drejtori, të dhënat personale që përpunohen dhe ruhen në sistemin e komunikimit dhe atij informativ, gjegjësisht në formë elektronike, mbrohen me atë që paraqitja në sistemin e komunikimit dhe atij informativ bëhet nëpërmjet identifikuesit të veçantë që lidhet vetëm me një person, gjegjësisht me personin e autorizuar për përpunimin e të dhënave personale (p.sh. fjalëkalimi për hyrjen në sistem, dalje automatike nga sistemi informativ pas një periudhe të caktuar pasiviteti (jo më shumë se 15 minuta), përditësim i rregullt i softuerit antivirus dhe politikë e definuar për përditësim të rregullt të programeve softuerike, instalimi i përditësimeve të sistemeve operative me verifikim automatik sipas vlerësimit të rrezikut, të paktën një herë në javë, etj.).

(11) Duke marrë parasysh faktin se drejtoria ka ueb-faqen e saj, nuk zbaton praktika që e rrisin rrezikun nga keqpërdorimi i mundshëm, përpunimi i padëshiruar (aksidental) ose i

обработка на личните податоци, а особено:

- не пренесува лични податоци преку URL без примена на протокол за криптирање (на пр. идентификатори или лозинки);
- не користи небезбедни услуги;
- не употребува сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страни, пристап до електронски пораки и слично;
- не ги поставува базите на податоци на сервери кои се директно достапни преку интернет и
- не ги споделува и употребува корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

(12) Дирекцијата применува технички и организациски мерки за обезбедување на тајност и заштита на личните податоци преку вршење видеонадзор, преку определување на рокот на чување на видео записите, определување на начинот на бришење, определување на начинот на правење сигурносна копија, како и за уредување на правата и обврските на овластените лица кои имаат пристап до системот за вршење на видеонадзорот.

(13) Притоа, од технички аспект, за секое овластено лице се определува единствено корисничко име, лозинка креирана од страна на овластеното лице, корисничко име и лозинка која овозможува пристап на овластеното лице до системот за видеонадзор во целина или поединечни апликации.

qëllimshëm i paautorizuar i të dhënave personale, veçanërisht:

- nuk bartë të dhënat personale nëpërmjet URL pa zbatuar protokollin për kriptim (p.sh. identifikues ose fjalëkalim);
- nuk përdor shërbime të pasigurta;
- nuk shfrytëzon serverë të cilët ruajnë bazat e të dhënave ose serverë si stacione pune, veçanërisht jo për kërkim në ueb-faqe, qasje te emaillet etj;
- nuk i vendos bazat e të dhënave në serverë që janë të qasshëm drejtpërdrejt nëpërmjet internetit dhe
- nuk i ndan dhe nuk i përdor llogaritë e përdoruesve midis dy ose më shumë personave të autorizuar (user accounts).

(12) Drejtoria zbaton masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së të dhënave personale nëpërmjet kryerjen së mbikëqyrjes me video, duke përcaktuar afatin e ruajtjes së video regjistrimeve, përcaktimin e mënyrës së fshirjes, përcaktimin e mënyrës së bërjes së kopjes rezervë, si dhe rregullimin e të drejtave dhe detyrimet e personave të autorizuar të cilët kanë qasje në sistemin e kryerjes së mbikëqyrjes me video.

(13) Kështu nga aspekti teknik, për çdo person të autorizuar përcaktohet emri i përdoruesit i veçantë, fjalëkalimi i krijuar nga ana e personit të autorizuar, emri i përdoruesit dhe fjalëkalimi që mundëson qasje të personit të autorizuar te sistemi i mbikëqyrjes me video në tërësi ose në aplikacione

Воедно, како заштитна мерка против недозволени обиди за влез и пробивање на системот, помеѓу системот за видеонадзор и интернет или која било друга форма на надворешна мрежа, се применува софтверска заштитна мрежна бариера (фајервол или рутер). Од организациски аспект, за обезбедување тајност и заштита на обработката на личните податоци преку системот за видеонадзор, во Дирекцијата се применува ограничен пристап или идентификација за пристап до системот за видеонадзор при што секое овластено лице има ограничен пристап до системот за видео надзор во однос на прегледување на видео записите. Воедно, уредено е автоматското уништување на видеозаписите по истекот на рокот за нивно чување, како и почитување на техничките упатства при инсталирање и користење на опремата за вршење видеонадзор.

индивидуално. Нјекохјесист, си масј mbrojtёse ndaj pёrpjekjeve tё palejuara pёr tё hyrё dhe pёr tё depёrtuar nё sistem, ndёrmjet sistemit tё mbikёqyrjes me video dhe internetit ose ёdo forme tjetёr tё rrjetit tё jashtёm, zbatohet nё pengesё rrjeti mbrojtёse softuerike (firewall ose ruter). Nga aspekti organizativ, pёr sigurimin e fshehtёsisё dhe mbrojtjes sё pёrpunimit tё tё dhёnave personale nёpёrmjet sistemit tё mbikёqyrjes me video, nё drejtori zbatohet qasje e kufizuar ose identifikim pёr qasje deri te sistemi pёr mbikёqyrje me video, ku ёdo person i autorizuar ka qasje tё kufizuar deri te sistemi pёr mbikёqyrje me video nё raport me kontrollimin e regjistrimeve me video. Nјekohјesisht, ёshtё rregulluar edhe asgjёsimi automatik i regjistrimeve me video pas skadimit tё afatit pёr nivelin e ruajtjes, si dhe respektimin e udhёzimeve teknike gjatё instalimit dhe shfrytёzimit tё pajisjeve pёr kryerjen e mbikёqyrjes me video.

Збирки на лични податоци кои се обработуваат и чуваат во Дирекцијата

Пёрмбледhја e тё dhёnave personale тё cilat janё тё pёrpunuara dhe тё ruajtura нё drejtori

Член 4

(1) Во Дирекцијата се обработува и чува збирка на лични податоци на вработените во Дирекцијата која ги содржи следните категории на лични податоци:

- име и презиме;
- име и презиме на еден од двата родители;
- датум на раѓање;
- место на раѓање;
- општина на раѓање
- адреса на живеење или престојување;

Нени 4

(1) Нё drejtori pёrpunohen dhe ruhen mbledhjet e тё dhёnave personale тё тё punёsuarve нё drejtori, e cila i pёrfshinё kategoritё нё vijim тё тё dhёnave personale:

- emri dhe mbiemri;
- emri dhe mbiemri i nјёrit prej prindёrve;
- data e lindjes;
- vendi i lindjes;
- komuna e lindjes;
- adresa e vendbanimit ose vendqёndrimi;

- место/општина на живеење;
- единствен матичен број;
- број на трансакциска сметка;
- држава;
- националност;
- пол;
- телефонски број;
- електронска адреса (е-маил);
- податоци за тековното вработување и за претходните вработувања (група, подгрупа, категорија, ниво и работно место);
- податоци за образованието, стручните квалификации и работните компетенции;
- податоци за висина на плата и висина на надоместоците на плата.
- vendbanimi/ komuna;
- numri i vetëm amzë;
- numri i llogarisë së transaksionit;
- shteti;
- kombësia;
- gjinia;
- numri i telefonit;
- adresa elektronike (e-mail);
- të dhënat për punësimin aktual dhe punësimin e mëparshëm (grupi, nëngrupi, kategoria, niveli dhe vendi i punës);
- të dhënat e shkollimit, kualifikimet profesionale dhe kompetencat e punës;
- të dhënat e pagës dhe lartësia e kompensimit të pagës.

Во рамките на оваа збирка на лични податоци се водат: евиденција за вработените, евиденција за плати, евиденција за редовност на работа, евиденција на задолжување со службена опрема и средства за работа, како и евиденција на службени телефонски броеви.

Податоците на вработените во Дирекцијата се обработуваат и чуваат во хартиена форма (досиеја на вработените) и во електронска форма (систем за управување со човечки ресурси; финансиска евиденција/пресметка на плати и надоместоци). Истите се обработуваат и чуваат во Одделението за управување и развој на човечки ресурси и во Одделението за финансиски прашања.

