ВОДИЧ ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Овој проект е финансиран од Европската Унија

ВОДИЧ ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Овој проект е финансиран од Европската Унија

СОДРЖИНА

Овој проект е финансиран од Европската Унија

1. ШТО СЕ ЛИЧНИ ПОДАТОЦИ И КОИ СЕ ПРАВНИТЕ ОСНОВИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Овој проект е финансиран од Европската Унија

1. Што се лични податоци и кои се правните основи за заштита на личните податоци

Законот за заштита на личните податоци (натаму во текстот: ЗЗЛП) („Службен весник на Република Северна Македонија“ бр. 42/20 и) дефинира дека личен податок е секоја информација што се однесува на идентификувано или физичко лице кое може да се идентификува (субјект на лични податоци), при што физичко лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на идентификатори како што се име и презиме, матичен број на граѓанинот, податоци за локација, идентификатори преку интернет, или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, генетски, ментален, економски, културен или социјален идентитет.
Освен тоа, ЗЗЛП дефинира и посебни категории на лични податоци, односно податоци кои откриваат расна или етничка припадност, политички ставови, верски или филозофски убедувања и членство во синдикати, како и генетски податоци, биометриски податоци, податоци за здравјето или податоци за сексуалниот живот или сексуалната ориентација. Ваквите податоци не смеат да се обработуваат, освен кога се исполнети условите дадени во член 13, став (2) од ЗЗЛП.

Понатаму, ЗЗЛП пропишува дека сите организации се должни да применат соодветни организациски и технички мерки за заштита на личните податоци во зависност од категоријата на лични податоци, контекстот, целта за која податоците се собираат и обработуваат и можните ризици од губење или злоупотреба на податоците.
Согласно член 66, став (6) од ЗЗЛП, директорот на Агенцијата за

заштита на личните податоци (натаму во текстот: АЗЛП) усвојува Правилник за безбедност на обработката на лични податоци (натаму во текстот: Правилник), кој утврдува насоки за активностите коишто контролорите и обработувачите треба да ги преземат за примена на технички и организациски мерки за заштита на обработката на личните податоци.

2. ШТО СЕ ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ?

Овој проект е финансиран од Европската Унија

2. Што се технички и организациски мерки?

Како што беше наведено погоре, ЗЗЛП пропишува дека сите организации се должни да применат соодветни технички и организациски мерки за заштита на личните податоци, во зависност од обемот и категоријата на лични податоци, контекстот, целта за која податоците се собираат и обработуваат и можните ризици од губење или злоупотреба на податоците.

Техничките мерки може да се дефинираат како мерки кои контролорите и обработувачите ги применуваат во нивните системи и сите технолошки средства на организацијата, како што се: објекти/згради, уреди, мрежи, хардвер и хартиени податоци кои тие ги користат како мерки за заштита од неовластено пристапување до личните податоци и најдобра можна одбрана од нарушување на безбедноста на личните податоци. Примери за технички мерки се кибер-безбедност, криптирање и псевдонимизација, физичка безбедност, соодветно ракување со податоците, лозинки, овластувања за пристап до податоците, итн., и истите се пропишани во Правилникот.

заштита на личните податоци (натаму во текстот: АЗЛП) усвојува Правилник за безбедност на обработката на лични податоци (натаму во текстот: Правилник), кој утврдува насоки за активностите коишто контролорОрганизациските мерки може да се дефинираат како мерки кои ги сочинуваат интерни политики, организациски методи или стандарди, како и контроли и проверки кои контролорите и обработувачите ги пропишуваат и ги применуваат за да гарантираат безбедност на личните податоци. Примери за организациски мерки се политики за информатичка безбедност, план за континуитет на деловната активност, политики и постапки за сите видови обработка на лични податоци во рамките на организацијата, градење свест и обука на вработените, контроли и ревизии на пропишаните и применетите мерки, итн.. И овие мерки се пропишани во Правилникот.

Причината зошто контролорите и обработувачите треба да применат соодветни технички и организациски мерки лежи во потребата за минимизирање на ризикот од случајно или незаконско уништување, губење, изменување, неовластено откривање или неовластено пристапување до личните податоци кои се пренесени, чувани или на друг начин обработени, и одржување на способноста да обезбедат континуирана доверливост, интегритет, достапност и отпорност на информатичкиот систем што се користи за обработка на личните податоци и способноста за навремено повратување на достапноста на личните податоци во случај на физички или технички инцидент за да се осигури континуиран работен процес.

3. УПРАВУВАЊЕ СО РИЗИЦИ

Овој проект е финансиран од Европската Унија

3. Управување со ризици

За да се утврди кои технички и организациски мерки треба да бидат пропишани и применети со цел минимизирање на ризикот од случајно или незаконско уништување, губење, изменување, неовластено откривање или неовластено пристапување до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат, важно е прво да се утврдат/дефинираат и да се анализираат сите деловни процеси во рамките на организацијата која обработува лични податоци и да се утврдат и проценат потенцијалните ризици.

Процесот на управување со ризици се одвива во неколку фази:

- утврдување и составување список или преглед на деловните процеси кои вклучуваат обработка на лични податоци;
- проценка на ризиците за секој процес на обработка на лични податоци утврден во првата фаза;
- примена и проверка на планираните мерки кои се резултат од проценката и евалуацијата на ризиците;
- спроведување периодични безбедносни проверки.

Од друга страна, утврдувањето и составувањето список на деловните процеси, во најмала рака, ги опфаќа местата каде личните податоци може да се користат како дел од деловната активност:

- хардверска опрема (на пр., сервери, лаптопи, хард-дискови и други медиуми) на која се чуваат лични податоци во дигитален формат;
- софтверска опрема (на пр., оперативни системи и софтвери развиени за потребите на контролорот) со која контролорот (или обработувачот) ги обработува личните податоци;

- комуникациски канали (на пр., оптички кабли, интернет, безжична мрежна технологија, т.е. ви-фи) преку кои личните податоци минуваат во овој деловен процес;
- хартиени документи (на пр., печатени документи, копии) на кои има лични податоци.

При проценка на ризиците, контролорите и обработувачите треба, во најмала рака, да вложат максимални заложби за:

(а) идентификација на потенцијалното влијание и ефектите врз правата и слободите на засегнатите физички лица од можни закани, т.е. настани, како што се:

- неовластено пристапување до личните податоци;
- непланирани промени на личните податоци;
- привремена или целосна недостапност на личните податоци.

(б) идентификација на изворите на ризици кои може да бидат причина за непосакуваниот настан, со земање предвид на внатрешните и надворешните човечки фактори (на пр., администратор на информатичкиот систем, овластено лице, надворешен напаѓач, конкурент), како и други внатрешни и надворешни не-човечки фактори (на пр., поплави, штетни материјали, пожари, вируси);

(в) идентификација на потенцијалните закани кои би можеле да се појават преку медиумите на кои се чуваат податоците (на пр., хардвер, софтвер, комуникациски канал, хартиени документи, итн.), а кои може да бидат :

- користени на несоодветен начин (на пр., злоупотреба на овластувања, грешка при ракување со податоците);
- модифицирани (на пр., заробен софтвер или хардвер – регистрација на притискања на тастатура (keylogger), инсталација на малициозен софтвер, итн.);

- изгубени (на пр., кражба или загуба на мобилна опрема како што се лаптопи и мобилни телефони или преносни медиуми како што се мемориски стикови);
- следени (на пр., геолокација на опремата);
- оштетени (на пр., вандализам, деградација поради вообичаено користење);
- преоптоварени (на пр., целосна исполнетост на капацитетот на медиумот за складирање, напад со недостапност на услугата (denial of service attack), итн.);

(г) утврдување на постојните или планираните мерки за решавање на конкретниот ризик (на пр., контрола на пристап, резервни/безбедносни копии, следливост, безбедност на просториите, криптирање или анонимизација);

(д) оценување на сериозноста и веројатноста на ризиците во однос на претходните елементи предвидени во проценката на ризици (на пр., скалата за проценка што може да се користи е следнава: занемарлив, умерен, значаен и максимален ризик);

(ѓ) доколку ризикот е проценет како значаен или максимален, утврдување на други мерки кои може да се применат за да се минимизира ризикот.

Како резултат на процесот за управување со ризиците, контролорите и обработувачите треба да изготват документација која ги покрива следниве аспекти со повеќе детали:

- идентификација, евалуација и класификација на ризиците по процесите за обработка на лични податоци (анализа на ризиците);
- општ опис на техничките и организациските мерки за да се обезбеди тајност и да се заштити обработката на податоците коишто се соодветни на ризикот.

По проценката на ризиците, контролорите и обработувачите мора да ги применат и да ги контролираат планираните мерки за да се осигурат дека тие и натаму ги одржуваат ризиците на минимално ниво.

Контролорите и обработувачите мора да спроведуваат периодични контроли на безбедноста на обработката за кои треба да изготват акциски планови чијашто имплементација ја следи раководството на организацијата. Периодичните контроли на безбедноста на обработката треба да се спроведуваат за целите на држење чекор со технолошкиот развој, за спречување потенцијални нови инциденти што се базираат на технолошките промени и за примена на заштитни мерки кои можат соодветно да одговорат на новите инциденти.

4. ДОКУМЕНТАЦИЈА ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ

Овој проект е финансиран од Европската Унија

4. Документација за технички и организациски мерки

Како главен документ за технички и организациски мерки, контролорите и обработувачите изработуваат политика за системот за заштита на личните податоци во нивната организација. Согласно деловните процеси и ризиците кои биле утврдени и анализирани како дел од чекорот опишан во претходното поглавје, таквиот документ треба да ги наведе техничките и организациските мерки што ги применува контролорот/обработувачот.

Врз основа на политиката за системот за заштита на личните податоци, контролорите и обработувачите донесуваат подетални политики и постапки за секоја обработка на лични податоци во рамките на нивната организација, кои пак содржат опис на техничките и организациските за лицата кои имаат овластувања за пристап до личните податоци и до информатичкиот систем и инфраструктура. Овој документ треба да вклучи повеќе детали за:

- идентификацијата, евалуацијата и класификацијата на ризиците по процесите за обработка на лични податоци (анализа на ризиците);
- генерален опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на податоци коишто се соодветни на ризикот;

- активности за обука и градење свест кај менаџментот и вработените за ризиците по приватноста и безбедноста во рамките на контролорот;
- дизајнот, развојот и одржувањето на софтверот за обработка на податоци, особено од аспект на техничката и интегрираната заштита на личните податоци (privacy by design and privacy by default);
- начинот за автентикација на овластените лица во информатичкиот систем;
- начинот за контрола на пристапот до информатичкиот систем;
- начинот за водење евиденција за најавувањата во информатичкиот систем (на пр., пристап до оперативните системи, заштитен sид, посебно дизајниран сервер за датотеки, бази на податоци, софтвер за управување со документи (DMS), софтвер за управување со односите со клиентите (CRM), итн.);
- начинот за управување со инциденти (кои ја нарушуваат доверливоста, интегритетот или достапноста на податоците);
- начинот за обезбедување на опремата на контролорот што се користи за обработка на податоци;
- начинот за обезбедување на преносните медиуми;
- начинот за обезбедување на внатрешната мрежа на контролорот (интранет);
- начинот за обезбедување на серверите и веб-страниците на контролорот;
- начинот за водење и чување документи во апликациите/програмите што се користат за обработка на податоци;
- начинот за обработка на псевдонимизирани податоци;

- начинот за обработка на криптирани податоци;
- обврските и одговорностите на администраторот на информатичкиот систем и на овластените лица во врска со користење на информатичката и комуникациската опрема;
- начинот и процесите за известување, реагирање на инциденти и враќање на системот во нормална состојба;
- начинот за креирање, архивирање и чување на резервни копии, и начинот за повратна достапноста на податоците;
- начинот за уништување на документите, како и начинот за уништување, бришење и чистење на медиумите;
- физичката безбедност;
- начинот за ангажирање и контрола на надворешните субјекти (обработувачите);
- динамиката и начинот за спроведување периодични контроли, како и процеси за внатрешна контрола;
- други мерки кои контролорот ги применува врз основа на спроведената анализа на ризиците.

