Врз основа на член 20 од Статутот на Јавното претпријатие за државни патишта, 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 294/21) и член 47 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Управниот одбор на седницата одржана на ден 10.10.2023 донесе

ПРАВИЛНИК

ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЈАВНОТО ПРЕТПРИЈАТИЕ ЗА ДРЖАВНИ ПАТИШТА

Член 1

Со овој Правилник се пропишуваат техничките и организациските мерки кои ги применува Јавното претпријатие за државни патишта (во натамошниот текст ЈПДП) во својство на контролор заради обезбедување безбедност и заштита на обработка на личните податоци .

Член 2

ЈПДП ја евидентира и ја чува целокупната документација за софтверските програми за обработка на личните податоци и за сите негови промени.

Член 3

Одредбите од овој Правилник се применуваат за:
-целосно и делумно автоматизирана обработка на личните податоци и
-друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на личните податоци.

Член 4

(1) ЈПДП 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 ризиците при нивната обработка.

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

Член 5

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

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

Член 6

Податоците кои содржат ЕМБГ задолжително се применуваат техничките и организациските мерки класифицирани на стандардно и високо ниво.

СТАНДАРДНО НИВО

Технички мерки

Член 7

ЈПДП 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 која 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. најавата во информацискиот систем во кој 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. правилата на доверливост и интегритет при пријавување, доделување и чување на лозинки, и автоматско менување по изминат период од три месеци;
7. криптирање на личните податоци;

8. автоматизирано одјавување од инфомацискиот систем по изминување на одреден период на неактивност (не подолг од 15 минути) и за повторно активирање на системот потребно е одново внесување на корисничкото име и лозинката;
9. автоматизирано отфрлање на информацискиот систем после три неуспешни обиди за најавување (внесување на погрешно корисничо име и лозинка) и автоматизирано известување на корисникот дека треба да побара упатство од администраторот на системот;
10. инсталирана хардверска/софтверска заштитна мрежна бариера („фајервол") или рутер помеѓу информацискиот систем и интернет или било која друга форма на надворешна мрежа, како заштитна мерка против недозволени или злонамерни обиди за влез или пробивање на системот;
11. ефективна и сигурна анти-вирусна и анти-спајвер заштита на инфомацискиот систем, која постојано ќе се ажурира заради превентивна од непознати и непланирани закани од нови вируси и спајвери;
12. ефективна и сигурна анти-спам заштита, која постојано ќе се ажурира заради превентивна заштита од спамови;
13. приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преу уред за непрекинато напојување;
14. обезбедување на веб-страницата на ЈПДП со примена на технички мерки со кои го гарантира точниот идентитет на страницата, како и доверливоста на информациите на страницата;
15. редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;
16. зачувување на податоците на корисниците на серверите на контролорот за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително со мерки за синхронизација или со резервни дополнителни мерки за заштита врз основа на анализа на ризикот;
17. ограничување на опцијата за приклучување на преносливите медиуми (УСБ, надворешни хард дискови и сл.) кон системите со примарна важност;
18. исклучен автоматски режим на работа за преносливите медиуми (Disable autorun for removable media);
19. алатките за далечинска администрација мора да бидат нагодени на начин што претходно задолжително треба да обезбедат согласност од овластеното лице од ЈПДП на работната станица на корисникот пред каква било интервенција на самата работна станица;
20. нагодување на информацискиот систем кое ќе обезбеди дека овластеното лице од ЈПДП врши далечинска администрација на работната станица на корисникот, како и за тоа кога истата завршила (на пример со прикажување на порака на екранот дека далечинската администрација завршила);

21. забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;
22. ограничување на употребата на софтверски програми што бараат администраторски права;
23. бришење на податоците што се наоѓаат на работна станица која треба да се предаде;
24. ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;
25. инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно; и
26. 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 контролорот.

Обезбедување на преносливите медиуми

Член 8

(1) ЈПДП 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 применува соодветни технички мерки и тоа:

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

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

Заштита на внатрешната мрежа

Член 9

(1) ЈПДП обезбедува заштита на својата внатрешна мрежа преку овозможување само на неопходните мрежни функции потребни за обработка на личните податоци, а особено преку:

- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (VoIP, peer to peer, итн.);
- управување со Wi-Fi мрежата кое опфаќа користење на најсовремените методи на криптирање (WPA2 или WPA2-PSK и со употреба на комплексна лозинка која на определен временски период се менува);

- во случај на далечински пристап, задолжително воспоставување на VPN конекција, со задолжителна автентикација на овластеното лице со употреба наквалификуван дигитален сертификат;
- 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 и прокси сервери.