(2) Во Дирекцијата се обработува и чува збирка на лични податоци на лицата- баратели на безбедносен сертификат за пристап до класифицирани информации, односно на лицата за кои започнува постапка за

Нë куадër të kësaj përmbledhjeje të të dhënave personale mbahet: evidenca e të punësuarve, evidenca e pagave, evidenca e rregullshmërisë në punë, evidenca e detyrimit me pajisje zyrtare dhe mjete të punës, si dhe evidenca e numrave zyrtarë të telefonit.

Të dhënat e të punësuarve në drejtori përpunohen dhe ruhen në formë të shkruar (dosja e të punësuarve) dhe në formë elektronike (sistemi i menaxhimit me burimet njerëzore; evidenca financiare/llogaria e pagave dhe kompensimeve). Të njëjtat përpunohen dhe ruhen në Njësinë e menaxhimit dhe zhvillimit të burimeve njerëzore dhe në Njësinë e çështjeve financiare.

(2) Në drejtori përpunohen dhe ruhen përmbledhjet e të dhënave personale të personave- parashtresit të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara, gjegjësisht personat për të cilat fillohet procedurë

издавање безбедносен сертификат за пристап до класифицирани информации и на лицата кои ги поминале безбедносните проверки за издавање безбедносен сертификат која ги содржи следните категории на лични податоци:

- име и презиме;
- датум и место на раѓање;
- адреса на живеење или престојување;
- единствен матичен број;
- податоци за документи за лична идентификација (лична карта или патна исправа);
- матичен лекар;
- здравствена состојба;
- брачен статус;
- име и презиме на членовите на семејството на лицето-барател на безбедносен сертификат;
- име и презиме на лица коишто живеат во исто домаќинство со лицето-барател на безбедносен сертификат;
- телефонски број;
- електронска адреса (е-маил).

Податоците од оваа збирка се обработуваат и чуваат во хартиена форма и во електронска форма (наменски изработен софтвер за предметите врзани за барањата за издавање безбедносен сертификат за пристап до класифицирани информации). Истите се обработуваат и чуваат во Одделението за персонална безбедност и во Одделението за индустриска безбедност.

(3) Во Дирекцијата се обработува и чува збирка на податоци на странките и трети лица при водење на управни постапки и прекршочни постапки согласно Законот за општата управна

пër lëshimin e certifikatës së sigurisë për qasje deri te informacionet e klasifikuara dhe të personave të cilët i kanë kaluar kontrollet e sigurisë për lëshimin e certifikatës së sigurisë e cila i përfshinë kategoritë e të dhënave personale si në vijim:

- emri dhe mbiemri;
- data dhe vendi i lindjes;
- adresa e vendbanimit ose vendqëndrimi;
- numri i vetëm amzë;
- të dhënat e dokumenteve për identifikim personal (letërnjoftim ose dokument udhëtimi);
- mjeku amë;
- gjendja shëndetësore;
- statusi martesor;
- emri dhe mbiemri i anëtarëve të familjes së personit – parashtruesi i certifikatës së sigurisë;
- emri dhe mbiemri i personit i cili jeto në të njëjtën shtëpi me personin – parashtruesi i certifikatës së sigurisë;
- numri i telefonit;
- adresa elektronike (e-maili).

Të dhënat nga kjo përmbledhje përpunohen dhe ruhen në formë të shkruar dhe në formë elektronike (Softuer i krijuar me qëllim për lëndët që lidhen me kërkesat për lëshimin e certifikatës së sigurisë për qasje deri te informacionet e klasifikuara). Të njëjtat përpunohen dhe ruhen në Njësine e sigurisë personale dhe në Njësine e sigurisë industriale.

(4) Në drejtori përpunohen dhe ruhen përmbledhja e të dhënave të palëve dhe personave të tretë gjatë mbajtjes së procedurave administrative dhe atyre të kundërvajtjes në pajtim me

постапка и Законот за класифицирани информации(*) која ги содржи следните категории на лични податоци:

- име и презиме;
- адреса на живеење или престојување;
- единствен матичен број;
- телефонски број;
- електронска адреса (е-маил);
- други лични податоци потребни за изведување како докази во постапките согласно закон.

Податоците од оваа збирка се обработуваат и чуваат во хартиена форма и во електронска форма. Истите се обработуваат и чуваат во Одделението за персонална безбедност.

(4) Во Дирекцијата се обработува и чува збирка на податоци на лица-баратели на безбедносен сертификат за пристап до класифицирани информации кои ја посетуваат веб-страната на Дирекцијата заради пристапување кон Електронскиот систем за обука на Дирекцијата која ги содржи следните категории на лични податоци:

- име и презиме;
- назив на работодавач;
- електронска адреса (е-маил).

Податоците од оваа збирка се обработуваат и чуваат во електронска форма. Истите се обработуваат и чуваат во Одделението за безбедносна акредитација на комуникациско-информатички системи и за комуникациско-информатичка поддршка безбедност.

(5) Во Дирекцијата се обработува и чуваат видеозаписи што произлегуваат од вршењето на видеонадзорот во

Ligjin e Procedurës së Përgjithshme Administrative dhe Ligjin e Informacioneve të Klasifikuara (*), që i përfshinë kategoritë e të dhënave personale si në vijim:

- emri dhe mbiemri;
- adresa e vendbanimit ose vendqëndrimi;
- numri i vetëm amzë;
- numri i telefonit;
- adresa elektronike (e-mail);
- të dhëna të tjera personale të nevojshme për paraqitje si dëshmi në procedurat në pajtim me ligjin.

Të dhënat nga kjo përmbledhje përpunohen dhe ruhen në formë të shkruar dhe në formë elektronike. Të njëjtat përpunohen dhe ruhen në Njësine e sigurisë personale.

(4) Në drejtori përpunohen dhe ruhen përmbledhjet e të dhënave të personave- parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara, të cilët e vizitojnë ueb-faqen e drejtorisë për shkak të qasjes te Sistemi elektronik i trajnimit në drejtori, e cila i përfshinë kategoritë e të dhënave personale në vijim;

- emri dhe mbiemri;
- emri i punëdhënësit;
- adresa elektronike (e-maili)

Të dhënat nga kjo përmbledhje përpunohen dhe ruhen në formë elektronike. Të njëjtat përpunohen dhe ruhen në Njësine e akreditimit të sigurisë së sistemeve të komunikimit dhe të informimit dhe për mbështetjen e sigurisë së komunikimit dhe të informimit.

(5) Në drejtori përpunohen dhe ruhen regjistrimet me video, që dalin nga kryerja e mbikëqyrjes me video në

Дирекцијата коишто содржат сликовен приказ на физичкиот изглед на вработените во Дирекцијата и на странките и третите лица што влегуваат во/излегуваат од просториите на Дирекцијата.

Видеозаписите се обработуваат и чуваат во електронска форма. Со видеозаписите ракува одговорното лице за спроведување видеонадзор од Одделението за физичка безбедност.

директори, të cilat përfshijnë tregues me fotografi të pamjes fizike të të punësuarve në drejtori dhe në palët dhe personat e tretë të cilët hynë/dalin nga hapësira e drejtorisë.

Regjistrimet me video përpunohen dhe ruhen në formë elektronike. Me regjistrimet me video udhëheqë personi përgjegjës për realizimin e mbikëqyrjes me video nga Njësia e sigurisë fizike.

Цели на обработката на личните податоци

Qëllimet e përpunimit të të dhënave personale

Член 5

Neni 5

(1) Целта на обработката на личните податоци е директно поврзана со постоењето на законски основ за обработка на личните податоци и законитоста на обработката на личните податоци.

(1) Qëllimi i përpunimit të të dhënave personale është drejtpërdrejt i lidhur me ekzistencën e bazës ligjore për përpunimin e të dhënave personale dhe ligjshmërinë e përpunimit të të dhënave personale.