5. ОРГАНИЗАЦИСКИ МЕРКИ

Овој проект е финансиран од Европската Унија

5. Организациски мерки

По дефинирањето/утврдувањето и анализата на деловните процеси во кои се обработуваат лични податоци и по утврдувањето и анализата на потенцијалните ризици по обработката, контролорите треба да пристапат кон обезбедување соодветни организациски мерки за безбедност на личните податоци што тие ги обработуваат во согласност со одредбите од ЗЗЛП и Правилникот.

5.1 Стандардно ниво на организациски мерки

Стандардното ниво на организациските мерки што една организација треба да ги примени врз основа на анализираните деловни процеси кои подразбираат обработка на лични податоци и врз основа на утврдените и анализираните потенцијални ризици е уредено во членовите 30 до 36 од Правилникот.

5.1 .1. Организациски мерки за заштита на личните податоци (минимален стандард)

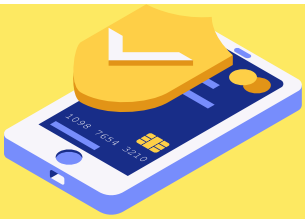
Член 30 од Прирачникот пропишува дека контролорите (и обработувачите) се должни да применат минимум стандард на организациски мерки, односно:

5.1.1.1. Утврдување на овластените лица кои имаат пристап до личните податоци

Во зависност од организацијата, т.е. од бројот на вработените, како и во зависност од деловните процеси на кои работат или нивните работни места, не се препорачува вработените да ги знаат личните (и другите) податоци кои се собираат и обработуваат, а кои не се поврзани со деловните процеси на нивното работно место.

Како мерка за заштита на личните податоци од неовластено пристапување во рамките на организацијата, контролорите треба да утврдат кои работни места, согласно работните процеси што ги извршуваат, имаат право на пристап, како и нивото на правото на пристап до и менување на личните податоци, и обемот на личните (и другите) податоци.

Примери:



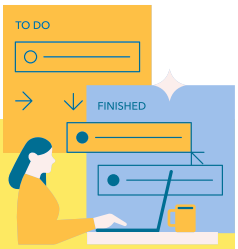
Една организација се занимава со продажба на резервни делови за возила и има сопствено седиште, магацин и продавница, сите на различни локации. Една од деловните политики на организацијата е да овозможи директна испорака на резервниот дел на домашната адреса на клиентите, доколку делот го има на залиха и доколку не станува збор за голем дел. Испораката на деловите до клиентите се врши од магацинот на организацијата.

Во продавницата, купувачот сака испорака на деловите за возило до неговата домашна адреса и продавачот ги собира и ги обработува неговите податоци (име, адреса и телефонски број) за деловите да бидат испорачани, и го информира дека испораката веќе е започната. Вработен во одделението за човечки ресурси нема потреба да биде запознаен со личните податоци на клиентот кои ги собира и ги обработува продавачот во продавницата за квалитетно да ги изврши своите деловни процеси. Од друга страна, вработен во магацинот треба да биде запознаен со личните податоци на овој купувач кои биле собрани и обработени од продавачот за да може да ги испорача деловите на клиентот во согласност со деловниот процес за испорака на делови.

Одделението за човечки ресурси се занимава со кадровските прашања во организацијата (обработка на податоците на вработените за склучување договори, поднесување пријави до други институции пропишани со законите за работни односи во Република Северна Македонија). Поради законските обврски и поради природата на деловниот процес, вработените во одделението за човечки ресурси собираат и обработуваат податоци за живеалиштето на вработените, членовите на нивните семејства, здравствената состојба на вработените, итн.

Вработените во магацинот или вработените во продавницата немаат потреба да бидат запознаени со личните податоци на другите вработени кои ги собира и обработува одделението за човечки ресурси. Исто така, раководителот на одделението за човечки ресурси не треба да има права/овластувања за додавање или менување на личните податоци за да може да раководи со одделението, и единственото право што ова лице треба да го има е правото на увид во таквите податоци.

Во зависност од големината на организацијата и расположливите ресурси, ова може да се регулира преку интерни акти/правилници кои ја опишуваат конкретната обработка на лични податоци и ги утврдуваат овластувањата/правата за обработка или пристап до личните податоци, интерни акти за систематизација на работните места и опис на работните места каде, исто така, може да се наведе кој има овластувања/права за обработка или пристап до личните податоци, или тоа може да биде дел од договорот за вработување и, како што е регулирано во член 31, ставови (4), (5) и (6) од Правилникот, преку изјава за тајност и заштита на обработката на лични податоци.



Примери:

Одделение за човечки ресурси на една организација почнува процес за вработување на ново лице. Меѓу другото, договорот за вработување вклучува и членови кои, според работното место, пропишуваат дека лицето ќе работи на компјутер до кој ќе има пристап преку единствено корисничко име и лозинка, дека ќе има право да работи со програми за подготовка на плати и право да додава, менува и обработува лични податоци на вработените за целите на исплата на плати и задолжителни придонеси. Исто така, лицето ќе има пристап до интернет преку соодветната програма да врши исплата на платите до банкарските сметки на вработените и да врши исплата на соодветните даноци и придонеси.

Една организација сака да воведе систем за видео надзор во согласност со одредбите од ЗЗЛП и Правилникот за вршење видео надзор, и за таа цел определува вработено лице кое ќе ја потпише ИЗЈАВАТА за безбедност на обработката на лични податоци преку системот за видео надзор каде се согласува и се обврзува да ги почитува начелата за заштита на личните податоци, да применува технички и организациски мерки за безбедност и доверливост на обработката на лични податоци, да ги обработува личните податоци во согласност со насоките дадени од неговата организација и да не открива какви било податоци или други лични информации кои му се достапни, односно ги дознал/ќе ги дознае како дел од неговите работни задачи во организацијата на трети страни.

Кога утврдуваат/одредуваат овластувања со право на пристап до лични податоци, контролорите се должни да внимаваат дали таквите овластувања дадени на некое лице се укинати и да обезбедат дека правото на пристап е повлечено веднаш по укинувањето на овластувањата. За таа цел и врз основа на спроведената анализа на ризиците, контролорите ги ревидираат и ажурираат овластувањата за пристап до информатичкиот систем во редовни интервали, но најмалку еднаш на секои три месеци.

5.1.1.2. Организациски правила за пристап до Интернет од страна на овластени лица во врска со симнување и снимање документи кои се преземаат од е-пошта или од други извори

Важно е контролорите да ја градат свеста на вработените за безбедно користење на е-поштата и содржините на Интернет, а за таа цел треба да пропишат организациски правила за пристап до Интернет од страна на овластени лица во врска со симнување и снимање документи кои се преземаат од е-пошта или од други извори. Подолу се дадени некои од основните правила за безбедно користење на Интернетот:

- кога користат Интернет, вработените треба да ги посетуваат само веб-страниците кои се потребни за извршување на нивната работа, односно официјалните веб-страници на компании или институции поврзани со нивната работа;
- вработените не смеат да ги користат хардверската опрема и Интернетот на организацијата за симнување, копирање или пиратирање софтверски програми, филмови, музика и електронски записи кои се заштитени со авторски права, трговски тајни или информации кои се однесуваат на сопственост, записи кои може да се наменети за хакирање

неовластени веб-страници, внесување малициозни софтвери во мрежата на компанијата или кои може да ја загрозат безбедноста на системите за електронска комуникација на организацијата;

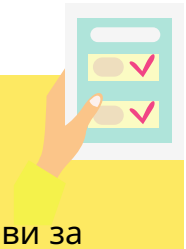
- службената е-пошта треба да се користи само за службена комуникација, а не за лични цели, за испраќање или објавување ланец-писма, за барање услуги/добра, или за рекламирање кое не е поврзано со службените цели или активности;
- вработените не треба да отвораат е-пошта од непознати испраќачи и/или со сомнителна содржина (на пр., ако добијат е-пошта од лице чиешто име е Питер Ли од mickey.mouse@mikrosoft.cn, самата адреса на е-поштата е неубедлива и не треба да се отвора. Ако содржината на е-поштата која доаѓа од официјална институција бара примателот да отвори линк и да внесе корисничко име и лозинка на веб-страницата на „официјалната институција" за проверка на корисничките податоци или за ажурирање на системот, таквата е-пошта не се смета за службена бидејќи ниту една институција не бара од корисниците да ги проверат корисничките податоци на таков начин и затоа вработените не треба да го отворат линкот. Во обата случаи, е-поштата треба да избрише или да се означи како „спам").

5.1.1.3. Уништување на документи по истекот на нивниот рок за чување

Уште една мерка за информатичка безбедност што ја пропишува ЗЗЛП се однесува на фактот дека личните податоци се чуваат само за временски период кога се потребни за целите за кои се обработуваат.

Целта на утврдувањето на оваа мерка од аспект на информатичката безбедност е намалување на обемот на лични податоци на минимално ниво во случај на кражба, неовластена или незаконска обработка на лични податоци.

Од тие причини, секоја организација треба постојано да води сметка од нејзините системи за обработка на лични податоци да ги отстрани оние податоци за коишто повеќе не постои цел за обработка и за коишто е истечен законскиот рок за чување.



Примери:

Во продавницата на една компанија која продава резервни делови за возила, клиентот сака деловите да бидат испорачани на неговата домашна адреса. За таа цел, од клиентот се собираат податоци за име/презиме, домашна адреса и телефонски број, и истите се внесуваат во компјутерска програма наменета за испорачување на деловите и известување на клиентот дека постапката за испорака е во тек. Деловите се испорачани до клиентот и тој недвосмислено ја потврдува испорака на испратницата за преземање на купените делови. По овој чин, компанијата нема потреба да ги чува горенаведените податоци на клиентот во софтверот за изработка на фактури.

Една компанија обезбедува услуги за фиксна телефонија и со корисникот склучува нов договор на секои две години. Договорот и личните податоци треба да се обработуваат и чуваат до исполнување на целта/до извршување на договорот (плус задолжителен период за можни

финансиски побарувања), додека фактурите се чуваат како сметководствени документи во согласност со прописите за сметководствени работи.

- Во одреден временски период, компанијата треба да ја уништи опремата што ја користи, и тоа поради грешка во работењето или поради застареност, а доколку опремата била изнајмена и рокот на изнајмување истекол, таа треба да биде вратена. Ваквата опрема (посебно компјутерите и мобилните уреди) сè уште содржи податоци. Податоците кои се чуваат во дигитална форма треба безбедно да се избришат/уништат пред отстранување на опремата како електронски отпад или пред нејзино донирање кога дел од опремата сè уште има одредена корисна вредност.
- Податоците во дигитална форма се чуваат на уреди за складирање:
- Дискови (хард-диск, ССД-диск, итн.) на компјутери, машини за копирање, опрема за снимање која е дел од системот за видео надзор, итн.;
- Дискови на мобилната опрема, мемориски картички, СИМ картички, мобилни уреди;
- Преносни медиуми: додатен диск, УСБ уред, мемориски картички, ЦД/ ДВД, магнетни ленти, итн.

Безбедно отстранување на податоците од дигиталниот медиум може да се направи преку:

- безбедно бришење на медиумот за складирање;
- физичко уништување на медиумот за складирање;
- демагнетизација.