Обезбедување на серверите

Член 10

(1) Примената на технички и организациски мерки за серверите на ЈПДП на кои се централизира обработката на голема количина на лични податоци, задолжителоно опфаќа:
- пристап до алатките и административни панели на серверите може да имаат единствено овластените лица од страна на директорот
- примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);
- примена 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);
- правење на сигурносни копии и нивна редовна проверка; и
--примена на TLS протокол (со замена на SSL13) или друг протокол што обезбедува шифрирање и автентикација, како минимум за каква било размена на податоци преку интернет и потврда на нејзината соодветна примена преку соодветни алатки.
(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 (specific account for each application); и
- примена на мерки против напади преку инјектирање на SQL код, скрипти и слично.

Обезбедување на веб-страниците на контролорот

Член 11

(1) За веб-страница на ЈПДП се применуваат технички мерки со кои се гарантира точниот идентитет на страницата (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа особено преку следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници, користејќи ја единствено најновата верзија и со проверка на неговата правилна имплементација;
- задолжителна употреба на криптографски протокол (TLS) за сите страници од вебстраницата, вклучително и формулари 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. Ако веб серверот прифаќа само врски со HTTPS протокол, само IP мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти мора да бидат блокирани;
- пристап до алатките и административните интерфејси, можат да имаат овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни; и
- ако се користат колачиња што не се потребни од услугата, се обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;

(2) Не треба да применува 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 пример идентификатори или лозинки);
- користење на небезбедни услуги;
- употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораки 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.

Администраторот на информацискиот систем и на овластените лица

Член 12

(1) Систем администратор е стручно лице од информатичко-комуникациска област, вработено во ЈПДП, 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 податоците.
(2) Информацискиот систем на ЈПДП е целокупниот систем составен од персонални компјутери, сервери и комуникациска опрема, опрема за обезбедување сигурност на податоците, базата на податоци, апликацискиот и останатите апликации и опрема кои се користат за обработка на податоци.
(3) Обврските и одговорностите на администраторот на информацискиот систем е дефиниран и утврден во Правила за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.
(4) Офицерот за заштита на личните податоци задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изготвува извештај за извршената контрола.
(5) Во извештајот треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности.

Обврски и одговорности на овластените лица

Член 13

(1) Обврските и одговорностите на секое овластено лице кое има пристап до личните податоци и до информацискиот систем, ЈПДП ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица.
(2) ЈПДП задолжително ги информира овластение лица од ставот (1) на овој член со документацијата за технички и организациски мерки кои се однесуваат на извршувањето на нивните обврски и одговорности.

Идентификација и проверка

Член 14

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

(2) Кога проверката се врши врз основа на корисничко име и лозинка, ЈПДП секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите.
(3) Лозинките треба автоматски да се менуваат по изминат временски период што не може да биде подолг од три месеци.
(4) Со цел да обезбеди идентификување на секој неовластен (измамнички) пристап или злоупотреба на лични податоци, како и да се утврди потеклото на овие инциденти, ЈПДП воспоставува и води евиденција за секој пристап до информацискиот систем – logs (од оперативните системи, од заштитниот ѕид (firewall), серверот дизајниран специјално за употреба како сервер за датотеки (file server), базите на податоци, системот (софтверот) за управување со документи (DMS System);
(5) Офицерот за заштита на личните податоци назначен во Одделението за ИКТ и/или од друго овластено лице од контролорот кое ги има потребните знаења и вештини, но нема администраторски привилегии, врши контрола на евидентирање на податоците од ставовите (2) и (3) на овој најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности
(6) Евиденцијата од ставот (1) на овој член се чува најмалку пет години.
(7)Овластените лица за управување со системот за евиденција за пристап до информацискиот систем го известуваат раководството раководителот на одделението за ИКТ и директорот за која било аномалија или безбедносен инцидент, веднаш, а најдоцна во рок од 12 часа од моментот на инцидентот.
(8)Раководителот на одделението ИКТ или овластеното лице за управување со системот на евиденција ја известува Агенцијата за заштита на личните податоци за секое нарушување на безбедноста на личните податоци, а доколку постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, и субјектите на личните податоци за да можат да ги ограничат последиците од нарушувањето на безбедноста.