(2) Податоците од збирката на лични податоци на вработените во Дирекцијата се обработуваат заради исполнување на законските одредби од доменот на трудовото право и управувањето со човечките ресурси во Дирекцијата, со цел:

(2) Të dhënat nga përmbledhja e të dhënave personale të të punësuarve në drejtori, përpunohen për shkak të përmbushjes së dispozitave ligjore në fushën e të drejtës së punës dhe menaxhimin me burimet njerëzore në drejtori, me qëllim:

- уредување на работните односи меѓу работниците и работодавачот;
- остварување и заштита на правата од работен однос кај работодавачот и надлежните органи и институции;
- уредување на обврските и одговорностите од работниот однос меѓу работниците и работодавачот;

- rregullimin e marrëdhënieve të punës midis punonjësve dhe punëdhënësit;
- realizimin dhe mbrojtjen e të drejtës së marrëdhënies së punës te punëdhënësi dhe organi kompetent dhe institucionet;
- rregullimin e detyrimeve dhe përgjegjësi të marrëdhënies së punës midis

- | | |
|--|---|
| | punonjësve dhe punëdhënësit; |
| - уредување на односите меѓу раководниот кадар и вработените и на односите меѓу вработените; | - rregullimin e marrëdhënieve midis kuadrit udhëheqës dhe të punësuarve dhe të marrëdhënieve midis të punësuarve; |
| - анализа на човечките ресурси (работната сила); | - analizën e burimeve njerëzore (fuqia punëtore); |
| - управување со податоците на персоналот – работната сила. | - menaxhimin me të dhënat e personelit- fuqia punëtore. |

(3) Податоците од збирката на лични податоци на лицата-баратели на безбедносен сертификат за пристап до класифицирани информации, односно на лицата за кои започнува постапка за издавање безбедносен сертификат за пристап до класифицирани информации и на лицата кои ги поминале безбедносните проверки за издавање безбедносен сертификат се обработуваат со цел исполнување на законската надлежност за издавање безбедносни сертификати од страна на директорот на Дирекцијата¹ и за водење соодветна евиденција за издадените безбедносни сертификати, пополнетите безбедносни прашалници и издадените дозволи за пристап до класифицирани информации во Република Северна Македонија.² Притоа, обработката е ограничена на оние лични податоци што се утврдени со безбедносниот прашалник, чијшто составен дел е и Изјавата што ја потпишува лицето за вистинитост, целосност и точност на дадените податоци со согласност истите да бидат проверени заради издавање на безбедносен сертификат за пристап до класифицирани информации.³

(3) Тë dhënat nga përmbledhja e të dhënave personale të personave-parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara, gjegjësisht të personave për të cilët fillohet procedurë për lëshimin e certifikatës së sigurisë për qasje deri te informacionet e klasifikuara dhe të personave të cilët i kanë kaluar kontrollet e sigurisë për lëshimin e certifikatës së sigurisë për përpunim me qëllim përmbushjen e kompetencave ligjore për lëshimin e certifikatës së sigurisë nga ana e drejtorit të drejtorisë¹ dhe për mbajtjen e evidencës përkatëse për lëshimin e certifikatës së sigurisë, plotësimin e pyetësorëve të sigurisë dhe lejet e lëshuara për qasje deri te informacionet e klasifikuara në Republikën e Maqedonisë së Veriut². Kështu, përpunimi është i kufizuar për ato të dhëna personale që janë përcaktuar nga pyetësi i sigurisë, pjesë përbërëse e të cilit është edhe Deklarata që e nënshkruan personi për vërtetësinë, plotësinë dhe saktësinë e të dhënave të lëshuara në pajtim që të njëjtat të kontrollohen për shkak të lëshimit të

¹ Ligji i Informacioneve të Klasifikuara(*) (Gazeta Zyrtare e RMV-së, nr. 275/19), neni 39

² Njëjtë, neni 64.

³ Rregullore për format dhe përmbajtjet e formularëve të pyetësorit të sigurisë dhe të certifikatave të sigurisë (Gazeta Zyrtare e RMV-së, nr. 123/20)

certifikatës së sigurisë për qasje deri te informacionet e klasifikuara³.

(4) Податоците од збирката на лични податоци на странките и трети лица при водење на управни постапки и прекршочни постапки согласно Законот за општата управна постапка и Законот за класифицирани информации(*) се обработуваат за истата цел како и податоците од збирката на податоци на лицата-баратели на безбедносен сертификат за пристап до класифицирани информации од причина што сите дејствија коишто се рефлектираат врз поседувањето безбедносен сертификат на едно лице се дел од комплексен процес. Дирекцијата има законска обврска при постапувањето по жалби од страна на лица на коишто им било издадено решение за одбивање на барањето за издавање безбедносен сертификат, како и законски надлежности при постапувањето по претставки за лица коишто ги прекршиле одредбите од Законот за класифицирани информации(*).

(5) Личните податоци од збирката на податоци на странките и трети лица при водење на управни постапки и прекршочни постапки согласно Законот за општата управна постапка и Законот за класифицирани информации(*) и од збирката на податоци на лицата баратели на безбедносен сертификат за пристап до класифицирани информации се обработуваат и чуваат во посебни досиеја за секој барател на безбедносен сертификат одделено и претставуваат дел од единствена евиденција којашто се води во Дирекцијата во електронска форма и има ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“.

(4) Тë dhënat nga përmbledhja e të dhënave personale të palëve dhe personave të tretë gjatë mbajtjes së procedurave administrative dhe të kundërvajtjes në pajtim me Ligjin e Procedurës së Përgjithshme Administrative dhe Ligjit të Informacioneve të Klasifikuara(*), përpunohen për qëllim të njëjtë si dhe të dhënat nga përmbledhja e të dhënave personale – parashtruesi i certifikatës së sigurisë për qasje deri te informacionet e klasifikuara nga arsyeja që të gjitha veprimtaritë të cilat reflektohen në bazë të posedimit të certifikatës së sigurisë të një personi janë pjesë e procesit kompleks. Drejtoria ka detyrim ligjor të veprojë për ankesat nga ana e personave të cilëve u është lëshuar aktvendim për refuzimin e kërkesës për lëshimin e certifikatës së sigurisë, si dhe kompetenca ligjore në veprimin me pretekst për personat të cilat kanë bërë shkelje të dispozitave të Ligjit të Informacioneve të Klasifikuara(*).

(5) Тë dhënat personale të përmbledhura në të dhënat e palëve dhe personave të tretë gjatë mbajtjes së procedurave administrative dhe të procedurave të kundërvajtjes, në pajtim me Ligjin e Procedurës së Përgjithshme Administrative dhe të Ligjit të Informacioneve të Klasifikuara (*) dhe nga përmbledhja e të dhënave të personave parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara që përpunohen nga parashtruesit e certifikatës së sigurisë veçanërisht dhe paraqesin pjesë nga evidenca e vetme e cila udhëhiqet nga drejtoria në formë elektronike dhe ka

shenjën “PËR PËRDORIM TË KUFIZUAR”.

(6) Личните податоци од збирката на податоци на лица-баратели на безбедносен сертификат за пристап до класифицирани информации кои ја посетуваат веб-страницата на Дирекцијата заради пристапување кон Електронскиот систем за обука на Дирекцијата се обработуваат со цел ефикасно обезбедување на бараната услуга, исполнување на законската обврска за организирање и спроведување обуки за безбедност на класифицирани информации,⁴ како и за анализа на посетите на порталот, односно барањата за пристап до Електронскиот систем за обука на Дирекцијата. Притоа, обработката е ограничена на оние лични податоци што се потребни за овозможување пристап до системот.

(7) Целта на обработката на податоците од видеозаписите што произлегуваат од вршењето на видеонадзорот во Дирекцијата е идентификација на лицата (вработени, странки и трети лица) што имаат право на влез во просториите и излез од просториите на Дирекцијата. Тоа подразбира почитување на прописите за движење во определените безбедносни зони во Дирекцијата, како и во одредени простории во коишто влезот е дозволен само на овластени лица, определени од страна на директорот на Дирекцијата со посебна одлука.