За безбедно да се избрише медиумот за складирање не е доволно само да се избришат податоците или форматот на медиумот, бидејќи избришаните или форматираните податоци можат успешно да се повратат. Безбедно бришење се врши со користење програми кои се специјално дизајнирани за таа цел. Медиумот за складирање се поврзува на компјутер на кој е сместена програмата за безбедно бришење, и потоа, преку пуштање на програмата и избирање на медиумот, се прави безбедно бришење на податоците. Процесот на безбедно бришење одзема многу време и затоа тој не се смета за стандардна опција за бришење датотеки и програми во оперативните системи, бидејќи тоа значително ја намалува брзината и функционалноста на компјутерот.

Безбедно бришење на паметните телефони и таблети се врши преку избирање на опцијата за враќање на фабричките поставки на уредот.

Физичко уништување на медиумите за складирање вклучува уситнување на најмали делови со цел, при обид за повторно вклучување на медиумот, да се оневозможи успешно повратување на достапноста на податоците кои се складирани на таквите медиуми. На пример, ЦД/ДВД, како и хартиени документи кои содржат податоци, се уништуваат со специјален уситнувач на ЦД/ДВД или уситнувач на хартија, и потоа се фрлаат. Дискови, додатни дискови и мемориски картички се уништуваат на мали делови со дробилка.

На пазарот постојат компании кои се специјализирани за безбедно бришење на медиумите и кои потоа издаваат сертификат за нивната услуга со кој се потврдува дека медиумот бил безбедно избришан.

Изборот на соодветен метод за безбедно бришење или уништување на податоци ќе зависи од:

- обемот на податоци кои се содржани на медиумот;
- видот на податоци кои се содржани на медиумот,
- видот на медиум на кој се чуваат податоците;
- состојбата на самиот медиум.

Организацијата треба да формира комисија која ќе состави записник со сите потребни информации за целосна идентификација на документите и категориите на лични податоци кои се содржани на опремата што се брише/уништува.

5.1.1.4. Мерки за физичка безбедност на просториите и информатичката и комуникациската опрема на која се собираат, обработуваат и чуваат лични податоци

Кога воспоставува заштитни мерки, организацијата треба да размисли за воведување соодветни физички мерки за заштита од неовластен пристап до нејзините простории и до опремата што ја користи.

При воведување мерки за физичка заштита, предвид треба да се земе следново:

- обезбедување на објектот од неовластен пристап вон работните часови на организацијата (на пр., преку инсталирање аларми против кражба и преку инсталирање на систем за видео надзор доколку проценката на ризикот покаже дека тоа е неопходно и оправдано);
- ограничување на пристапот до канцеларискиот мебел и просториите каде се чуваат лични и други доверливи податоци (на пр., простории каде се лоцирани компјутери/сервери на кои се чуваат податоците, простории и ормани каде се чуваат податоци во хартиена форма, итн.);

- ограничување на пристапот до опремата на која се чуваат податоци (сервери на компјутерите, диск-системи, екстерни дискови) преку нивно поставување на соодветен канцелариски мебел (на пр., полици за сервери) или во простории кои се соодветно обезбедени од неовластен пристап (на пр., со користење клучеви или паметни картички);
- поставување на другата опрема (на пр., интернет-рутери, мрежни прекинувачи) на соодветен канцелариски мебел (на пр., полици за сервери) или во простории кои се соодветно обезбедени од неовластен пристап (на пр., со користење клучеви или паметни картички);
- физичко одделување на канцелариската опрема (компјутери, печатачи, машини за копирање, итн.) кои се користат за интерактивна работа со корисниците на деловните услуги од самите корисници на услугите или, во најмала рака, отежнување на пристапот до опремата и до податоците (на пр., меѓу корисниците и работното место) преку поставување шалтер кој го спречува корисникот да пристапи до опремата, печатачите, машините за копирање и канцелариското мебел каде се чуваат податоците во хартиена форма, или обезбедување дека тие се доволно далеку за да спречат корисникот да има увид во податоците, мониторот на компјутерот е свртен со задната страна кон корисникот, итн.

5.1.1.5. Усогласеност со техничките насоки за инсталирање и ракување со информатичката и комуникациската опрема што се користи за обработка на лични податоци

Сите работи што организацијата ќе ги пропише во своите технички насоки (или некој друг документ) кои се однесуваат на мерки за заштита на

личните податоци мора да се спроведуваат и применуваат. Во спротивно, тие ќе останат само „мртво слово на хартија“. Од тие причини, важно е организацијата да ги применува сите мерки за заштита на личните податоци пропишани во интерните документи за да го минимизира ризикот од случајно или незаконско уништување, губење, изменување, неовластено откривање или неовластено пристапување до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат, и за да ја одржи способноста за обезбедување континуирана доверливост, интегритет, достапност и отпорност на информатичкиот систем што се користи за обработка на податоци и способноста за навремено враќање на достапноста и пристапот до личните податоци во случај на физички или технички инцидент за целите на овозможување континуитет на работните процеси.

5.1.2. Информирање и едукација за заштита на личните податоци

Човечкиот фактор е најважниот фактор во процесот на спроведување на пропишаните технички и организациски мерки за заштита на личните податоци, па затоа ако сите вработени, без оглед на нивното ниво во хиерархијата на организацијата (од директор/сопственик до хигиеничари), не се свесни за важноста на информатичката безбедност и одговорноста на секое лица за заштита на податоците, тогаш пропишаните мерки немаат никакво значење.

Дури и кога само еден вработен не е свесен за тоа и ги занемарува мерките за информатичка безбедност и заштита на личните податоци, тој/таа го загрозува целиот систем на организацијата и го изложува на

потенцијална кражба, злоупотреба и загуба на личните и другите деловни податоци што се собираат и обработуваат како дел од деловната активност. Во зависност од категоријата на „изгубените“ податоци и нивниот обем, последиците може да биде катастрофални за самата организацијата, и последователно, за вработениот кој покажал неодговорност.

Од исклучителна важност е сите вработени да бидат свесни за следново:

- кои лични (и деловни) податоци ги користат и ги обработуваат како дел од нивната секојдневна работа;
- на кои категории на лични податоци тие им припаѓаат (дали се „обични“ лични податоци, лични податоци на деца, посебни категории на лични податоци);
- каде се лоцирани овие податоци за време на нивната обработка;
- кои се потенцијалните ризици од кражба, злоупотреба и загуба на овие податоци;
- како тоа може негативно да влијае врз организацијата во којашто работат и, во крајна линија, врз самите вработени;
- какви мерки треба да се применат за да се заштитат овие податоци;
- потребата да ги применуваат препорачаните и пропишаните заштитни мерки на секојдневна основа за да ги сведат потенцијалните ризици од неовластено пристапување и злоупотреба на минимално ниво.

Затоа, уште при самото ангажирање или вработување кај контролорот, и посебно пред почетокот на нивната кариера во организацијата, сите вработени мора да бидат запознаени со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

Вработените или ангажираните лица потпишуваат изјава за тајност и заштита на обработката на лични податоци, која се чува како дел од досието на вработеното или ангажираното лице.

Вработените кои се одговорни за управување со човечки ресурси кај контролорот го известуваат администраторот на информатичкиот систем за вработување или ангажирање овластени лица со права за пристап до информатичкиот систем за да се обезбеди дека овие лица ќе добијат корисничко име и лозинка за пристап до делови од информатичкиот систем врз основа на нивните овластувања за пристап до лични податоци, како и за прекинување на работниот статус или ангажманот на ваквите лица, за да се обезбеди дека нивните кориснички имиња и лозинки ќе бидат избришани, т.е. заклучени за натамошно користење. Тоа треба да се направи и кога вработеното или овластеното лице го менува работното место или кога добива поголеми или помали овластувања поради промените во донесената документација за технички и организациски мерки.

Исто така, организацијата треба да обезбеди континуирана информираност и едукација за раководителите и овластените лица во врска со нивите директни обврски и одговорности за заштита на личните податоци.

5.1.3. Обврски и одговорности на администраторот на информатичкиот систем и на овластените лица

Овластените лица, а посебно администраторите, немаат само права, туку и обврски и одговорности поврзани со информатичкиот систем. Контролорот треба да ги запознае администраторите и овластените лица со документацијата за технички и организациски мерки која се однесува на извршување на нивните обврски и одговорности. Во најмала рака, нивните одговорности се однесуваат на користење на документите и на информатичката и комуникациската опрема преку спроведување на мерките пропишани во Правилникот и интерната документација со која е уредена заштитата на личните податоци во организацијата и треба да бидат запознаени со нивните обврски и одговорности во врска со информатичкиот систем (исто како што се запознаат со нивните права).

Поради големите овластувања што ги имаат во врска со информатичкиот систем на организацијата, администраторите на такви системи треба да бидат под надзор и контролорите мора да спроведуваат периодични контроли на работата на администраторот на информатичкиот систем и да изготвуваат извештаи од таквите контроли. Овие извештаи треба да содржат информации за утврдените нерегуларности (кога тоа е соодветно) и предлог мерки за отстранување на истите.

5.1.4. Заштита на податоците кои се чуваат во хартиена форма

И покрај современите компјутери и модерните технологии, деловните субјекти сè уште користат податоци кои се чуваат во хартиена форма. Оттука произлегува потреба за утврдување соодветни мерки за заштита на податоците во хартиена форма од неовластено пристапување.

Како што беше наведено претходно, без оглед на тоа дали податоците се чуваат во дигитална или хартиена форма, потребно е да се утврди кои работни позиции, во согласност со деловните процеси што ги извршуваат, имаат право на пристап до широк спектар на лични (и други) податоци кои се потребни за извршување на нивната работа.

Бидејќи хартијата е физички медиум, тоа налага физички мерки за заштита од неовластено пристапување до податоците што се чуваат во хартиена форма. По користењето, ваквите податоци мора да се чуваат во соодветен простор и во соодветен канцелариски мебел (фиока, орман, огноотпорен орман, итн.) кои се заштитени од неовластено пристапување со користење клуч или на друг безбедносен начин (на пр., картичка со чип и читач на чипови), наместо да се чуваат на отворено (на пр., на работната маса, на отворена полица, итн.).

Примената на правилото „чисто биро“ е начин кој обезбедува дека сите важни документи, доверливи писма, папки, книги, итн., се отстрануваат од бирото и се заклучуваат во соодветен простор и во соодветен канцелариски мебел кога повеќе не се користат или

кога вработениот го напушта неговото работно место. Тоа е една од врвните стратегии што може да се користи за намалување на ризикот од нарушување на безбедноста на личните податоци. Исто така, во работниот простор не треба да има самолепливи ливчиња за белешки и хартии со информации како што се корисничка име, лозинка или број на банкарска сметка, и овој простор треба да биде ослободен од сите несуштински документи.

По исполнувањето на целта и по истекот на законската обврска за чување на податоците во хартиена форма, ваквите документи треба да се уништат со користење на машина за уситнување хартија. За таа цел, контролорот формира комисија која составува записник со сите информации коишто се потребни за целосна идентификација на документите и категориите на личните податоци содржани на истите.

5.2. Високо ниво на организациски мерки

Високото ниво на организациски мерки е уредено во член 45 од Правилникот, каде се вели дека во случај на копирање и умножување на документи, тоа може да се врши единствено од страна на овластени лица кои се определени од контролорот во постапка во која задолжително се утврдуваат мерките и начинот на копирање и умножување на документи. Уништувањето на копираните или умножените документи треба да се направи на начин кој ќе оневозможи натамошно обновување/ повратување на содржаните лични податоци. И член 46 од Правилникот се однесува на високо ниво на организациски мерки и пропишува дека, во случај на физички пренос на документи, контролорот мора да примени мерки за заштита од неовластено пристапување или ракување со личните податоци содржани во таквите документи.

6. Технички мерки

Овој проект е финансиран од Европската Унија

6. Технички мерки

По дефинирањето/определувањето и анализата на деловните процеси кои подразбираат обработка на лични податоци и по идентификувањето и анализата на потенцијалните ризици за обработката, како и по дефинирањето соодветни организациски мерки за безбедност на личните податоци кои ги обработуваат, контролорите треба да ги применат сите мерки кои се пропишани во усвоените документи за технички и организациски мерки.

