Република Северна Македонија
Дирекција за безбедност
на класифицирани информации
Бр. 02- 1039/2
Скопје, 30 11 2024 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

ПРАВИЛНИК
ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ДИРЕКЦИЈАТА ЗА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

I. Општи одредби

Член 1

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

Член 2

Одредбите од овој правилник се применуваат за:

- целосна или делумна автоматизирана обработка на личните податоци и
- рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Член 3

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

Технички и организациски мерки

Член 4

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

(2) Техничките и организациските мерки од ставот (1) на овој член се применуваат пропорционално на активностите за обработка на личните податоци и се класифицирани во две нивоа:

- стандардно ниво и
- високо ниво.

Член 5

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

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

СТАНДАРДНО НИВО

1. Технички мерки

Член 6

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

1. единствено корисничко име и лозинка за секое овластено лице;
2. лозинка составена од комбинација од осум алфанумерички карактери – букви (мали и големи) и специјални знаци;
3. корисничко име и лозинка кое овозможува пристап на овластеното лице до информацискиот систем во целина, пристап до поединечни апликации

и/или поединечни збирки на личните податоци потребни при извршување на работните задачи;

4. најава во информацискиот систем во којшто се обработуваат, чуваат и управуваат податоците преку воспоставените системи преку квалификуван дигитален сертификат и единствено корисничко име и лозинка за секое овластено лице на дигиталниот сертификат;
5. евиденција за овластените лица кои имаат авторизиран пристап до документите и информацискиот систем и постапки за идентификација и проверка на авторизираниот пристап;
6. правила на доверливост и интегритет при пријавување, доделување и чување на лозинки и автоматско менување по изминат период од три месеци;
7. автоматизирано одјавување од информацискиот систем по изминување на одреден период на неактивност (не подолг од 15 минути) и за повторно активирање на системот со одново внесување на корисничкото име и лозинката;
8. автоматизирано отфрлање на информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничко име и лозинка) и автоматизирано известување на корисникот дека треба да побара упатство од администраторот на системот;
9. инсталирана хардверска/софтверска заштитна мрежна бариера (firewall) или рутер помеѓу информацискиот систем и интернет или која било друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;
10. ефективна и сигурна антивирусна заштита и антиспајвер заштита на информацискиот систем која постојано ќе се ажурира заради превентивна заштита од непознати и непланирани закани од нови вируси и шпионски софтвери (spyware);
11. ефективна и сигурна антиспам заштита која постојано ќе се ажурира заради превентивна заштита од спамови;
12. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување (UPS уред);
13. обезбедување на веб-страната на Дирекцијата со примена на технички мерки со кои се гарантира идентитетот на страната и интегритетот и доверливоста на информациите на страната;
14. редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;
15. зачувување на податоците на корисниците на серверите на Дирекцијата за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително користење на мерки за синхронизација или резервни дополнителни мерки за заштита врз основа на анализа на ризикот;

16. ограничување на опцијата за приклучување на преносливите медиуми (USB, DVD, CD, надворешни хард дискови и слично) кон системите со примарна важност;
17. исклучен автоматски режим на работа на преносливите медиуми (Disable Autorun for Removable Media);
18. алатките за далечинска администрација мора да бидат нагодени на начин што претходно задолжително треба да обезбедат согласност од овластеното лице од Дирекцијата на работната станица на корисникот пред каква било интервенција на самата работна станица;
19. нагодување на информацискиот систем кое ќе обезбеди овластеното лице од Дирекцијата да врши далечинска администрација на работната станица на корисникот, како и приказ за тоа кога истата завршила (на пр. со прикажување на порака на екранот дека далечинската администрација завршила);
20. забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;
21. ограничување на употребата на софтверски програми што бараат администраторски права;
22. бришење на податоците што се наоѓаат на работна станица која треба да се предаде;
23. ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;
24. инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно;
25. подигнување на нивото на свесност во однос на тоа, на што овластените лица треба да се посветат и податоци за контакт на лицата што треба да ги контактираат во случај на инцидент или појава на необичен настан што влијае на информациите и комуникацијата на системите на Дирекцијата.

Обезбедување на преносливите медиуми

Член 7

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

- подигање на свеста на овластените лица за специфичните ризици поврзани со користење на преносливите медиуми и преземање мерки за намалување на ризици и
- употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на постојните услови и безбедносни гаранции.

Заштита на внатрешната мрежа

Член 8

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

- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси;
- во случај на далечински пристап, задолжително воспоставување на VPN конекција со задолжителна автентикација на овластеното лице;
- обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително да се изврши преку VPN) и
- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен ѕид (firewall) и прокси сервери.

Обезбедување на серверите

Член 9

(1) Примената на техничките мерки за серверите на Дирекцијата на кои се централизира обработката на личните податоци задолжително опфаќа:

- пристап до алатките и административните панели на серверите само за овластените лица од страна на директорот на Дирекцијата;
- примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);
- приемена на посебна политика за креирање и употреба на лозинките за администраторите на информацискиот систем;
- инсталирање на сите важни ажурирања (updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (auto update) и
- правење сигурносни копии (backup) и нивна редовна проверка.