Рокови за чување и архивирање на личните податоци

Член 6

(6) Тë dhënat personale nga përmbledhja e të dhënave të personave – parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara të cilët e vizitojnë ueb-faqen e drejtorisë për shkak të qasjes tek Sistemi elektronik i trajnimeve të drejtorisë, përpunohen me qëllim sigurimin efikas të shërbimit të kërkuar, përmbushjen e detyrimit ligjor për organizimin dhe realizimin e trajnimeve për sigurinë e informacioneve të klasifikuara⁴, si dhe për analizimin e vizitave në portal, gjegjësisht kërkesat për qasje deri te Sistemi elektronik i trajnimeve të drejtorisë. Kështu përpunimi është i kufizuar për ato të dhëna personale, që janë të nevojshme për të mundësuar qasje deri te sistemi.

(7) Qëllimi i përpunimit të të dhënave nga regjistrimet me video të cilat dalin nga kryerja e mbikëqyrjes me video në drejtori është identifikimi i personit (të punësuarit, palët dhe personat e tretë) që kanë të drejtë të hyjnë dhe të dalin nga hapësirat e drejtorisë. Kjo nënkupton respektimin e rregullave për lëvizje në zonat e caktuara të sigurisë në drejtori, si dhe në hapësirat e caktuara ku hyrja është e lejuar vetëm për personat e autorizuar, të caktuar nga ana e drejtorit të drejtorisë me vendim të veçantë.

Afatet për ruajtjen dhe arkivimin e të dhënave personale

Neni 6

⁴ Ligji i Informacioneve të Klasifikuara(*), neni 69, paragrafi 2, nënparagrafi 10.

(1) Дирекцијата ги почитува законски предвидените рокови за чување на личните податоци, па така и податоците од збирката за човечки ресурси и трудово право се чуваат согласно прописите за архивско работење. Следствено на тоа, досиејата на вработените се чуваат 45 години од периодот на престанок на работниот однос на вработениот, а за останатите лични податоци (избор на кандидати за работа, документи за користење годишен одмор, боледување, отсуство, пресметка на плата и на надоместоци на плата и слично), Дирекцијата ги определува роковите за чување, согласно важечката Листа на документарен материјал со рокови на негово чување.

(2) Во случај на престанок на работниот однос, досиејата на тие вработени се чуваат одделно. Со тоа Дирекцијата го ограничува пристапот до досието на поранешен вработен од причина што секторот за човечки ресурси повеќе нема потреба на дневна основа да пристапува до овие податоци.

(3) Збирката на податоци заради спроведување на конкретни права и обврски од областа на трудовото право и човечки ресурси се чува во ормари за чување документи со клуч до кои пристап има овластеното лице за обработка на податоците.

(4) Збирката на податоци на лицата баратели на безбедносен сертификат за пристап до класифицирани информации, односно на лицата за кои започнува постапка за издавање безбедносен сертификат за пристап до класифицирани информации и на лицата кои ги поминале безбедносните проверки за издавање безбедносен сертификат се чува во ормари за чување

(1) Drejtoria i respekton afatet e parapara me ligj për ruajtjen e të dhënave personale, kështu edhe të dhënat nga përmbledhja e burimeve njerëzore dhe të drejtës së punës ruhen në pajtim me rregullat për punë arkivore. Si rrjedhojë, dosjet e të punësuarve ruhen 45 vjet nga periudha e ndërprerjes së marrëdhënies së punës të të punësuarit, kurse për të dhënat e tjera personale (zgjedhja e kandidatit për punë, dokumente për shfrytëzimin e pushimit vjetor, pushimi mjekësor, mungesa në punë, llogaria e pagës dhe e kompensimeve të pagës dhe të ngjashme), drejtoria i përcakton afatet për ruajtje në pajtim me Listën e vlefshme të materialit të dokumentuar me afatet e ruajtjes.

(2) Në rast të ndërprerjes së marrëdhënies së punës, dosjet e atyre të punësuarve ruhen në veçanti. Me këtë drejtoria e kufizon qasjen deri te dosja e të punësuarit të mëparshëm për arsye se sektori i burimeve njerëzore nuk ka nevojë më tepër të qaset deri te këto të dhëna.

(3) Përmbledhja e të dhënave për shkak të realizimit të të drejtave dhe detyrimeve konkrete nga fusha e të drejtës së punës dhe burimeve njerëzore, ruhen në dollapë të mbyllura me çelës për ruajtjen e dokumenteve, deri te të cilat qasje ka vetëm personi i autorizuar për përpunimin e të dhënave.

(4) Përmbledhja e të dhënave të personave parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara, gjegjësisht procedura e filluar për personat për lëshimin e certifikatës së sigurisë për qasje deri te informacionet e klasifikuara dhe për personat të cilët i kanë kaluar kontrollet e sigurisë për lëshimin e certifikatës së sigurisë dhe ruhet në dollapë me çelës

документи со клуч до кои пристап има овластеното лице за обработка на податоците.

(5) Збирката на податоци на странките и трети лица при водење на управни постапки и прекршочни постапки согласно Законот за општата управна постапка и Законот за класифицирани информации(*) се чува во ормари за чување документи со клуч до кои пристап има овластеното лице за обработка на податоците.

(6) Збирката на податоци на лица баратели на безбедносен сертификат за пристап до класифицирани информации кои ја посетуваат веб-страната на Дирекцијата заради пристапување кон Електронскиот систем за обука на Дирекцијата се чува во електронска форма (data base) на комуникациско-информациски систем на којшто се имплементирани безбедносни мерки што овозможуваат пристап само на овластеното лице за обработка на податоците. Овие податоци се чуваат согласно роковите утврдени во процедурите за работа на електронскиот систем за учење на Дирекцијата за важењето на потврдата за успешно помината обука.

(7) Видеозаписите што произлегуваат од вршењето на видеонадзорот во Дирекцијата се чуваат до 180 дена на хард-дискот (hard disk) на персоналниот компјутер во работната просторија на овластеното лице за обработка на лични податоци преку системот за вршење видеонадзор. По истекот на рокот, истите автоматски се бришат.

(8) Личните податоци за кои сè уште не истекол рокот за нивно чување согласно закон, а за кои престанала

пër ruajtjen e dokumenteve, ku qasje ka personi i autorizuar për përpunimin e të dhënave.

(5) Përmbledhja e të dhënave të palëve dhe personave të tretë në udhëheqjen e procedurave administrative dhe procedurave të kundërvajtjes në pajtim me Ligjin e Procedurës së Përgjithshme Administrative për Informacione të Klasifikuara(*), ruhen në dollapë me çelës për ruajtjen e dokumenteve, ku qasje ka personi i autorizuar për përpunimin e të dhënave.

(6) Përmbledhja e të dhënave të personave parashtrues të certifikatës së sigurisë për qasje deri te informacionet e klasifikuara, të cilët e vizitojnë ueb-faqen e drejtorisë për shkak të qasjes të Sistemi elektronik i trajnimit të drejtorisë për ruajtjen në formë elektronike të (data base) sistemit të komunikimit dhe atij informativ, ku janë zbatuar masat e sigurisë që mundësojnë qasje vetëm të personit të autorizuar për përpunimin e të dhënave. Këto të dhëna ruhen në pajtim me afatet e përcaktuara në procedurën e punës së sistemit elektronik të mësimi të drejtorisë për vlefshmërinë e vërtetimit për trajnimin e përfunduar me sukses.

(7) Regjistrimet me video që dalin nga kryerja e mbikëqyrjes me video në drejtori, ruhen deri më 180 ditë në hard diskun (hard disk) e kompjuterit personal në hapësirën e punës së personit të autorizuar për përpunimin e të dhënave personale, nëpërmjet sistemit për kryerjen e mbikëqyrjes me video. Pas skadimit të afatit, të njëjtat fshihen në mënyrë automatike.