6.1. Стандардно ниво на технички мерки

По дефинирањето/утврдувањето и анализата на деловните процеси кои подразбираат обработка на лични податоци и по идентификувањето и анализата на потенцијалните ризици на обработката, како и по дефинирањето соодветни организациски мерки за безбедност на личните податоци кои ги обработуваат, контролорите треба да ги применат сите мерки кои се пропишани во усвоените документи за технички и организациски мерки.

Членовите 12 до 29 од Правилникот се однесуваат на стандардното ниво на технички мерки што една организација треба да ги примени врз основа на анализата на потенцијалните ризици и да примени соодветни технички мерки за безбедност на личните податоци кои се обработуваат.

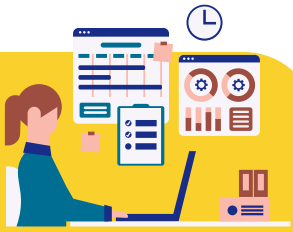
6.1.1. Примена на соодветни технички мерки за исполнување на одредбите за овластувања за пристап до личните податоци

Овластувањата за пристап до личните податоци би останале само „мртво слово на хартија“ без каква било практична цел ако не се спроведат соодветни технички мерки кои се однесуваат на структурата/објектите на организацијата, мрежите, хардверската опрема и безбедноста на податоците во хартиена форма.

Овластувањата на вработените кои им се доверени како дел од нивните работни позиции и личните податоци кои ги обработуваат треба да бидат спроведени во сите делови од информатичкиот систем на организацијата, а не само во деловите до кои овие вработени имаат овластувања за пристап. Тоа вклучува хардверска опрема (компјутери, печатачи, скенери, итн.), комуникациска опрема, деловен софтвер и простории/канцеларии кои имаат пропишана цел. Ваквите права за пристап треба да бидат укинати веднаш по истекот на овластувањата.

Врз основа на спроведената анализа на ризиците, контролорите ги ревидираат и ги ажурираат овластувањата за пристап до информатичкиот систем на овластените лица во редовни временски интервали, но најмалку на секои три месеци, а по упатство од контролорот, администраторот на информатичкиот систем доделува, менува или укинува овластувања за пристап до личните податоци и до информатичката и комуникациската опрема во согласност со критериумите што ги утврдил контролорот.

Сите овластени вработени пристапуваат до информатичкиот и комуникацискиот систем преку единствени идентификатори, како што се корисничко име и лозинка, единствена паметна картичка што им доделена, дигитален потпис или некој друг метод за автентикација во согласност со најновата технологија којшто обезбедува единствени идентификатори поврзани само со овластеното лице во контекст на спроведената анализа на ризиците.



На пример:

Согласно природата на неговата работа, администраторот на системот има административен пристап до сите компјутери и до оперативниот систем во рамките на организацијата преку административно корисничко име и лозинка, до собата со сервери преку паметна картичка, до серверите и до другата информатичка опрема во собата за сервери преку административна лозинка за секој сервер и за секој дел од опремата на серверот, до комуникациската опрема и мрежа, до оперативните системи на серверите, до деловниот софтвер и до базите на податоци преку административни лозинки за целите на администрација и поправка.

Поради ваквите големи овластувања и врз основа на спроведена анализа на ризиците, таквиот пристап може да се подели на неколку администратори при што секој од нив има можност да пристапи само до строго определените делови од информатичкиот систем на организацијата, на пример, еден администратор има право за пристап до комуникациската опрема и мрежа, друг администратор има право за пристап до оперативниот систем на серверот, трет администратор има право за пристап до деловниот софтвер и базите на податоци содржани на софтверот, итн.

Од друга страна, вработените во одделот за сметководствени работи кои ги пресметуваат платите на вработените имаат право на пристап до нивните работни компјутери преку сопствено корисничко име и лозинка (или преку сопствена паметна картичка), до деловниот софтвер за плати преку сопствено корисничко име и лозинка, но немаат право на пристап до, на пример, компјутерите и деловниот софтвер во одделот за сметководствени работи кои обработуваат лични податоци на клиентите.

Врз основа на спроведената анализа на ризиците за конкретниот работен процес, контролорите може да користат комбинација од два или повеќе методи за автентикација за некои или за сите овластени лица (на пр., единствено корисничко име и лозинка во комбинација со паметна картичка).

Контролорите мора да водат евиденција за овластените лица со права за пристап до документи и до информатичкиот систем, и мора да воспостават постапки за идентификација и верификација на овластувањата за пристап.

Врз основа на спроведената анализа на ризиците и во случаи кога верификацијата што се заснова на корисничко име и лозинка (Правилникот пропишува дека лозинката треба да биде составена од најмалку 8 карактери и/или знаци), контролорите мора да применуваат правила кои гарантираат доверливост и интегритет во врска со известувањето, доделувањето и чувањето на такви информации, при што лозинките мора автоматски да се сменат по истекот на дефиниран временски период кој не смее да биде подолг од три месеци.

Со оглед на тоа дека лозинките се најчесто користен метод за заштита на информатичкиот и комуникацискиот систем од неовластено пристапување, сите треба да бидат свесни за неколку правила што се однесуваат на креирањето лозинки.

Една силна лозинка мора да содржи:

- 16 или повеќе карактери или знаци, колку повеќе – толку подобро;
- големи букви (ABCDEFGH, итн.);
- мали букви (abcdefgh, итн.);
- бројки (34 123456);
- симболи (@ # $% {} [] () / \ '",;:. <>...).

При креирање лозинка треба да се избегнува следново:

- зборови од речници, посебно на англиски јазик (airplane, laptop, RedSox, car, bicycle, computer, итн.);
- често користени и генерално познати лозинки (password, default, admin, guest, итн.);
- сопствени лични податоци или податоци на роднини (име/презиме, датум на раѓање, венчавка, вработување, итн., адреса на живеење, имиња на деца, блиски роднини, домашни миленици, име на компанија, итн.) (Vlatko Markovski, Vlatko 14.02.1988., 14.02.1988, Ulica 111, 1000 Skopje, итн.);
- корисничко име (vlatko.markovski, vmarkovski, итн.),
- серија на исти букви, бројки или знаци (aaaaa, aaaa1111, aa11 ++, ..)
- повторување на исти зборови (vlatkovlatko, plainplain, итн.);
- серија на букви и/или бројки од тастатурата (qwertz, 123456, 1q2w3e4r5t, итн.);

- добропознати идентификациски податоци (на пр., матичен број, број на здравствено осигурување, број на лична карта, број на регистерска табличка, адреса на работното место, кат и број на канцеларија, итн. (SK-2324-BC, Boulevard Alexander the Great 29, итн.);
- лошо креирани лозинки или лошо конвертирани фрази (password123, password356, john1234, vlatko12345, p@ssw0rd, l0z1nk@).

На Интернет постојат генератори кои креираат силни лозинки врз основа на горенаведените правила (пример за генерирана лозинка: UZCQf] &} q {f4c + ct).

Лозинките кои се генерирани на овој начин (случајно избрана низа на букви, бројки и симболи) се тешки за помнење. Од таа причина, корисниците може да го искористат трикот со избирање фраза или цитат за генерирање лозинка. Потоа се додаваат симболи и некои букви се заменуваат со бројки или симболи (на пример, од фразата „Fruit after rain" може да се креира лозинката % Fru1t#@fT3r=r@1N+?). Ваква лозинка полесно се помни за разлика од случајно избрана низа на букви, бројки и симболи.

Силните лозинки не мора периодично да се менуваат согласно безбедносните препораки дадени погоре. Истражувањата покажуваат дека поради честите промени на лозинката и потребата за креирање единствена лозинка за пристап на секој дел од програмата и за секоја програма одделно, корисниците почнуваат да користат помалку безбедни лозинки или ја користат истата лозинка за повеќе уреди и програми. Кога постои сомнеж дека е компромитирана од неовластен корисник и овозможува неовластено пристапување, силната лозинка треба да биде сменета на уредот или во програмата.

Во денешната дигитална ера, сите користиме разна опрема, дигитални информатички системи, дигитални услуги, итн. и за тоа ни требаат одреден број кориснички имиња и лозинки за овластен пристап до секој дел од опремата, до секој дел од информатичкиот систем, до секоја дигитална услуга, итн., или, во најмала рака, ни треба уникатна лозинка. За да ги запомниме сите лозинки, на Интернет може да се најдат голем број бесплатни и комерцијални програми за управување со лозинки коишто можат да се инсталираат на компјутер или на мобилен телефон. Ваквите програми ги чуваат сите кориснички имиња и лозинки во строго криптирана база на податоци за да ги заштитат од неовластено пристапување и тие може да бидат корисни за лесно извлекување на лозинките кога ни требаат.

Вработените не треба да ги откриваат нивните кориснички имиња и лозинки на другите вработени. Доколку тоа е неопходно поради исклучителни и оправдани причини (на пр., вработениот е на долго боледување и треба да се пристапи до неговиот компјутер, деловните програми и/или е-поштата), по завршувањето на таквата причина вработениот треба веднаш да ги замени старите лозинки со нови.

6.1.2. Обезбедување на опремата што се користи за обработка на лични податоци

Контролорите треба да ги применат следниве технички мерки за обезбедување на опремата што ја користат за обработка на лични податоци:

- автоматско одјавување на корисникот од информатичкиот систем по истекот на определен период на неактивност (не подолго од 15 минути);
- автоматско отфрлање од информатичкиот систем во случај на одреден број неуспешни обиди за најавување кои се спротивни на политиките за автентикација на контролорот; контролорите треба да го утврдат бројот на неуспешни обиди за најавување што е соодветен на ризикот и природата на работните процеси поврзани со обработката на лични податоци, но тој не смее да биде повеќе од пет последователни неуспешни обиди;
- во случај на повторено неуспешно најавување, овластените лица треба да подлежат на автентикација за да се идентификува дали тие сè уште имаат овластувања за пристап до тој дел од информатичкиот систем или им е забранет пристап поради промени во работната средина (промена на работните процеси, лицето повеќе нема овластувања за пристап, итн.);
- инсталирање на заштитен ѕид (firewall) во информатичкиот систем и поставки кои дозволуваат само ограничен број на овластени порти за комуникација за лицата за кои е строго неопходно да имаат таков пристап, за да се овозможи правилно функционирање на апликациите кои се инсталирани на работните станици кај контролорот;
- инсталирање на антивирусна програма на сите компјутери (работни станици или сервери) и дефинирана политика за редовно ажурирање на антивирусната програма, критичко ажурирање на оперативниот систем и на деловниот софтвер, при што се дефинира дека сите овие системи/програми треба да се ажурираат за да се спречат критички фабрички недостатоци и тоа во интервал кој не е подолг од една недела;

- претходна конфигурација на апликациите за да се обезбеди автоматско безбедносно ажурирање;
- кога е применливо, складирање на податоците на корисникот на серверите на контролорот со правење редовни резервни копии, а во случај на локално складирани податоци (кога контролорот нема сервери за складирање на податоците) и врз основа на спроведената анализа на ризиците, задолжително спроведување на синхронизација на податоци или мерки за правење резервни копии;
- воведување на ограничена опција за приклучување на преносни/ екстерни медиуми (УСБ, мемориски картички, екстерни хард-дискови, итн.) на деловите од информатичкиот системот кои се од критичко значење;
- оневозможување на функцијата за авто-вчитување на преносни/ екстерни медиуми (УСБ, мемориски картички, екстерни хард-дискови, итн.);
- добивање претходна согласност од корисниците на работните станици (овластените лица) за користење администраторски алатки од далечина пред интервенција на нивните работни станици и соодветно известување по завршувањето на администрирање од далечина (на пр., преку прикажување порака на нивниот екран дека администрирањето од далечина е завршено);
- приклучување на уреди за непрекинато снабдување со електрична енергија (УПС уреди) на важните делови од информатичкиот систем (работни станици, сервери, делови за складирање на информации, мрежна опрема);
- забрана за слободно симнување и инсталирање на апликации од Интернет или барем забрана за работа со симнати апликации кои не доаѓаат од безбеден извор;

- ограничување на користењето апликации кои налагаат правата за администрирање да ги имаат само администраторите,
- бришење на податоците кои постојат на работните станици што треба да бидат доделени на друго лице;
- во случај на компромитирани работни станици, преземање активности за идентификација на изворот и траги од упадот во информатичкиот систем на контролорот, со цел да се утврди дали и други елементи од истиот се под закана;
- безбедносно следење на софтверската и хардверската опрема што се користи во информатичкиот систем на контролорот, вклучително и редовно следење на националниот центар за одговор на компјутерски инциденти (MKD-CIRT) во врска со предупредувања и совети за ранливости на конкретната софтверска и хардверска опрема;
- градење на свеста кај овластените лица за прашања кои налагаат посебно внимание и обезбедување контакт информации за лицата кои треба да ги контактираат во случај на инцидент или појава на невообичаен настан кој влијае врз информатичкиот и комуникацискиот систем на контролорот.

