Република Северна Македонија
Дирекција за безбедност
на класифицирани информации
Бр. 02- 1039/1
Скопје, 30 11 2021 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

ПОЛИТИКА ЗА ВОСПОСТАВУВАЊЕ СИСТЕМ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Цел и опсег

Член 1

Со политиката за воспоставување систем за заштита на личните податоци 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).

Принципи при обработка на личните податоци

Член 2

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

- 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.

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

Член 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 сé 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, 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-страната, 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 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 проценатa на ризик, а најмалку еднаш неделно и слично).

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

Збирки на лични податоци кои се обработуваат и чуваат во Дирекцијата

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;
- 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.

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-барателиа 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 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 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-барателиа 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 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.

Цели на обработката на личните податоци

Член 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.

(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:

- 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;
- уредување на односите меѓу раководниот кадар и вработените и на односите меѓу вработените;

- анализа на човечките ресурси (работната сила);
- управување со податоците на персоналот – работната сила.

(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 Дирекцијата[1] 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]

(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 досиеа 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“.

(6) Личните податоци од 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 обработуваат со цел ефикасно обезбедување на бараната услуга, исполнување на законската обврска за организирање и

---

[1] Закон за класифицирани информации(*) („Службен весник на РСМ“ бр. 275/19), член 39

[2] Исто, член 64.

[3] Правилник за формата и содржината на обрасците на безбедносниот прашалник и на безбедносните сертификати („Службен весник на РСМ“, бр. 123/20)

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

(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 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.

---

[4] Закон за класифицирани информации(*), член 69, став 2, алинеа 10.

(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 сé уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, Дирекцијата ги архивира на безбеден начин, особено ако архивираните 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.

Копирање, умножување и уништување на документите

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

Одговорни лица за заштита на личните податоци

Член 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 Дирекицијата, 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 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 проценатa на влијанието на предвидените активности на обработката во однос на заштитата на личните податоци и го следи извршувањето на проценатa во согласност со членот 39 од Законот за заштита на личните податоци(*);
- соработува со Агенцијата за заштита на личните податоци;
- 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 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 ѕид (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 (прераспоредување 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 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;
- 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.

Периодични контроли

Член 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;
- 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.

Соработка со Агенцијата за заштита на личните податоци и известувања при нарушување на безбедноста на личните податоци

Член 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

Член 13

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

Директор,

Стојан Славески