(8) Të dhënat personale të cilave ende nuk u ka skaduar afati për ruajtjen e tyre në pajtim me ligjin, por të cilat nuk

потребата од нивна непосредна и секојдневна обработка, Дирекцијата ги архивира на безбеден начин, особено ако архивираниите податоци се посебни категории на лични податоци (чувствителни податоци) или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци доколку бидат компромитирани.

janë më të nevojshme për përpunimin e tyre të menjëhershëm dhe të përditshëm, drejtoria i arkivon në mënyrë të sigurt, veçanërisht nëse të dhënat e arkivit janë kategori e veçantë e të dhënave personale (të dhëna të ndjeshme) ose të dhëna që mund të kenë ndikim serioz mbi subjektet e të dhënave personale nëse komprometohen.

Копирање, умножување и уништување на документите

Kopjimi, shumëfishimi dhe asgjësimi i dokumenteve

Член 7

Neni 7

(1) Копирањето или умножувањето на документите се врши единствено од страна на овластени лица определени со процедура од страна на Дирекцијата.

(2) Уништувањето на копиите или умножените документи се врши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци, односно да не можат истите повторно да бидат искористени (рачно кинење и ситнење, уништување со машина или горење).

(3) За уништувањето на документите комисијски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

(4) По пренесувањето на личните податоци од медиумот на којшто истите се содржани во електронска форма или

(1) Kopjimi ose shumëfishimi i dokumenteve, bëhet veçanërisht nga ana e personit të autorizuar të caktuar me procedurë nga ana e drejtorisë.

(2) Asgjësimi i kopjeve ose shumëfishimi i dokumenteve bëhet në atë mënyrë që do të mundësojë parandalimin e rikuperimit të të dhënave personale që përmbahen në to, gjegjësisht të mos mundet të njëjtat prapë të shfrytëzohen (shqyerja dhe copëtimi me duar, asgjësimi me makinë ose djegie).

(3) Për asgjësimin e dokumenteve nga komisioni përpilohet procesverbal, i cili përfshinë të gjitha të dhënat për identifikim të plotë të dokumentet, si dhe për kategoritë e të dhënave personale të përfshira në të.

(4) Pas bartjes së të dhënave personale nga media, ku të njëjtat përfshihen në formë elektronike ose pas

по истекот на определениот рок за нивно чување, медиумот се брише или пак се чисти од личните податоци што се содржани на него.

(5) Уништувањето на медиумот се врши со механичко разделување на неговите составни делови при што истиот повторно да не може да биде употреблив. Бришењето или чистењето на медиумот се врши на начин што оневозможува понатамошно обновување на снимените лични податоци.

(6) За уништувањето и бришењето или чистењето на медиумот се составува записник што содржи податоци за идентификација на медиумот и на категориите на лични податоци што биле снимени на истиот.

Одговорност на раководниот кадар и на вработените за заштита на личните податоци

Член 8

(1) Раководството на Дирекцијата треба да биде запознаено со имплементираните технички и организациски мерки и да придонесува за унапредување на системот за заштита на личните податоци во Дирекцијата. Со тоа што безбедноста ќе биде третирана на ниво на раководството, раководниот кадар ќе се грижи за подигнување на свеста за ризиците и заштита на личните податоци, ќе бидат обезбедени доволно ресурси за таа намена, итн.

(2) Во таа насока, раководството е должно да ги донесе пропишаните документи (политики, планови, правилници и други акти) од областа на заштитата на личните податоци, да

skadimit të afatit të caktuar për ruajtjen e tyre, media fshihet ose pastrohet nga të dhënat personale që përfshihen në të.

(5) Asgjësimi i medias bëhet me ndarje mekanike të pjesëve përbërëse të saj, ku e njëjta përsëri të mos mundet të jetë e përdorshme. Fshirja ose pastrimi i medias bëhet në mënyrën që të pamundësojë rikuperimin e mëtejshëm të të dhënave personale të regjistruara.

(6) Për asgjësimin dhe fshirjen ose pastrimin e medias, përpilohet procesverbal që përfshinë të dhënat për identifikimin e medias dhe kategoritë e të dhënave personale që kanë qenë të regjistruara në të.

Përgjegjësia e kuadrit udhëheqës dhe të punësuarave për mbrojtjen e të dhënave personale

Neni 8

(1) Udhëheqësit e drejtorisë duhet të jenë të njoftuar me masat e zbatuara teknike dhe organizative dhe të kontribuojnë në avancimin e sistemit të mbrojtjes së të dhënave personale në drejtori. Me atë që siguria do të trajtohet në nivelin e udhëheqjes, kuadri udhëheqës do të kujdeset për ngritjen e ndërgjegjes për rreziqet dhe mbrojtjen e të dhënave personale, do të sigurohen burime të mjaftueshme për këtë qëllim, etj.

(2) Në atë drejtim, udhëheqja është e detyruar t'i miratojë dokumentet e përcaktuara (politikat, planet, rregulloret dhe aktet e tjera) nga fusha e mbrojtjes së të dhënave personale, të

воспостави систем за заштита на личните податоци и точно да ги определи и соодветно да ги распредели задолженијата и работните задачи за ефикасно спроведување на заштитата на личните податоци.

(3) Исто така, раководството треба да ја развива културата на почитување на заштитата на личните податоци. Тоа значи дека раководниот кадар треба да избере компетентни, доверливи и одговорни вработени лица, како и да манифестира пристап кон унапредување на компетенциите на вработените во доменот на заштитата на личните податоци во поглед на правата, но и различните видови одговорност кои може да произлезат од непочитувањето на законските услови и стандардите за заштита на личните податоци.

(4) Клучни компоненти на овој процес се:

- **креирање на документацијата** – при креирање на документацијата, најраспространет е слоевитиот пристап. Според овој пристап, на најгорниот слој се документи од високо ниво со кои се дефинираат политиките на Дирекцијата во улога на контролор. Во следниот слој се наоѓаат подетални документи со кои се определуваат видовите на контрола коишто ќе се имплементираат со цел да се реализираат политиките. Во третиот слој се наоѓаат најдеталните документи со кои се опишани оперативните процеси;
- **технологијата при примена на принципот на безбедност на електронските информации** – контролорот мора да се осигура дека новата технологија може да

кrijojë sistem për mbrojtjen e të dhënave personale dhe me saktësi t'i përcaktojë dhe në mënyrë adekuate t'i shpërndajë detyrat dhe obligimet e punës për zbatimin efikas të mbrojtjes së të dhënave personale.

(3) Gjithashtu, udhëheqësit duhet ta zhvillojnë kulturën e respektimit për mbrojtjen e të dhënave personale. Kjo d.m.th. se kuadri udhëheqës duhet të zgjedhë punonjës kompetentë, të besueshëm dhe përgjegjës, si dhe të manifestoje qasje tek avancimet e kompetencave të të punësuarve në fushën e mbrojtjes së të dhënave personale në pikëpamje të të drejtave, por edhe llojet e ndryshme të përgjegjësisë që mund të dalin nga mosrespektimi i kushteve ligjore dhe standardeve për mbrojtjen e të dhënave personale.