6.1.3. Водење евиденција за најавите во информатичкиот систем

Член 15 од Правилникот ја содржи следнава одредба:
„(1) Со цел да обезбеди идентификување на секој неовластен (измамнички) пристап или злоупотреба на личните податоци, и да се утврди потеклото на таквите инциденти, контролорот воспоставува и води евиденција за секој пристап/најава во информатичкиот систем (на пр., од оперативните системи,

заштитниот ѕид, специјално дизајнираниот софтвер за употреба како софтвер за датотеки, базите на податоци, системот/софтверот за управување со документи, системот/софтверот за управување со односите со клиенти, итн.).

(2) Евиденцијата од ставот (1) на овој член посебно ги содржи следниве податоци: име/презиме на овластеното лице, работната станица од каде се пристапува до информатичкиот систем, датум и време на пристапувањето, личните податоци до кои е пристапено, видот на пристапување со операции преземени во однос на обработка на личните податоци, записи за автентикација на пристапувањето, записи за сите неовластени пристапувања, и записи за автоматско одбивање од страна на информатичкиот систем.

(3) Евиденцијата од ставот (1) од овој член содржи и информации за идентификација на информатичкиот систем кој бил користен за надворешен обид за пристапување до оперативните функции или личните податоци без потребното ниво на овластување.

(4) Операциите кои овозможуваат водење евиденција за информации од ставовите (2) и (3) на овој член ги контролира офицерот за заштита на личните податоци и/или друго лице овластено од контролорот кое ги поседува потребните знаења и вештини, но нема администраторски привилегии и истите треба да бидат нагодени/конфигурирани на начин кој оневозможува тие да бидат исклучени/деактивирани. Во однос на евиденцијата за пристапи/најави, контролорот може да користи и алатки кои генерираат такви податоци во едноставна и лесно читлива форма.

(5) Евиденцијата од ставот (1) на овој член се чува за период од најмалку пет години.

(6) Офицерот за заштита на личните податоци ја врши контролата од ставовите (2) и (3) на овој член најмалку еднаш месечно и изготвува извештаи за извршената контрола и констатираните неправилности.

(7) Контролорот ги известува овластените лица за воспоставениот систем за евиденција на пристап во информатичкиот систем.

(8) Контролорот обезбедува заштита на системот за евиденција на пристап до информатичкиот систем од какво било неовластено пристапување, особено од страна на лицата чијашто активност се евидентира во записите од системот за евиденција.

(9) Контролорот обезбедува дека овластените лица за управување со системот за евиденција на пристап до информатичкиот систем го известуваат раководството за сите аномалии или безбедносни инциденти веднаш или најдоцна во рок од 12 часа од моментот на таквиот инцидент.

(10) Контролорот ја известува Агенцијата за заштита на личните податоци за секое нарушување на безбедноста на личните податоци, а доколку постои веројатност дека таквиот настан ќе резултира со висок ризик по правата и слободите на физичките лица, ги информира и субјектите на лични податоци за тие да можат да ги ограничат последиците од нарушувањето на безбедноста.

(11) Контролорот не смее да ги користи информациите од евиденцијата за пристап до информатичкиот систем за цели кои се различни од целта за соодветно користење на информатичкиот систем (на пр., користење на записите за следење на работните часови на вработените претставува злоупотреба на информатичкиот систем).“

Иако многу делови од информатичкиот систем имаат сопствени записи за пристап, таквите записи не секогаш ги исполнуваат одредбите од член 15 од Правилникот во однос на обемот на информации што треба да се соберат во врска со евиденцијата за пристап (став (2) и став (3) од член 15). Исто така, многу делови од информатичкиот систем може автоматски да алармираат за аномалии во однос на овластено пристапување до делови од информатичкиот систем (потенцијално неовластено пристапување). Член 15 од Правилникот пропишува дека овластените лица го известуваат раководството за сите аномалии или безбедносни инциденти веднаш или во рок од 12 часа од моментот кога настанал таков инцидент.

Сето ова тешко може да се утврди ако не се примени систем што може да ги следи сите пристапи/најави во информатичкиот систем, да ги анализира и да ги алармира овластените лица за аномалиите во однос на овластено пристапување до деловите од информатичкиот систем.

За да се исполнат барањата дадени во член 15 од Правилникот, контролорите треба да применат систем за информатичка безбедност и управување со настани (SIEM). Ваквиот систем/софтвер го комбинира управувањето со информатичката безбедност и управувањето со безбедносни настани за да обезбеди анализа во реално време на безбедносните аларми што ги генерираат програмите и мрежната хардверска опрема. SIEM системот/софтверот функционира преку собирање записи за пристапи и настани што ги генерираат работните програми кои ги користи организацијата, безбедносните уреди и системите за хостирање, и сите ги става на едно место, т.е. на централизирана платформа.

SIEM системот/софтверот собира информации од антивирусни настани, записи на заштитниот sид и од други локации, и истите ги групира по категории, на пример, малициозна активност или неуспешно/успешно најавување во системот. Кога ваквиот систем/софтвер идентификува закана преку следење на безбедноста на мрежата, тој генерира аларм и го дефинира нивото на закана врз основа на претходно утврдени правила. На пример, кога некој се обидува да се најави во системот преку корисничко име/сметка 10 пати во период од 10 минути – тоа се смета за нормално, но кога постојат 100 обиди за најавување во период од 10 минути, таквиот настан мора да се означи како обид за напад на системот. На тој начин, системот ги детектира заканите и веднаш креира безбедносни аларми.

6.1.4. Обезбедување на мобилната опрема и преносните медиуми

Поради фактот дека може да се користат надвор од безбедната средина во рамките на организацијата, мобилната опрема (лаптопи/таблети, преносни печатачи со внатрешна меморија, мобилни телефони, итн.) и преносните медиуми (екстерни дискови, УСБ уреди, ЦД РОМ, ДВД, мемориски картички, СИМ картички, итн.) се повеќе и почесто изложени на неовластено пристапување, губење или кражба, и во таква ситуација, тие се подложни на потенцијално нарушување на безбедноста на личните податоци.

Па затоа, врз основа на спроведената анализа на ризиците и резултатите од таквата анализа, интерната документација на контролорот треба да го уреди начинот за користење на таквата опрема во рамките на организацијата, при што таа треба да се користи само од страна на

вработени со соодветни овластувања и по претходно добиена согласност. Кога не ја користат ваквата опрема, вработените со соодветни овластувања треба да ја чуваат на безбедно место или локација до која пристап имаат само овластени лица кои се определени во интерните документи на контролорот. Исто така, овластените лица треба да бидат запознаени со интерните правила кои се однесуваат на користење на ваквата опрема. На пример, кога поради природата на нивното работно место, дополнително на канцелариската работа вработените треба да работат и надвор од организацијата, тие треба да потпишат документ за прием на опремата за која имаат соодветно овластување за користење и пред користењето на истата треба да бидат запознаени со пропишаните интерни правила за соодветно користење на опремата, како и за мерките што треба да ги применат за да ја заштитат истата. Па така, кога не ја користат опремата, вработените треба да ја чуваат на безбедно место или локација пропишана од контролорот, како што се канцеларии и/или ормани до кои пристап имаат само овластените вработени.

Пристапот до мобилната опрема треба да биде заштитен со корисничко име и лозинка, а доколку опремата нуди таква опција, и со програма со повеќе фактори за автентикација. Мобилната опрема за чување податоци (дискови) и преносните медиуми (екстерни дискови, ЦД РОМ, ДВД, мемориски картички, СИМ картички) треба да бидат криптирани со силни мерки за криптирање кои, во случај на губење или кражба, ќе гарантираат дека податоците што се чуваат на нив нема да бидат читливи без овластувања за пристап.

Доколку оперативниот систем на мобилната опрема нуди криптирање на дисковите, криптирањето може да се направи преку таа опција, а во спротивно, за таа цел треба да се користат кредибилни софтверски програми кои се дизајнирани за криптирање дискови за чување податоци и преносни медиуми со примена на правилото за креирање силни лозинки. Ваквите програми треба да користат докажани алгоритми за криптирање како што се AES, Serpent, Twofish, Camellia, Kuznyechik или каскадни комбинации од истите за дополнителна безбедност со докажани хаш-функции за криптирање, на пример SHA-256, SHA-512, RIPEMD-160, итн. Кога постои таква опција, се препорачува примена на функцијата за бришење на целата содржина на медиумите за чување податоци по одреден број неуспешни обиди за овластено пристапување и тоа во однос на пристапувањето до мобилните уреди (најава и лозинка) или во однос на декриптирање на медиумот.

Кога се планира користење на компјутерски услуги во облак (cloud services) за чување на податоците, контролорите прво треба да утврдат дали давателот на таквите услуги применува соодветна заштита на личните податоци преку спроведување анализа на ризиците и треба да ги примени сите организациски мерки пропишани во ЗЗЛП и Правилникот (склучување договор, дефинирање на обврските на договорните страни, мерки што треба да се применат за заштита на личните податоци, итн.)

Чувањето податоци на мобилна опрема и преносни медиуми треба да се ограничи само на минималниот обем на податоци кои се потребни за соодветно извршување на работните задачи.

Дополнителна мерка што може да се примени се однесува на поставување филтри за приватност на екраните на мобилната опрема кога таа се користи на јавни места или да се користи мобилна опрема која веќе има интегрирани филтри за приватност.
Друга дополнителна мерка вклучува криптирање на уредите за чување на податоци, но и криптирање на податоците кои се чуваат на мобилната опрема и/или преносните уреди.
Уште една препорачана дополнителна мерка се однесува на конфигурирање на автоматско заклучување на мобилните уреди по неколку минути неактивност, како и чистење на собраните податоци веднаш штом тие ќе бидат пренесени во информатичкиот систем на контролорот.

6.1.5. Обезбедување на интерната мрежа (интранет)

Во зависност од големината на организацијата и бројот на работна опрема (компјутери, лаптопи, печатачи, вмрежени машини за копирање, итн.) и работните процеси, ваквата опрема треба да се конектира во рамките на локална мрежа. За конектирање на опремата се користат мрежни прекинувачи.

И мрежните прекинувачи мора да бидат физички заштитени од неовластено пристапување со тоа што ќе бидат сместени во внатрешниот простор на организацијата, во мрежни ормани или друг канцелариски мебел кои се обезбедени со клуч, при што физички пристап до таквите ормани имаат само овластени лица во организацијата.