Контрола на пристап

Член 15

(1)Овластените лица задолжително имаат авторизиран пристап само до личните податоци и информатичко-комуникациска опрема кои се неопходни за извршување на нивните работни задачи.
(2) ЈПДП воспоставува механизми за да се оневозможи пристап на овластени лица до личните податоци и информатичко-комуникациска опрема со права различни од тие кои се авторизирани.

(3)Администраторот на информацискиот систем кој е овластен согласно Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица, може да доделува, менува или да го одзема авторизираниот пристап до личните податоци и информатичко-комуникациската опрема само врз основа на налог дадена од страна на директорот на ЈПДП и во согласност со критериуми кои се утврдени од страна на ЈПДП.

Превенирање, реакција и санирање на инциденти

(обезбедување континуитет)

Член 16

(1) ЈПДП изготвува Правила за превенирање, реакција и санирање на инциденти на својот информациски систем и список на овластените лица кои се одговорни за превенирање, како и за навремено повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на настанат физички или технички инцидент.

(2) ЈПДП ги определува постапките кои се применуваат за повторно враќање на личните податоци и начинот на евидентирање на овластените лица од ставот (1) на овој член, кои ги извршиле операциите за повторно враќање на личните податоци, категориите на личните податоци кои се вратени или кои биле рачно внесени при враќањето.

(3) Превенирањето на инцидентите ги опфаќа сите мерки и контроли утврдени со овој правилник, а врз основа на спроведената анализа на ризик опфаќа (користење на непрекинато напојување за да се заштити опремата што се користи за обработка на личните податоци, едновремена употреба на повеќе уреди во низа за зачувување на личните податоци /RAID технологија/, редовно тестирање на функционалноста на уредите и слично).

Сигурносни копии и повторно враќање на зачуваните лични податоци (обезбедување континуитет)

Член 17

(1) ЈПДП врз основа на анализата на ризикот прави сигурносни копии на личните податоци на редовни временски интервали, со цел да го намали ефектот во случај на нивно непосакувано губење или оштетување.

(2) Сигурносните копии од ставот (1) на овој член треба да се прават и тестираат редовно, за што се усвојува План за обезбедување континуитет (business continuity plan) кој ги предвидува сите можни инциденти (на пример: хардверски инцидент).

(3) ЈПДП прави фрагментирана (incremental back-up), односно поединечна копија на дневна основа во однос на сите настанати промени во текот на денот, а целосна сигурносна копија (full back-up) во редовни временски интервали по негова оценка, а најмалку еднаш месечно, на начин кој ќе гарантира повторно воспоставување на достапноста до личните податоци во случај на настанат физички или технички инцидент.
(4) ЈПДП задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци.
(5) Сигурносните копии се чуваат надвор од просториjата во која се наоѓаат серверите и се физички и криптографски заштитени, заради оневозможување на каква било модификација.
(6) Во однос на сигурносните копии се применува истото безбедносно ниво на технички и организациски мерки како и за податоците кои се зачувани на оперативните сервери на кои врши обработка на личните податоци со криптирање на сигурносните копии, со чување на безбедно место на сигурносната копија за кое се применети мерки и контроли кои го минимизираат ризикот од поплава, пожар, кражба и слично, или во случај на договорно регулирање и аутсорсирање на услугата, соодветна заштита која треба да ја примени и обработувачот.

Начин на архивирање и чување на податоците

Член 18

(1) ЈПДП, во однос на личните податоци за кои се уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, врши архивирање на безбеден начин, особено ако архивираните податоци се чувствителни податоци (посебни категории на лични податоци), или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци, доколку бидат компромитирани.
(2) ЈПДП ја пропишува постапката за управување со архивскиот материјал во однос на тоа кои податоци треба да се архивираат, како и каде се чуваат и кој, како и под кои услови има пристап до нив.
(3) ЈПДП изготвува „Список (преглед) со рокови на чување на личните податоци" во кој се содржани информации за моментот на активирање на периодот (рокот) за чување на личните податоци, идентификуваните периоди (рокови) за чување на личните податоци, причините за чување на личните податоци, законскиот основ за чување на личните податоци и сопственикот на податоците, кој се ревидира и усогласува годишно согласно промените во работењето и законските услови за чување на личните податоци.