(4) Komponentët kyç të këtij procesi:

- **krijimi i dokumentacioneve** – gjatë krijimit të dokumentacioneve, qasja më e zakonshme është ajo e shtresave. Sipas kësaj qasjeje, në shtresën e lartë janë dokumentet e nivelit të lartë që përcaktojnë politikat e drejtorisë në rolin e saj si kontrollues. Shtresa tjetër në vijim përfshin dokumente më të detajuara që përcaktojnë llojet e kontrolleve që do të zbatohen për realizimin e politikave. Në shtresën e tretë përfshihen dokumentet më të detajuara që përshkruajnë proceset operative;
- **teknologjia në zbatimin e parimit të sigurisë së informacioneve elektronike** – kontrolluesi duhet të sigurojë që teknologjia e re mund të

ги задоволи барањата на принципот на безбедност. Освен енкрипцијата, постојат и други задолжителни барања, како што се антивирус, антиспам, firewall, управување со пристапот (access management), детекција на инциденти, превенција од губење податоци (data loss prevention), двофакторска автентикација и лог менаџмент;

- **физичка околина** - безбедна физичка околина е уште еден дел од генералната безбедност. Софистицирани контролни системи за влез, видеонадзор, заклучени плакари и правилото „чисто биро“ се само дел од контролните мерки кои ѝ се на располагање на Дирекцијата во улога на контролор;

- **управување со ризици од обработувачи и добавувачи** - Дирекцијата мора:

- да одбере соодветни обработувачи согласно законските одредби,
- да склучи договор со обработувачот и
- да спроведе контрола на квалитет и усогласеност за времетраење на договорот.

(5) Секој вработен во Дирекцијата, во својство на овластено лице кое има пристап до личните податоци ги има следните обврски и одговорности:

- да се придржува до сите правила и процедури востановени со донесените интерни акти на Дирекцијата;
- да ги применува сите мерки на физичка безбедност на

plotësojë kërkesat e parimit të sigurisë. Përveç kriptimit, ekzistojnë edhe kërkesa të tjera të detyrueshme, si antivirus, antispam, firewall, menaxhim me qasjen (access management), zbulimi i incidenteve, parandalimi i humbjes së të dhënave (data loss prevention), autentifikimi me dy faktorë dhe menaxhimi i regjistrave;

- **mjedisi fizik** - mjedisi i sigurt fizik është një pjesë tjetër e sigurisë së përgjithshme. Sistemet e sofistikuara të kontrollit të hyrjes, mbikëqyrja me video, dollapët e mbyllur dhe rregulli i "tavolinës së pastër" janë vetëm disa nga masat e kontrollit që disponon drejtoria në rolin e saj si kontrollues;

- **Menaxhimi i rrezikut nga përpunuesit dhe furnizuesit** - Drejtoria duhet:

- të zgjedhë përpunuesit e duhur në pajtim me dispozitat ligjore,
- të lidh kontratë me përpunuesin dhe
- të kryejë kontroll të cilësisë dhe pajtueshmërisë për kohëzgjatjen e kontratës.

(5) Çdo i punësuar në drejtori, në cilësinë e personit të autorizuar, i cili ka qasje te të dhënat personale i ka detyrimet dhe përgjegjësitë në vijim:

- t'i përmbahet të gjitha rregullave dhe procedurave të përcaktuara me akte të brendshme të miratuara të drejtorisë;
- t'i zbatojë të gjitha masat e sigurisë fizike në hapësirat ku gjenden të dhënat personale;

просториите каде што се наоѓаат личните податоци;

- не смее да ја прекршува преземената обврска за доверливост со која се обврзува дека секој податок до кој ќе дојде во текот на работењето во Дирекцијата, а кој спаѓа во категоријата на личен податок согласно прописите за заштита на личните податоци, ќе го чува како доверлив и нема да го пренесува, оддава, ниту на друг начин ќе го стави на располагање на кое било друго лице и во која било форма, надвор од системот на пропишани и воспоставени технички и организациски мерки според кои Дирекцијата врши обработка на личните податоци;
- покрај договор за работа, овластеното лице потпишува и изјава за тајност и заштита на личните податоци;
- овластеното лице при работа со документи кои содржат лични податоци треба да внимава истите да не ги направи непотребно видливи за трети лица;
- овластеното лице по престанокот на работното време и за време на паузи и отсуства документите кои содржат лични податоци треба да ги чува на место на кое што нема да бидат непотребно видливи.

(6) Овластените лица за обработка на збирките на лични податоци

- nuk duhet të shkelë detyrimin e marrë për konfidencialitetin, i cili e detyron të ruajë çdo të dhënë që merr gjatë punës së tij në drejtori dhe që hyn në kategorinë e të dhënave personale në pajtim me rregulloret për mbrojtjen e të dhënave personale, do t'i ruaj si konfidenciale dhe nuk do t'i transferojnë, tregojë, apo t'i bëjnë të disponueshme për ndonjë person tjetër dhe në çfarëdo forme, jashtë sistemit të masave të përcaktuara dhe të vendosura teknike dhe organizative, sipas të cilave drejtoria përpunon të dhënave personale;

- krahas kontratës së punës, personi i autorizuar nënshkruan dhe deklaron për fshehtësinë dhe mbrojtjen e të dhënave personale;

- personi i autorizuar gjatë punës me dokumente të cilat i përfshijnë të dhënave personale, duhet të jetë i kujdesshëm që të mos i bëjë ato të dukshme në mënyrë të panevojshme për palët e treta;

- personi i autorizuar pas përfundimit të orarit të punës dhe gjatë kohës së pauzave dhe mungesave, dokumentet të cilat përfshijnë të dhënave personale, duhet t'i ruajë në vendin ku nuk do të duken pa qenë e nevojshme.

(6) Personat e autorizuar për përpunimin e përmbledhjes së të

задолжително се информираат за техничките и организациските мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

dhënave personale, domosdoshmërisht informohen për masat teknike dhe organizative, të cilat kanë të bëjnë me realizimin e detyrimeve dhe përgjegjësi të tyre.

Одговорни лица за заштита на личните податоци

Personat përgjegjës për mbrojtjen e të dhënave personale

Член 9

Neni 9

(1) За спроведување на системот за заштита на личните податоци, во Дирекцијата се определуваат офицер за заштита на личните податоци, лице одговорно за информацискиот систем и лице одговорно за видеонадзорот.

(2) Офицерот за заштита на личните податоци е вработен во Дирекцијата и за прашања од доменот на одговорност директно одговара пред директорот на Дирекцијата. Тој е должен да ја почитува тајноста или доверливоста во однос на извршувањето на своите работи, во согласност со закон.

(3) Офицерот за заштита на личните податоци може да врши и други задачи и должности при што Дирекцијата, во својство на контролор, обезбедува дека таквите задачи и должности не доведуваат до судир на интереси.

(4) Офицерот за заштита на личните податоци ги врши најмалку следните работи:

- ги информира и советува контролорот или обработувачот и вработените кои вршат обработка на личните податоци за нивните обврски според одредбите од

(1) Për zbatimin e sistemit të mbrojtjes së të dhënave personale, në drejtori caktohet oficeri i mbrojtjes së të dhënave personale, personi përgjegjës për sistemin informativë dhe person përgjegjës për mbikëqyrje me video.

(2) Oficeri i mbrojtjes së të dhënave personale është i punësuar në drejtori dhe për çështje nga fusha e përgjegjësisë drejtpërdrejt i përgjigjet drejtorit të drejtorisë. Ai është i detyruar ta respektojë fshehtësinë dhe konfidencialitetin në raport me realizimin e çështjeve të tyre, në pajtim me ligjin.

(3) Oficeri i mbrojtjes së të dhënave personale mund të kryejë edhe detyra dhe obligime të tjera, të cilat drejtoria në cilësinë e kontrolluesit, siguron se detyrat dhe obligimet e tilla të mos dërgojnë në konflikt interesi.