Доколку е можно, се препорачува користење на мрежни прекинувачи кои може да се конфигурираат. Таквите прекинувачи дозволуваат поставување дополнителни безбедносни мерки како што е ставање вон функција на местата за мрежни кабли преку кои се конектираат уредите до моментот кога и тие треба да бидат ставени во употреба.

Исто така, таквите прекинувачи дозволуваат поставки кои утврдуваат кои уреди може да се поврзат едни со други и кои уреди имаат право за поврзување на Интернет. Доколку организацијата нема вакви мрежни прекинувачи, поврзувањето на Интернет може да се постави преку заштитниот ѕид и/или интернет-рутерите. Контролорите обезбедуваат заштита на нивната интерна мрежа преку дозвола за користење само на оние мрежни функции кои се неопходни за обработка на личните податоци, и посебно преку ограничување на пристапот до Интернет, како и преку блокирање на несуштинските услуги (на пр., интернет телефонија (VoIP), врски „точка до точка“ (peer to peer), итн.).

Интернет-рутер е уред кој овозможува конектирање на локалниот информатички систем на Интернет и истиот се добива од давателот на интернет услуги што го користи организацијата, и тоа како дел од опремата за пристап до Интернет. Бидејќи овој рутер е директно поврзан на Интернет и претставува врската меѓу дигиталната опремата на организацијата и Интернетот, од суштинско значење е тој да има соодветни нагодувања/поставки за да обезбеди квалитетна заштита од неовластено пристапување.

Давателите на интернет услуги обезбедуваат рутери со претходно дефинирано корисничко име и лозинка за администрирање или конфигурирање на поставките на интернет-рутерот. Во зависност од моделот и марката на интернет-рутерот, овие информации се добро познати па затоа мора да се променат за да се спечи лесен пристап од страна на хакери кои може да ги искористат таквите информации за администрирање на интернет-рутерот и за влегување во работниот систем на контролорот преку Интернет за да спроведат натамошни малициозни активности. Од таа причина, контролорите треба да го сменат претходно-дефинираното корисничко име и лозинка за администрирање на овој уред со единствено корисничко име и лозинка кои се познати само на вработените кои се овластени за администрирање на интернет-рутерите.

За соодветно да функционира, секој интернет-рутер содржи програма (фирмвер) која го овозможува функционирањето. Производителите на интернет-рутери постојано објавуваат нови верзии на фирмвер по откривање на грешки во работењето на таквата програма и безбедносни ранливости на поставките за програмата. Од таа причина, контролорите треба редовно да ги ажурираат рутерите со најновата официјална верзија објавена од производителот на моделот и марката на интернет-рутерот што тие го користат.

Се препорачува целата опрема од информатичкиот систем на организацијата која треба да се поврзе на Интернет преку рутер да се конектира преку мрежни кабли. Одредена опрема, на пример паметни телефони и таблети, нема можност за поврзување преку кабли, па затоа таа мора да се поврзе преку безжичната мрежа на интернет-рутерот (т.н. ви-фи мрежа). За таа цел, во поставките на

рутерот се дефинира лозинка за безжично поврзување со користење на безбедносниот протокол WPA2-PSK и креирање лозинка во согласност со препораките за силни лозинки.

Опцијата за WPS е наменета за полесно безжично поврзување на уредите на интернет-рутерот преку кликање на копчето на рутерот или преку внесување нумерички ПИН. Хакерите лесно може да го откријат ПИН-от за безжично поврзување преку WPS, па затоа оваа опција треба да биде оневозможена/исклучена.

Поновите модели на интернет-рутери имаат опција која дозволува пристап од далечина до рутерот преку Интернет (т.н. екстерен пристап). Доколку нема потреба за административен пристап до интернет-рутерот однадвор, се препорачува и оваа опција да биде оневозможена/исклучена од безбедносни причини.

Исто така, поновите модели на интернет-рутери вклучуваат опција за универзално вклучување и вчитување (UPnP), која е наменета за лесно приклучување на модерните уреди во домаќинствата (на пр., ТВ уред, конзоли за игри, итн.) за да се избегне нагодување преку прозорците за поставки со цел тие да се поврзат на рутерот. Доколку оваа опција е вклучена/овозможена, разни вируси може да дозволат административен пристап до интернет-рутерот, па затоа таа треба да биде исклучена/ оневозможена.

Пристапот до интернет-рутерот преку филтрирање на MAC-адресите на уредот (компјутер, мобилен телефон, таблет, итн.) може да се ограничи со соодветно нагодување на безбедносните поставки. MAC-адресата е дел од уредот кој му дозволува да се поврзе на некоја мрежа и обично таа се прикажува во мрежните поставки на

уредот во форма на 6 пара на цифри одделени со цртичка (01-23-45-67-89-ab) или во форма на 6 пара на цифри одделени со две точки (01: 23: 45: 67: 89: ab). Внесувањето на MAC-адресата на уредот кој има дозволен пристап до интернет-рутерот го оневозможува пристапот до сите други уреди кои не се наведени на таа листа.

Посебно внимание треба да се посвети на оневозможување пристап до деловниот интернет-рутер и со тоа оневозможување пристап до Интернет за вработените кои немаат потреба да користат Интернет како дел од нивните работни процеси, како и за трети страни (деловни партнери, клиенти, корисници, итн.). Доколку за целите на зголемување на нивото на услугите организацијата сепак сака да обезбеди пристап до Интернет за сите вработени и за трети страни преку ви-фи мрежа, тогаш таквата мрежа треба да биде одделена, не треба да дозволува пристап до деловната интерна мрежа, а интернет-рутерот треба да има опција за користење на таканаречена мрежа за гости. Ако интернет-рутерот нема таква опција, тогаш тоа треба да се направи преку друг рутер и заштитен ѕид.

Интернет-рутерот треба да биде и физички заштитен од неовластено пристапување. Се препорачува рутерот да биде сместен во затворен простор или канцелариски мебел кој е обезбеден со клуч, и до кој физички пристап имаат само овластените лица во организацијата. Доколку има потреба за пристап од далечина до системот на интерната информатичка мрежа, таквата конекција треба да се воспостави преку VPN конекција со користење на докажани и безбедни протоколи и алгоритми за криптирање (на пр. L2TP и IPSec, SSTP, итн.) и со задолжителна автентикација за овластените лица (на пр., паметна картичка, уред за генерирање еднократна лозинка - OTP, итн.)

Доколку има потреба за одржување од далечина, тогаш треба да се осигури дека интерфејсот или поставките на системот за администрирање не се директно достапни преку Интернет. Тоа може да се направи само преку VPN конекција, како што беше објаснето погоре.

Сообраќајот преку мрежата треба да се ограничи преку филтрирање на влезните/излезните комуникации на опремата со заштитни ѕидови, прокси сервери, итн. (на пр., ако организацијата има веб-сервер кој е дел од нејзината инфраструктура, тогаш веб-серверот користи HTTPS и затоа треба да се обезбеди дека влезните комуникации на овој сервер се одвиваат само преку портата 443 и дека сите други порти се блокирани).

Доколку има потреба за одржување од далечина, тогаш треба да се осигури дека интерфејсот или поставките на системот за администрирање не се директно достапни преку Интернет. Тоа може да се направи само преку VPN конекција, како што беше објаснето погоре.

Сообраќајот преку мрежата треба да се ограничи преку филтрирање на влезните/излезните комуникации на опремата со заштитни ѕидови, прокси сервери, итн. (на пр., ако организацијата има веб-сервер кој е дел од нејзината инфраструктура, тогаш веб-серверот користи HTTPS и затоа треба да се обезбеди дека влезните комуникации на овој сервер се одвиваат само преку портата 443 и дека сите други порти се блокирани).

6.1.6. Обезбедување на серверите

Имајќи предвид дека серверите обработуваат (и чуваат) голем обем на податоци, тие треба да имаат приоритет во однос на примената на соодветни технички и организациски мерки.

Правилникот пропишува дека, како минимум стандард, контролорите треба да ги применат следниве мерки:

- Строго ограничување на пристапот до серверите, серверските алатки и административните панели само за овластени вработени (администратори) кои се определени во интерните документи со кои се уредуваат овластувањата за пристап до серверите. Контролорите треба да имаат предвид дека овластените вработени треба да поседуваат соодветно знаење за администрирање на серверите. Во случај кога, поради недостиг на соодветни човечки ресурси, контролорот треба да ангажира надворешни соработници, тогаш тој треба да ги примени сите безбедносни мерки пропишани во ЗЗЛП и Правилникот (на пр., администраторот на интерната мрежа треба да има овластувања за пристап до и администрирање само на деловите од серверите кои ги администрираат корисниците на мрежата и нивните овластувања и не треба да има пристап до базите на податоци кои се чуваат на серверите или до содржината на уредите за чување на податоци).

- Овластувањата за пристап на вработените кои не се администратори на информатичкиот систем треба да бидат ограничени само на пристап до не-административните делови од серверите согласно интерните документи на контролорот и природата на работата што ја извршуваат овие вработени (на пр., контролорот донел политика дека сите вработени треба да ги зачуваат дигиталните документи во папка со датотеки на серверот, при што секој вработен има сопствена папка на серверот и овластувања за пристапување/читање/уредување само на документите во неговата/нејзината папка и нема овластувања за пристап до другите папки на серверот, додека раководителите – освен овластувањата за пристап до нивните папки – имаат овластувања и за прегледување документи од папките на вработените во неговиот/нејзиниот оддел).
- Поради огромните овластувања што администраторите на системот ги имаат во однос на информатичкиот систем, контролорот треба да донесе посебна политика за креирање лозинки за администраторите која е различна од политиката за креирање лозинки за вработените кои немаат административни привилегии (на пр., автентикација со повеќе фактори за административни сметки/налози, промена на лозинката по заминување од работното место на некој администратор, итн.).

- Поради зголемениот ризик од неовластено пристапување до серверот споредено со ризикот од неовластено пристапување до работните станици, врз основа на спроведената анализа на ризиците сите ажурирања на серверот (на пр., ажурирање на оперативниот систем, влезно-излезниот систем – BIOS, серверот со база на податоци, работните програми, итн.) треба да се прават во редовни интервали кои не се подолги од една недела. За постигнување на ова цел и кога е можно, треба да се применува авто-ажурирање (на пр., авто-ажурирање на оперативниот систем, на серверот со бази на податоци, итн.).
- Според спроведената анализа на ризиците, контролорите треба да креираат резервни копии на серверот во редовни интервали. Исто така, контролорите треба да прават редовни проверки на функцијата за повратување на системот за да утврдат дали содржината на серверот може да биде соодветно вратена во нормална состојба (без загуба на податоци) во случај на инцидент.
- Доколку серверот се користи за онлајн размена на податоци, како минимум стандард, таквата комуникација треба да биде криптирана со протокол кој е дизајниран за безбедни комуникации преку компјутерска мрежа (на пр., TLS1.3). Исто така, контролорот треба да прави годишни проверки на конфигурацијата на криптографскиот протокол за да види дали тие се правилно нагодени/поставени или секогаш кога има јавно достапни информации за големи безбедносни ранливости на конкретниот протокол, со цел да се осигури ефективноста на заштитата.

Кога серверот се користи за чување бази на податоци, за целите на безбедно администрирање на базите на податоци, како минимум стандард, контролорот треба да користи персонализирани профили за пристап до истите и креирање конкретни кориснички имиња за секоја апликација/програма. Друга мерка што треба да се примени како минимум стандард во однос на серверите со бази на податоци се однесува на соодветна заштита од напади со инјектирање кодови во базите на податоци (SQL injection).

6.1.6. Обезбедување на серверите

Кога серверот се користи за чување бази на податоци, за целите на безбедно администрирање на базите на податоци, како минимум стандард, контролорот треба да користи персонализирани профили за пристап до истите и креирање конкретни кориснички имиња за секоја апликација/програма. Друга мерка што треба да се примени како минимум стандард во однос на серверите со бази на податоци се однесува на соодветна заштита од напади со инјектирање кодови во базите на податоци (SQL injection).