(2) Во случај кога се врши администрирање на базите на податоци, се применуваат следните мерки:

- употреба на персонализирани профили за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација и
- заштита од напади преку инјектирање на SQL код (компјутерски јазик за комуникација со базата на податоци), скрипти и слично.

Обезбедување на веб-страната на Дирекцијата

Член 10

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

- имплементација на криптографски протокол за сите страници на веб-страната, вклучително и на формуларите за собирање лични податоци или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавно достапни;
- ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации и
- пристап до алатките и административните интерфејси можат да имаат само овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни.

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

- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пр. идентификатори или лозинка);
- користење на небезбедни услуги;
- употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страни, пристап до електронска пошта и слично;
- поставување на базите на податоци на сервери кои се директно достапни преку интернет и
- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

Администратор на информациски систем

Член 11

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

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

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

(4) Офицерот за безбедност на личните податоци задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изготвува извештај за извршената контрола. Во него треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

Обврските и одговорности на овластените лица

Член 12

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

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

Идентификација и проверка

Член 13

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

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

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

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

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

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

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

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

Контрола на пристап

Член 14

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

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

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

Превенирање, реакција и санирање на инциденти (обезбедување континуитет)

Член 15

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

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

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

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

Член 16

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

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

Управување со медиуми

Член 17

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

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

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

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

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

Физичка безбедност на информацискиот систем

Член 18

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

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

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

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

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

Контрола на информацискиот систем и на комуникациско-информациската опрема

Член 19

(1) Офицерот за заштита на личните податоци врши периодични контроли заради следење на усогласеноста на работењето на Дирекцијата со прописите за

заштита на личните податоци и со донесената документација за технички и организациски мерки.

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

Управување со обработувачи

Член 20

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

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

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

- дали и како се врши криптирање на податоците според нивната чувствителност;
- дали и како се врши криптирање на преносот на податоци;
- постоење на процедури што гарантираат дека никој нема да има неовластен пристап до податоците;
- гаранции во однос на следење на пристапот до информацискиот систем (логови);
- управување со правата на пристап;
- автентикација и
- други мерки за безбедност на обработката на личните податоци.

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

- предметот, должината и целта на обработката на личните податоци;
- обврските за обработувачот во однос на преземање на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци;
- обврските во однос на тајноста на доверените лични податоци;
- минималните стандарди за автентикација на овластените лица;

- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;
- правилата за известување на Дирекцијата и управување со инциденти во случај на нарушување на безбедноста на личните податоци;
- обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на Дирекцијата и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

2. Организациски мерки

Член 21

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

- ограничен пристап или идентификација за пристап до личните податоци;
- уништување на документи по истекот на рокот за нивно чување;
- мерки за физичка сигурност на работните простории и на комуниникациско-информацискатa опрема на која се обработуваат личните податоци;
- почитување на техничките упатства при инсталирање и користење комуниникациско-информациска опрема на која се обработуваат личните податоци.

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

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

Информирање и едуцирање за заштитата на личните податоци

Член 22

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

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

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

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

(5) Изјавата од ставот (4) на овој член особено го содржи следното:

- дека лицето ќе ги почитува начелата за заштита на личните податоци пред нивниот пристап до личните податоци;
- ќе врши обработка на личните податоци согласно упатствата добиени од Дирекцијата, освен ако со закон поинаку не е уредено;
- личните податоци ќе ги чуваат како доверливи и
- ќе ги применуваат пропишаните мерки за заштита на личните податоци.

(6) Изјавата од ставот (4) на овој член задолжително се чува во досието на лицето коешто се вработува или се ангажира во Дирекцијата.

(7) Дирекцијата врши континуирано информирање и едуцирање на раководството и на овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Пристап до документите

Член 23

(1) Пристапот до документите треба да биде ограничен само за овластени лица во Дирекцијата.

(2) За пристапување до документите се врши идентификација на овластените лица и за категориите на личните податоци до кои се пристапува се води евиденција на пристапи.

(3) Пристапувањето на неовластените лица до документи треба да биде во придружба на лице кое е овластено за пристапување до документите.

Правило „чисто биро“

Член 24

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

Чување на документи

Член 25

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

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

Уништување на документи

Член 26

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

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

ВИСОКО НИВО

1. Технички мерки

Управување со лозинки

Член 27

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

Управување со преносливи медиуми

Член 28

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

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

Тестирање на информацискиот систем

Член 29

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

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

Пренесување на медиуми

Член 30

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

Пренесување на личните податоци преку мрежа за електронски комуникации

Член 31

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

2. Организациски мерки

Копирање и умножување на документите

Член 32

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

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

Пренесување на документите

Член 33

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

Влегување во сила

Член 34

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

Директор,
Стојан Славески