(4) Oficeri i mbrojtjes së të dhënave personale i realizon këto punë:

- informon dhe këshillon kontrolluesin ose përpunuesin dhe të punësuarit të cilët kryejnë përpunimin e të dhënave personale për detyrimet e tyre sipas dispozitave nga Ligji i

Законот за заштита на личните податоци(*);

- ја следи усогласеноста на постапувањето со личните податоци во Дирекцијата со Законот за заштита на личните податоци(*) и други релевантни закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распределување на обврски, подигнување на свеста и обучување на вработените кои што учествуваат во операциите на обработка,
- врши контроли за заштита на личните податоци;
- врши редовна проценка за потребата за изготвување и донесување нови интерни акти или промена на постојните од аспект на нивно усогласување со прописите за заштита на личните податоци;
- каде што е потребно, дава совети во однос на процената на влијанието на предвидените активности на обработката во однос на заштитата на личните податоци и го следи извршувањето на процената во согласност со членот 39 од Законот за заштита на личните податоци(*);
- соработува со Агенцијата за заштита на личните податоци;

Mbrojtjes së të Dhënave Personale(*);

- ndjek harmonizimin e veprimit me të dhënat personale në drejtori me Ligjin e Mbrojtjes së të Dhënave Personale(*) dhe me ligje të tjera relevante, të cilat i referohen mbrojtjes së të dhënave personale në Republikën e Maqedonisë së Veriut, si dhe për politikat e kontrolluesit ose përpunuesit në raport me mbrojtjen e të dhënave personale, duke përfshirë ndarjen e detyrimeve, ndërgjegjësimin dhe trajnimin e të punësuarve, të cilët marrin pjesë në operacionet e përpunimit;
- kryen kontrole për mbrojtjen e të dhënave personale;
- kryen vlerësime të rregullta të nevojës për përgatitjen dhe miratimin e akteve të reja të brendshme ose ndryshimin e akteve ekzistuese nga aspekti i harmonizimit të tyre me rregullat e mbrojtjes së të dhënave personale;
- ku është e nevojshme, jep këshilla në raport me vlerësimin e ndikimit të aktiviteteve të parapara në përpunimin në raport me mbrojtjen e të dhënave personale dhe ndjek realizimin e vlerësimit në pajtim me nenin 39 të Ligjit të Mbrojtjes së të Dhënave Personale(*);
- bashkëpunon me Agjencinë e Mbrojtjes së të Dhënave Personale;

- дејствува како контакт точка за Агенцијата за заштита на личните податоци во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација од членот 40 од Законот за заштита на личните податоци(*), како и советување според потребите за сите други прашања.

(5) При извршувањето на своите работи, офицерот за заштита на личните податоци ги зема предвид ризиците поврзани со операциите на обработката, како и природата, обемот, контекстот и целите на обработката.

(6) Лицето одговорно за информацискиот систем има одговорност во делот на обезбедување непречено и безбедно функционирање на информацискиот систем за обработка на податоците од збирките на личните податоци во Дирекцијата. Тоа лице е вработено во Дирекцијата и за својата работа одговара пред непосредниот претпоставен. Во случај на сигурносни проблеми и ризици кои се однесуваат на обработката на личните податоци, лицето одговорно за информацискиот систем го известува офицерот за заштита на личните податоци.

(7) Лицето одговорно за информацискиот систем соработува со офицерот за заштита на личните податоци при што дава предлози за ефикасно управување со ризици и унапредување на техничките и организациските мерки кои се применуваат за да обезбедат безбедност соодветна на ризикот, од пристап од страна на трети лица, и воедно учествува во изработката на анализи, извештаи и други релевантни документи со коишто се регулира обработката на личните

- Vepron si pikë kontaktuese për Agjencinë e Mbrojtjes së të Dhënave Personale në raport me çështjet lidhur me përpunimin, duke përfshirë konsultimin paraprak sipas nenit 40 të Ligjit të Mbrojtjes së të Dhënave Personale(*), si dhe këshillimin sipas nevojës për të gjitha çështjet e tjera.

(5) Gjatë realizimit të punëve të tij, oficeri i mbrojtjes së të dhënave personale, i merr parasysh rreziqet lidhur me operacionet e përpunimit, si dhe natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit.

(6) Personi përgjegjës për sistemit informativ ka përgjegjësi në pjesën e sigurimit pa pengesa dhe funksionimin e sigurve të sistemit informativ për përpunimin e të dhënave nga përmbledhja e të dhënave personale në drejtori. Ai person është i punësuar në drejtori dhe për punën e tij përgjigjet para eprorit të drejtpërdrejtë. Në rast të problemeve të sigurisë dhe rreziqeve të cilat kanë të bëjnë me përpunimin e të dhënave personale, personi përgjegjës për sistemin informativ e informon oficerin e mbrojtjes së të dhënave personale.

(7) Personi përgjegjës i sistemit informativ bashkëpunon me oficerin e mbrojtjes së të dhënave personale, ku jep edhe propozime për menaxhim efikas me rreziqet dhe avancimin e masave teknike dhe organizative të cilat zbatohen që të sigurojnë sigurinë e përshtatshme me rrezikun, nga qasja e personave të tretë, njëkohësisht merr pjesë në përpunimin e analizave, raporteve dhe dokumenteve të tjera relevante me të cilat rregullohet përpunimi i të dhënave personale në

податоци во електронска форма, вклучувајќи и изработка на процедури за постапување во случај на инциденти со коишто се нарушува доверливоста, интегритетот или достапноста на личните податоци, прегледи на применетите алатки за заштита на пристапот до информацискиот систем (примена на идентификатори или лозинки, порти на заштитниот сид (firewall) и слично).

(8) Одговорното лице за видеонадзор е вработено во Дирекцијата и за својата работа одговара пред непосредниот претпоставен. Негова одговорност е издавање корисничко име и лозинка за пристап до системот за видео надзор. Со престанок на надлежностите на лицата овластени за пристап до системот на видео надзорот (пераспоредување на друго работно место или во друга организација), одговорното лице им оневозможува пристап со бришење, односно блокирање на нивните кориснички имиња, односно лозинки.

Документација за заштита на личните податоци

Член 10

(1) Согласно оваа политика, системот за заштита на личните податоци во рамките на работењето на Дирекцијата со цел обезбедување тајност и заштита на обработката на личните податоци се состои од следните интерни акти:

- Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните

formë elektronike, duke përfshirë edhe përpunimin e procedurave për veprim në rast të incidenteve që cenojnë konfidencialitetin, integritetin ose disponueshmërinë e të dhënave personale, kontrollimin e mjeteve aplikuarra për mbrojtjen e qasjes deri te sistemi informativ (aplikimi i identifikuesve ose fjalëkalimeve, portat e murit të zjarhtë (firewall) dhe të tjerë).

(8) Personi përgjegjës për mbikëqyrjen me video është i punësuar në drejtori dhe për punën e tij përgjigjet para eprorit të drejtpërdrejtë. Përgjegjësia e tij është të krijojë një emër përdoruesi dhe fjalëkalim për qasje deri te sistemi për mbikëqyrje me video. Me ndërprerjen e kompetencave të personit të autorizuar për qasje deri te sistemi i mbikëqyrjes me video (risistemimi në vend tjetër të punës ose në organizatë tjetër), personi përgjegjës i pamundëson qasje me fshirjen, gjegjësisht bllokimin e emrit të përdoruesit dhe fjalëkalimit.

Dokumentacioni i mbrojtjes së të dhënave personale

Neni 10

(1) Në pajtim me këtë politikë, sistemi i mbrojtjes së të dhënave personale në kuadër të punës së drejtorisë, me qëllim të sigurimit të fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale, përbëhet nga aktet e brendshme që vijnë:

- Rregullore për masat teknike dhe organizative për sigurinë e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave

податоци во Дирекцијата за безбедност на класифицираните информации;

- Правилник за роковите на чување на личните податоци;
- Правилник за начинот на вршење на видеонадзор во Дирекцијата за безбедност на класифицираните информации;
- Правилник за определување на обврските и на одговорностите на администраторот на информацискиот систем и на овластените лица за обработка на лични податоци;
- Правилник 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;
- Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за начинот на повторно враќање на зачуваните лични податоци што се предмет на автоматизирана обработка;
- Правилник за начинот на превенирање и управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци;
- Преглед на збирки на лични податоци кои се обработуваат и чуваат во Дирекцијата за безбедност на класифицирани информации со рокови на нивно чување;

personale në Drejtorinë për Sigurinë e Informacioneve të Klasifikuara;