Управување со медиуми

Член 19

(1) ЈПДП 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 и време на примање, испраќач, број на медиуми кои се примени, видот на документот кој е снимен на медиумот, начин на испраќање на медиумот, име и презиме на лицето овластено за прием на медиумот.
(2)Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на ЈПДП.
(3) Преносливите медиуми на кои се врши обработка на личните податоци треба да се чуваат на локација до која пристап имаат само овластените лица утврдени со овој Правилник.
(4)Пренесувањето на медиумите надвор од работните простории се врши само со претходно овластување од страна на директорот на ЈПДП.
(5)За пренесените медиуми надвор од работните простории на ЈПДП, се преземаат непходни мерки за да се спречи неовластено обработување на лични податоци снимени на нив. Медиумите можат да се пренесуваат надвор од работните простории ако личните податоци се криптирани или ако се заштитени со соодветно методи кои гарантираат дека податоците нема да бидат читливи, при што само администраторот на информацискиот систем може да ги декриптира или лице овластено од него.
(6)По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.
(7)Уништувањето на медиумот се врши со механичко разделување на неговите составни делови при што истиот да не може да биде употреблив .
(8)Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.
(9)За случаите од ставовите (7) и (8) на овој член се обезбедува информациска трага (на пример: записник), која ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци кои биле снимени на истиот.

Криптирање на личните податоци

Член 20

(1) Личните податоци можат да се пренесуваат преку елетронско-комуникациската мрежа само ако се криптирани или ако се посебно заштитени со соодветни методи кои гарантираат дека податоците нема да бидат читливи при преносот.
(2)Криптирање на личните податоци, се врши со примена на најсовремени технички решенија за криптирање со кои го обезбедува интегритетот, доверливоста и автентичноста на личните податоци и тоа: да се наведат од подолу наведените

ЈПДП ги променува SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC користејќи SHA-256, bcrypt, scrypt или PBKDF2 за чување лозинки, AES или AES-CBC за симетрично криптирање, RSA-OAEP v2.1 за асиметрично криптирање...), безбедни алгоритми за криптирање а воедно обезбедува заштита на тајните клучеви за криптирање со ограничувачки права за пристап и посебно креирана безбедна лозинка за пристап.

(3) ЈПДП донесува внатрешна процедура во која задолжително се пропишува начинот на управување со тајните клучеви и сертификати, земајќи го предвид и управувањето со ризикот на заборавени лозинки.

Физичка безбедност на информацискит систем

Член 21

(1)Серверите на кои се инсталирани софтверските програми за обработка на личните податоци, се физички лоцирани, хостирани и администрирани од страна на ЈПДП.
(2) ЈПДП обезбедува зајакнато ниво на безбедност во однос на просториите во кои се сместени и се чуваат серверите и мрежната опрема преку кои се врши обработка на личните податоци и тоа:
-Физички пристап до просторија во која се сместени серверите имаат само лица посебно овластени од директорот на ЈПДП.
-Просторијата во која се сместени серверите се заштитаува од ризиците преку примена на мерки и контроли за превенција 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 зачувани на серверите, тогаш тоа лице ќе биде придружувано и надгледувано од лицето овластено од директорот на ЈПДП.
- ажуриран список на лица или категории на лица кои се овластени да влезат во просториите каде се чува опрема на која се врши обработка на личните податоци;
- одржување на просториите за серверите (климатизација, UPS, итн.).
- водење на евиденција за пристап до просториите каде што се чуваат серверите кои содржат лични податоци;
(2) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот.
(3) Во случајот од ставот (2) на овој член, меѓусебните права и обврски на ЈПДП и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, се уредуваат со договор во писмена форма, кој

задолжително ќе содржи мерки за безбедност на личните податоци согласно прописите за заштита на личните податоци.

Контрола на информацискиот систем и информатичката инфраструктура

Член 22

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

(2) Информацискиот систем и информатичката инфраструктура на ЈПДП задолжително подлежат на годишна внатрешна контрола со цел да се провери дали постапките и упатствата содржани во (техничките и организациските мерки кои се применуваат) правилата и политиките за безбедност на личните податоци се применуваат и се во согласност со прописите за заштита на личните податоци.