6.1.7. Обезбедување на веб-страниците

Кога користат веб-страници контролорите треба да обезбедат дека тие се заштитени од неовластени пристапување, посебно во случај на веб-страници кои обработуваат лични податоци (на пр., колачиња, овластувања за пристап до деловите од веб-страницата кои налагаат такви овластувања, пополнување формулари кои обработуваат лични податоци, итн.).

За да ги заштитат своите веб-страници контролорите треба да ги преземат следниве чекори:

1. **Водење сметка дека софтверот и сите приклучоци се ажурирани**

Ажурирањата се од витално значење за здравјето и безбедноста на една веб-страница, бидејќи ако софтверот и приклучоците не се ажурирани тогаш веб-страницата не е безбедна. Ажурираните верзии често вклучуваат зајакнувања на безбедноста и поправки на ранливостите на ваквите програми. Од таа причина, контролорите треба да проверуваат достапност на ажурирани верзии и да додадат приклучок со известување за нови/ажурирани верзии. Некои платформи дозволуваат автоматско ажурирање, и тоа е уште една опција која овозможува безбедност на веб-страницата.

2. **Додавање на сертификати за HTTPS и SSL**

За да се осигурат дека веб-страницата е безбедна, посебно кога од посетителите се бара да се регистрираат или да се најават или кога прават трансакции, потребно е веб-страницата да има безбеден URL (односно линк до веб-страницата, на пример: https://mywebsite.mk) и конекцијата да биде криптирана. Зошто треба да се користи HTTPS наместо HTTP протокол? Имено, HTTPS (Hypertext Transfer Protocol Secure) е протокол кој се користи за обезбедување безбедност преку Интернет. Тој спречува пресретнување на комуникацијата и прекини при пренесување на содржината.

За да се осигури безбедна онлајн комуникацијата, веб-страницата треба да има SSL-сертификат. SSL (Secure Sockets Layer) ги криптира информациите кои се пренесуваат преку Интернет од веб-страницата до опремата на корисниците со цел да спречи нивно читање од трети страни за време на преносот. Исто така, овој сертификат оневозможува пристап до податоците без соодветно овластување.

3. Забрана на Интернет комуникациските порти кои не се неопходни

Комуникациските порти треба да бидат ограничени само на оние кои се строго потребни за соодветно функционирање на веб-страницата. На пример, доколку веб-серверот прифаќа конекции само преку HTTPS протокол, сообраќај преку IP-мрежа треба да се дозволи само преку портата 443, а сите други порти треба да бидат блокирани.

4.Избор на силна лозинка

Системот за управување со содржина (CMS) налага најава и за таа цел треба да се избере силна лозинка во согласност со одредбите дадени во член 11 од Правилникот, па затоа се препорачува креирање силна лозинка, онака како што е објаснето во овој водич. Исто така, лозинките не треба да се чуваат во рамките на регистрите на веб-страницата.

5.Користење безбеден давател на услуги за хостирање веб-страници

За да илустрираме што е име на веб-домен и што е веб-хост, т.е. веб-домаќин, доменот на вашата веб-страница сметајте го како улица на адресата, а веб-хостот како парцелата на која вашата веб-страница постои во онлајн просторот.

Исто како што се проверува парцелата за да се обезбеди дека таа е доволно безбедна за вашата куќа, така треба да се провери и потенцијалниот давател на услуги за веб-хостирање за да се види дали тој е вистинскиот за потребите на контролорот. При избирањето безбеден давател на вакви услуги треба да се разгледа/испита следново:

- Дали давателот на услуги нуди протокол за безбеден пренос на датотеки (SFTP)?
- Дали е исклучена опцијата за користење протокол за пренос на датотеки (FTP) од непознат корисник?
- Дали давателот на услуги користи руткит скенер (Rootkit Scanner)?
- Дали давателот на услуги нуди креирање резервна копија на датотеките?

6.Утврдување на овластувањата за администрирање и евиденција на пристапот од корисници

Како што е уредено во член 11 од Правилникот, како дел од интерната документација контролорот утврдува кој има права за администрирање на веб-страницата. Исто така, согласно член 15 од од Правилникот, контролорот води евиденција за пристапот до веб-страницата од страна на корисници. Ваквата евиденција треба да ги содржи следниве информации: име/презиме на овластеното лице, работни станици од каде е пристапено до информатичкиот систем, датум и време на пристапувањето, личните податоци до кои било пристапено, видот на пристап со акцијата што била презема во однос на обработка на личните податоци, запис за автентикација на пристапувањето, запис за секој неовластен пристап, и запис за автоматско одбивање на пристапот од страна на информатичкиот систем.

7.Менување на стандардните поставки на CMS-системот и осигурување безбедност на регистрите на веб-страницата до степен до кој тоа е можно

Највообичаените напади на веб-страниците се целосно автоматизирани. Она на што многу напаѓачи се надеваат е корисниците да ги имаат оставено нивните CMS-системи со фабрички поставки. Кога хакерите напаѓаат некоја веб-страница, тие сакаат да добијат пристап до базата на податоци или регистрите за администрирање. Овие две работи треба да бидат во фокусот на контролорите кога ги обезбедуваат нивните веб-страници. Треба да се запомни дека сите хакерски напади се секогаш насочени кон тие две области. Хакерите често ги скенираат регистрите со имиња како „админ“ или „најава“. Доколку постои таква опција, овие регистри треба да се преименуваат. Ако не може да бидат преименувани, тогаш треба да се смени дозволата за пристап до нив и до други осетливи датотеки. Бришење или уредување на папките и датотеките треба да биде ограничено, односно оневозможено без дозвола од контролорот.

8.Создавање резервна/сигурносна копија од веб-страницата

Како што беше наведено во однос на креирањето резервни копии од податоците, постојат различни причини кои може да доведат до загуба на податоци на веб-страницата. На пример, веб-серверот може да падне или да биде инфициран со вирус кој ќе ги уништи податоците, некој вработен може намерно или ненамерно да ги избрише податоците, податоците може да бидат уништени од хакерски напад, или може да се случи

природна катастрофа (пожар, земјотрес, поплава, итн.). Од тие причини веб-страниците треба да имаат резервна копија. Ваква копија треба да постои за целата веб-страница и нејзините датотеки, и тоа на посебна локација, како што е регулирано во член 22 од Правилникот и како што е наведено во поглавјето за правење резервни копии од овој водич.

9.Познавање на датотеките за конфигурација на веб-серверот

Вработените кои имаа овластувања за администрирање на веб-страницата треба да ги познаваат датотеките за конфигурација на веб-серверот каде е сместена веб-страницата. Тие може да се најдат во главниот регистер на веб-страницата и овозможуваат администрирање на серверските правила. Различни веб-сервери користат различен вид на датотеки, на пример, веб-серверите Apache користат датотеки од видот .htaccess, додека серверите Nginx користат nginx.conf, серверите на Microsoft IIS користат датотеки од видот web.config.

10.Користење на заштитен ѕид за веб-апликации

На веб-страницата треба да се користи заштитен ѕид за веб-апликации (WAF). Тој треба да биде поставен меѓу серверот на веб-страницата и податочната конекција, а целта на ваквиот заштитен ѕид е читање секој бит на податоци кои поминуваат преку него за да ја заштити веб-страницата. Исто така, заштитниот ѕид може да филтрира други видови на непосакуван сообраќај преку Интернет, на пример, спамови и малициозни ботови.

11.Зајакнување на безбедноста на мрежата

Контролорите треба да ја анализираат безбедноста на нивната мрежа. Вработените со овластувања за администрирање на веб-страницата може ненамерно да создадат небезбедна патека до веб-страницата. За да се спречи овозможување таков пристап до серверот на веб-страницата, се препорачува контролорите да ги преземат следниве чекори:

- поставки за најавување преку компјутер кое истекува по одреден краток период на неактивност;
- поставки за системот да ги известува корисниците за промена на лозинката на секои три месеци;
- обезбедување дека сите уреди кои се приклучени на мрежата се скенираат за малициозни програми секој пат кога тие се приклучуваат на мрежата.

6.1.8. Спречување, реакција и повратување на системот по инциденти (обезбедување континуитет)

Врз основа на спроведената анализа на ризици и ризиците кои биле утврдени и кои би можеле да го нарушат континуитетот на процесите кои подразбираат обработка на лични податоци и веројатноста тие да се случат, контролорите треба да изготват планови за управување со континуитетот на нивните информатички системи. Овие планови треба да вклучат акции што се преземаат за спречување такви ризици, список на овластени лица кои се одговорни за спречување на секој можен ризик што бил идентификуван како закана за континуитетот на обработката. Како дел од истиот или како посебен план, контролорите треба да утврдат акции кои се преземаат во случај некој ризик да се материјализира, вклучително и список на овластени лица кои се одговорни за повратување на системот во нормална состојба, категории на лични податоци кои ќе се повратат или категории на лични податоци кои ќе бидат рачно внесени во системот како дел од неговото повратување во почетната состојба за секој ризик што бил идентификуван како можна закана за континуитетот на обработката со цел системот да се врати во нормална состојба колку што е можно порано. Сите вработени кај контролорот треба да бидат запознаени со плановите за управување со континуитетот на информатичкиот систем, како и нивната улога во рамките на тој план за да се избегне одложување на постапките за реакција и повратување. Контролорите обезбедуваат дека овластените лица, обработувачите и под-обработувачите се свесни за случаите кога треба да се алармира и да се поднесе известување за инциденти.

Спречувањето инциденти опфаќа мерки и контроли, онака како што се пропишани во Правилникот, кои се базираат на спроведената анализа на ризици и се наведени во интерните документи на контролорот (на пример, користење уреди за непрекинато снабдување со електрична енергија за да се заштити опремата која се користи за обработка на податоци во случај на пад на системот за снабдување со електрична енергија, РАИД технологија (резервна низа од евтини дискови), редовно тестирање на функционирањето на уредите, редовна едукација на вработените за заштита на личните податоци, итн.).

6.1.9. Резервни копии и повратување на личните податоци (обезбедување континуитет)

Постојат различни причини што кои може да доведат до загуба на податоците во некоја организација, на пример, расипување на дискот на компјутер, кршење на паметен телефон или таблет, инфицирање на компјутер или мобилни уреди со вирус кој ги уништува податоците, намерно или ненамерно бришење на податоци од страна на вработен, уништување на податоците со хакерски напад, природна катастрофа (пожар, земјотрес, поплава) итн. Од тие причини, потребно е да постои резервна копија на податоците која ѝ овозможува на организацијата непречено да работи и ја прави способна да продолжи со работата и во такви непредвидени околности.

Врз основа на спроведената анализа на ризиците, квалитетното создавање резервни копии на податоците налага примена на следниве чекори:

1. Идентификување на податоците за кои се прави резервна копија

Во зависност од дејноста, секоја организација одлучува кои податоци се важни за нејзино непречено работење и за кои задолжително треба да постои резервна копија. Во суштина, резервни копии треба да се направат од сите податоци кои не може да бидат едноставно и лесно повратени или не можат да бидат заменети во случај на губење.

2. Утврдување на медиумот за чување на резервните копии

Изборот на медиум за резервни копии зависи од важноста на податоци за кои се прави резервна копија, роковите за чување на резервната копија, колку често се прави резервна копија, како и способностите на организацијата за правење резервни копии. Медиумите за чување резервни копии може да бидат ЦД/ДВД, УСБ уред, екстерен диск, магнетна лента, систем со дискови, резервна копија во облак, итн.

3. Утврдување на локацијата на резервните копии од податоците

Медиумите со резервни копии на податоците треба да се чуваат на безбедна локација (на пр., заклучени во огноотпорна фиока или орман) до која пристап имаат само овластените лица во организацијата. Во идеални услови, медиумите со резервни копии треба да се чуваат на локација која е безбедна и доволно оддалечена од оригиналната локација на податоци што ќе овозможи безбедно повратување на податоци и нормално работење во случај на природна катастрофа или друга штета од огромен обем.