- Rregullore për afatet e ruajtjes së të dhënave personale;
- Rregullore për mënyrën e kryerjes së mbikëqyrjeve me video në Drejtorinë për Sigurinë e Informacioneve të Klasifikuara;
- Rregullore për përcaktimin e detyrimeve dhe përgjegjësitë e administratorit të sistemit informativ dhe personit të autorizuar për përpunimin e të dhënave personale;
- Rregullore për mënyrën e asgjësimit të dokumenteve të të dhënave personale pas skadimit të afatit të ruajtjes së tyre dhe për mënyrën e fshirjes, pastrimit dhe asgjësimit të mediave, që shfrytëzohen për përpunimin e të dhënave personale;
- Rregullore për mënyrën e bërjes së kopjes së sigurve, arkivimin dhe ruajtjen, si dhe për mënyrën e kthimit të të dhënave personale që janë lëndë në përpunim të automatizuar;
- Rregullore për mënyrën e parandalimit dhe menaxhimit me incidentet të cilat e cenojnë konfidencialitetin, integritetin ose disponueshmërinë e të dhënave personale;
- Kontroll të përmbledhjeve të të dhënave personale të cilat përpunohen dhe ruhen në Drejtorinë për Sigurinë e Informacioneve të Klasifikuara me afatet e ruajtjes së tyre;

- | | |
|--|---|
| <ul style="list-style-type: none"> - Политика за креирање и употреба на лозинки за администратори. - Политика за користење на преносливи уреди и работа од далечина (teleworking); - Политика за чист екран и чисто биро; - Процедура за копирање и умножување документи што содржат лични податоци; - План и насоки за создавање систем за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци; - Анализа на ризиците на активностите за обработка на личните податоци и начинот на управување со ризици. | <ul style="list-style-type: none"> - Politikë të krijimit dhe përdorimit të fjalëkalimeve të administratorëve; - Politikë të shfrytëzimit të pajisjeve portative dhe punës në distancë (teleworking); - Politikë për ekran dhe tavolinë të pastër; - Procedurë për kopjimin dhe shumëfishimin e dokumenteve të cilat përfshijnë të dhëna personale; - Plan dhe drejtime për krijimin e sistemit të masave teknike dhe organizative për sigurinë e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale; - Analizë të rreziqeve të aktiviteteve për përpunimin e të dhënave personale dhe mënyrën e menaxhimit të tyre. |
|--|---|

Периодични контроли

Kontrollet periodike

Член 11

Neni 11

(1) Офицерот за заштита на личните податоци во Дирекцијата најмалку еднаш годишно ги врши следните контроли:

- контрола на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци;
- контрола на евиденцијата на секој авторизиран/неавторизиран пристап до информацискиот систем на Дирекцијата;

(1) Oficeri i mbrojtjes së të dhënave personale në drejtori, së paku një herë në vit i kryen kontrollet në vijim:

- kontrollimin e masave teknike dhe organizative për sigurinë e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale;
- kontrollimin e evidencës së çdo qasjeje të autorizuar/ të paautorizuar te sistemi informativ i drejtorisë;

- контрола на доверливоста и сигурноста на лозинките и на останатите форми на идентификација;
- контрола на уништување на документи коишто содржат лични податоци по истекот на рокот на чување, како и начинот на уништување, бришење и чистење на медиумите и управување со нив;
- контрола на примена на правилото „чисто биро“;
- контрола на писмените овластувања за работа со лични податоци издадени од директорот на Дирекцијата;
- контрола на воспоставениот начин на физичката сигурност на работните простории и опремата на Дирекцијата каде што се обработуваат личните податоци;
- контрола на начинот на пристап до целиот информациски систем преку персоналните компјутери;
- контрола на начинот на правење сигурносни копии, архивирање и чување, како и повторно враќање на зачуваните лични податоци;
- контрола на начинот на физички пристап до просторијата во која се сместени серверите;
- контрола на постапката за потпишување на изјави за тајност и заштита на личните податоци од страна на вработените и ангажираните лица во Дирекцијата.
- kontrollimin e konfidencialitetit dhe sigurisë së fjalëkalimeve dhe të formave të tjera të identifikimit;
- kontrollimin e asgjësimit të dokumenteve të cilat përfshijnë të dhënat personale pas skadimit të afatit të ruajtjes, si dhe mënyrën e asgjësimit, fshirjes dhe pastrimit të mediave dhe menaxhimin e tyre;
- kontrollimin e zbatimit të rregullit “tavolinë e pastër”;
- kontrollimin e autorizimeve me shkrim për punë me të dhënat personale, të lëshuara nga drejtori i drejtorisë;
- kontrollimin e mënyrës së vendosur të sigurisë fizike të hapësirave të punës dhe pajisjeve të drejtorisë, ku përpunohen të dhënat personale;
- kontrollimin e mënyrës së qasjes deri te sistemi i plotë informativ, nëpërmjet kompjuterëve personalë;
- kontrollimin e mënyrës së bërjes së kopjeve të sigurta, arkivimin dhe ruajtjen, si dhe kthimin e të dhënave personale të ruajtura;
- kontrollimin e mënyrës së qasjes fizike deri te hapësirat, ku janë të vendosur serverët;
- kontrollimin e procedurës për nënshkrimin e deklaratave për fshehtësinë dhe mbrojtjen e të dhënave personale nga ana e të punësuarve dhe personave të angazhuar në drejtori.

Соработка со Агенцијата за заштита на личните податоци и известувања при

Bashkëpunimi me Agjencinë e Mbrojtjes së të Dhënave Personale dhe

**нарушување на безбедноста на
личните податоци**

**njoftimin gjatë cenimit të sigurisë së
të dhënave personale**

Член 12

Neni 12

(1) Дирекцијата во улога на контролор мора да ја чува документацијата и евиденцијата за обработка на лични податоци во хартиена или електронска форма и да ја направи достапна на барање на Агенцијата за заштита на личните податоци.

(2) Во случај да настане нарушување на безбедноста на личните податоци, а согласно членовите 37 и 38 од Законот за заштита на личните податоци(*), контролорот има обврска да ја извести Агенцијата за заштита на личните податоци, а во одредени ситуации и засегнатите субјекти на личните податоци.

(3) Доколку контролорот врши обработка на личните податоци со визок ризик за правата и слободите на физичките лица, задолжително мора да ја извести Агенцијата за заштита на личните податоци.

Примена и ревизија на политиката

(1) Drejtoria në rolin e kontrolluesit duhet ta ruajë dokumentacionin dhe evidencën e përpunimit të të dhënave personale në formë elektronike dhe të shkruar, dhe ta bëjë të qasshme në kërkesat e Agjencisë së Mbrojtjes së të Dhënave Personale.

(2) Në rast të cenimit të sigurisë së të dhënave personale, në pajtim me nenet 37 dhe 38 të Ligjit të Mbrojtjes së të Dhënave Personale(*), kontrolluesi ka për detyrë ta njoftojë Agjencinë e Mbrojtjes së të Dhënave Personale, si dhe në situata të caktuara edhe subjektet e prekura të të dhënave personale.

(3) Nëse kontrolluesi kryen përpunimin e të dhënave personale me rrezik të lartë për të drejtat dhe liritë e personave fizik, domosdoshmërisht duhet ta njoftojë Agjencinë e Mbrojtjes së të Dhënave Personale.

Zbatimi dhe revizioni i politikës

Член 13

Neni 13

(1) Оваа политика почнува да се применува од денот на нејзиното донесување и истата се објавува на веб-страницата на Дирекцијата.

(2) Оваа политика ќе се ревидира во случај на промена на основот на којшто е донесена и по потреба за изменување и дополнување на системот за заштита на личните податоци што се обработуваат во Дирекцијата.

(1) Kjo politikë fillon të zbatohet nga dita e miratimit të saj dhe e njëjta publikohet në ueb-faqen e drejtorisë.

(2) Kjo politikë do të rishikohet në rast të ndryshimit të bazës mbi të cilën është miratuar dhe sipas nevojës për ndryshimin dhe plotësimin e sistemit të mbrojtjes së të dhënave personale që përpunohen në drejtori.

Директор/ Drejtori

Стојан Славески