Управување со обработувачи

Член 23

(1) ЈПДП обезбедува заштита на лични податоци во елеткронска форма при нивната размена кон надворешните субјекти, преку безбедносни системи со овозможување на криптирана врска за размена на строги правила за идентификација при размена.

(2) Меѓусебните права и обврски на ЈПДП и обработувачот мора да бидат уредени со договор при што ЈПДП пред да го склучи договорот е должно да побара од обработувачот (давател на услугата), да му ја презентира својата безбедносна политика во однос информацискиот систем и информатичкта инфраструктура на која ќе се врши обработката на личните податоци во име на контролорот.

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

- дали и како се врши криптирање на податоците според нивната чувствителност;
- постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;
- дали и како се врши криптирање на преносот на податоци;
- гаранции во однос на следливост (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 да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци;
- обврските во однос на доверливоста 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 управување и известување на контролорот во случај на инциденти,односно во случај на нарушување на безбедноста на личните податоци;
-обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на контролорот; 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 24

(1) ЈПДП применува соодетни организациски мерки за тајност и заштита на личните податоци и тоа:
1.ограничен пристап или идентификација за пристап до личните податоци;
2. уништување на документи по истекот на рокот за нивно чување;
3.мерки за физичка сигурност на работните простории и на информатичко комуникациска опрема на која се обработуваат личните податоци;
4.почитување на техничките упатства при инсталирање и користење на информатичко – комуникациската опрема на која се обработуваат личните податоци.
(2) Вработеното лице во организационата единица за човечки ресурси во ЈПДП, 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 било кои 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 25

(1) Лицата кои се вработуваат или се ангажираат во ЈПДП, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.
(2) За лицата кои се ангажираат за извршување на работа во ЈПДП во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.
(3) Пред непосредното започнување со работа на овластените лица, раководно лице од Одделението за управување со човечки ресурси дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.
(4) Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.
(5) Изјавата од ставот (4) на овој член особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.
(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.
(7) ЈПДП задолжително врши континуирано информирање и едуцирање на раководството и овластените лица за непосредните обврски и одговорности за заштита на личните податоци.

Пристап до документите

Член 26

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

Правило „чисто биро“

Член 27

ЈПДП 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 28

Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

Уништување на документи

Член 29

(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.
(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.

Начин на чување на документите

Член 30

Плакарите (орманите), 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 овластените лица.

ВИСОКО НИВО

1. Технички мерки

Управување со лозинки

Член 31

ЈПДП користи обезбедува дека различните лозинки за секоја услуга, или софтверска програма соодветно се чуваат, при што пропишува Политика за управување со лозинки.

Управување со преносливи медиуми

Член 32

(1) ЈПДП воспоставува систем за евидентирање на медиумите кои се примаат со цел да овозможи директна или индиректна идентификација на видот на медиумот кој е примен, датум и време на примање, испраќач, број на медиуми кои се примени, вид на документ кој 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 контролорот, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.

Тестирање на информацискиот систем

Член 33

(1) ЈПДП задолжително врши тестирање на информацискиот систем пред неговото 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 став (1) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци.

Пренесување на медиуми

Член 34

Медиумите можат да се пренесуваат надвор од работните простории 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 може да ги декриптира или лице овластено од него.

Пренесување на личните податоци преку мрежа за електронски комуникации

Член 35

Личните податоци можат да се пренесуваат преку мрежата 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 36

(1) Копирањето или умножувањето на документите може да се врши единствено од страна на овластени лица определени со претходно писмено овластување од страна на директорот на ЈПДП и согласно процедурите во која задолжително се утврдуваат мерките и начинот на копирањето и умножувањето на документите.

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

Пренесување на документи

Член 37

Во случај на физички пренос на документите контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат.

V.ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Престанување на важење

Член 38

Со денот на влегувањето во сила на овој Правилник престанува да важи Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци во Јавното претпријатие за државни патишта бр.02-7926/15 од 17.10.2014 година.

Член 39

Овој Правилник влегува во сила од денот на неговото донесување и истиот се објавува на ВЕБ страната на ЈПДП.

Заменик Претседател на Управен одбор

Блажена Бојовска