4. Утврдување на рокот и начинот за чување на резервните копии

Рокот за чување и начинот за креирање на резервните копии (дали се прави резервна копија на сите податоци или само на оние кои биле изменети, т.е. на новите податоци) се утврдува во зависност од дефиницијата на зачестеноста на менување на податоци и обемот на податоци кои треба да се чуваат. Ваквите резервни копии може да се прават веднаш по појавата на податоци, периодично во текот на еден ден, еднаш дневно, еднаш седмично, два пати месечно, еднаш месечно, еднаш на секои шест месеци или еднаш годишно. Во практика, периодични резервни копии обично се прават за датотеки кои биле креирани од текстуална или табеларна програма, за бази на податоци кои се користат од страна на компјутерски програми, е-пошта, итн., додека резервна копија на компјутерските програми и оперативните системи се прави пред големи ажурирања или инсталирање на понови верзии. На пример, по завршување на работниот ден се прави резервна копија на датотеките во кои е направена промена, седмична резервна копија се прави на конкретно специфицирани датотеки, е-пошта и бази на податоци кои не се менуваат често, и месечна, полугодишна или годишна резервна копија се прави за целиот компјутер.

5. Тестирање на резервните копии на податоците

За да се осигури дека податоците може успешно да се повратат и користат од резервната копија, од таквата копија треба да се направи нова резервна копија и истата треба да се тестира.

Тестирање на резервната копија се препорачува во следниве случаи:

- по креирањето на првата резервна копија треба да се осигури дека таа е коректно направена и дека програмите, базите на податоци и/или датотеките може да биде безбедно повратени;

- по набавка на нов компјутер треба да се осигури дека сите потребни датотеки, бази на податоци и програми може да се користат на новиот компјутер;
- по големо ажурирање на постојниот оперативен систем или по ажурирање со понова верзија на оперативниот систем треба да се обезбеди дека промените во системот не влијаат на соодветното функционирање на програмата и на непреченото користење на датотеките и базите на податоци;
- по ажурирање на програмата или инсталирање на програма која креира текстуални, табеларни или други видови на датотеки во кои се чуваат податоци треба да се обезбеди дека датотеките може соодветно да се отворат и да се користат;
- периодично се проверува дека медиумите на кои се чуваат резервните копии од податоците не се оштетени.

Од големината на организацијата, обемот на податоците кои се обработуваа и сложеноста на деловните процеси зависи и начинот на кој се прават резервни копии од податоците. На пример, фризерски салон кој користи еден компјутер за обработка на податоци кои се чуваат во текстуални или табеларни датотеки може да користи програма што е интегрирана во оперативниот систем или некоја од програмите за компресирање за создавање датотека која служи како резервна копија, додека за чување на истата може да користи преносен диск или УСБ уред со соодветен капацитет. Се разбира, несомнено е дека треба да се применат сите мерки за заштита на личните податоци кои се пропишани за таквиот софтвер или медиум за чување на податоци. Од друга страна, продавница за резервни делови на автомобили која користи различни програми за чување на податоци во база на податоци и која обработува голем обем на податоци можеби треба да набави програма наменета за

автоматско креирање резервни копии, како и медиум за чување на податоци со поголем капацитет од преносен диск или дури диск за чување на податоци. Доколку некоја организација одлучи креирањето на резервни копии да го довери на надворешен соработник кој обезбедува компјутерски услуги и чување податоци во облак, треба да се провери дали давателот на ваквите услуги обезбедува и гарантира високо ниво на безбедност за податоците кои се чуваат на таков начин, односно дали податоците се чуваат во криптирана форма, дали давателот на услуги применува високо ниво на заштита од неовластено пристапување до податоците, дали обезбедува безбедна интернет конекција (VPN) меѓу корисниците и облакот, и дали ги применува сите други технички и организациски мерки кои обезбедуваат еднакво ниво на заштита на личните податоци.

6.1.10. Начин на архивирање и чување на податоците

Постојат одредени лични податоци кои не се потребни за непосредна и секојдневна обработка и кои, поради правилата пропишани со законот што ја опфаќа предметната обработка, треба да бидат архивирани или чувани во одреден законски период. На пример, компанија која обезбедува услуги за фиксна телефонија и склучува двегодишен договор со корисникот. Договорот и личните податоци треба да се обработуваат и чуваат до исполнување на целта, односно до истекот на договорот (плус период за застарување на побарувањата), а фактурите се чуваат како сметководствени документи во согласност со законските прописи. Друг пример се личните податоци на вработени кои ги обработуваат одделенијата за човечки ресурси и за финансии. Откако лицето повеќе не е вработено во организацијата, овие одделенија треба да архивираат одредени податоци пропишани со закон и да ги чуваат за одреден период дефиниран во тој закон (одделението за човечки ресурси го применува

Законот за работи односи, додека одделението за финансии го применува Законот за плати).

Таквите лични податоци треба да се архивираат на безбеден начин, посебно кога архивираните податоци се од осетлива природа (на пр., посебни категории на лични податоци или лични податоци на деца) или тие може сериозно да влијаат на правата на субјектите на лични податоци во случај да бидат компромитирани.

Со оглед на тоа дека личните податоци кои треба да се архивираат може да се чуваат во дигитална и/или хартиена форма, за да обезбеди соодветно архивирање и чување на таквите податоци контролорот воспоставува постапки за управување со архивска граѓа за таквите податоци, како и каде се чуваат, како и во кои услови може да се пристапи до истите.

Контролорот мора да донесе соодветен документ насловен „список (преглед) на роковите за чување на личните податоци“ кој содржи информации за моментот кога почнува периодот/рокот за чување, причините за чување на личните податоци, правниот основ за чување на личните податоци и сопственикот на таквите податоци. Исто така, контролорот треба да врши годишна проверка и усогласување на овој документ со промените кои настанале во неговото работење и со законските барања за чување на личните податоци.

6.1.11. Криптирање на личните податоци

Криптирање на обработката на лични податоци треба да се земе предвид од аспект на криптирање на пристапот до личните податоци, преносот на личните податоци преку електронски комуникациски мрежи и чувањето на лични податоци во криптирана форма.

За секој од горенаведените аспекти, контролорите треба да користат соодветно признати и безбедни алгоритми за криптирање кои се применуваат за конкретниот аспект и се темелат на спроведената анализа на ризиците.

Од аспект на криптирање на пристапот до оперативните системи за обработка на лични податоци, постојат комерцијални програми и системи за управување кои применуваат соодветни алгоритми за криптирање за чување на кориснички имиња и лозинки и може да се користат за овластено пристапување. Контролорите треба да преземат соодветни мерки за примена на признати и безбедни алгоритми за криптирање (на пр., bcrypt, scrypt или PBKDF2) за целите на чување лозинки. Заедно со компанијата што го развива нивниот софтвер, контролорите треба да проверат дали се применуваат соодветни алгоритми за помнење на овластени кориснички имиња и лозинки на безбеден начин. Во таа смисла и врз основа на спроведена анализа на ризиците, контролорите треба да размислат за тоа дека и дисковите за складирање што се дел од мобилната опрема (дискови) и преносните медиуми (надворешни дискови, УСБ уреди, ЦД РОМ, ДВД, мемориски картички, СИМ картички) мора да имаат силни мерки за криптирање во случај на губење, со цел податоци кои се чуваат на нив да не може да бидат прочитани без овластен пристап. Доколку оперативниот систем на мобилната опрема нуди криптирање на дискови, таквата опција треба да се искористи, а во спротивно, контролорите треба да користат софтвер од доверба дизајниран за користење на дискови и преносни медиуми за чување податоци кои ги применуваат правилата за креирање силни лозинки. Ваквите апликации треба да користат веќе докажани алгоритми за криптирање, на пример,

AES, Serpent, Twofish, Camellia, Kuznyechik или каскадни комбинации на истите за дополнителна безбедност со докажани криптографски хаш-функции (hash), на пример SHA-256, SHA-512, RIPEMD-160, итн.

Друг аспект е криптирањето на лични податоци кои се пренесуваат преку електронските комуникациски мрежи. Врз основа на спроведената анализа на ризиците, контролорите донесуваат одлука дали и локалната мрежна комуникација треба да биде криптирана, во најмала рака во случај на онлајн размена на податоци меѓу веб-страница и веб-сервер. Како минимум стандард, таквата комуникација треба да биде криптирана со криптографски протокол дизајниран да овозможи безбедност на комуникациите што се одвиваат преку компјутерска мрежа (на пр., TLS1.3). Освен тоа, доколку има потреба за пристап од далечина преку Интернет до интерната информатичка мрежа или има потреба за воспоставување врска преку Интернет помеѓу две организации на одделни локации, таквата врска треба да се воспостави преку VPN конекција со примена на признати и безбедни протоколи и алгоритми за криптирање (на пр., L2TP и IPSec, SSTP, итн.) со задолжителна автентикација на овластените лица (на пр., паметна картичка, уред за генерирање еднократна лозинка, итн.).

Третиот аспект е чување на личните податоци во криптирана форма. Врз основа на спроведената анализа на ризици, контролорот треба да утврди кои лични податоци треба да се чуваат во криптирана форма со цел ваквите податоци да бидат некорисни во случај на неовластено пристапување до местото на кое се чуваат без познавање на алгоритамот или клучот за декриптирање.

Алгоритми за криптирање треба да се вградат во кодот на деловните програми, а во зависност од спроведената анализа на ризиците, треба да се користат соодветни алгоритми за криптирање (на пр., AES или AES-CBC за симетриско криптирање, RSA-OAEP v2.1 за асимтериско криптирање, итн.) и за декриптирање (на пр., DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, и 256-bit AES, итн.). Како минимум стандард, се препорачува во криптирана форма да се чуваат посебните категории на лични податоци, личните податоци на деца или личните податоци кои може да имаат сериозно влијание врз правата на субјектите на лични податоци во случај тие да бидат компромитирани.

Контролорот може да ги користи услугите на обработувач за чување на податоците надвор од неговите простории и/или да користи софтверски програми за обработка кои може да бидат физички лоцирани, хостирани и администрирани надвор од неговите простории. Во таков случај, контролорот треба да ги уреди взаемните права и обврски со обработувачот во форма на пишан договор, кој мора да вклучи и одредби за мерки за безбедност на личните податоци во согласност со прописите за заштита на личните податоци. Пред склучување на договорот, контролорот треба да провери дали обработувачот применува соодветни технички и организациски мерки за заштита на личните податоци, и според ова поглавје, дали ги исполнува барањата за криптирање од сите аспекти наведени погоре. Врз основа на спроведената анализа на ризиците, контролорот треба да утврди дали сите лични податоци треба да бидат криптирани пред нивното чување во информатичкиот систем на обработувачот.

Контролорот донесува интерни постапки кои го пропишуваат начинот за управување со тајните клучеви и сертификати, земајќи го превид управувањето со ризиците поврзани со заборавени лозинки.

6.1.12. Размена на податоци преку електронска пошта

Електронската пошта (е-пошта), а посебно електронската пошта преку јавни сервиси (Gmail, Hotmail, Yahoo Mail...) е многу небезбеден начин за комуникација и размена на податоци. Иако комуникацијата преку е-пошта може да биде криптирана со протоколот SSL/TLS, ако серверот за е-пошта на испраќачот или на примателот не поддржува таков протокол, содржината на е-поштата ќе се пренесе како некриптирана. Исто така, електронските пораки се чуваат на серверот за е-пошта во некриптирана форма.

Како мерка за заштита, целата содржина на е-пораките може да се криптира со кредибилна алатка за криптирање (Public Key Infrastructure) наменета за е-пошта (на пр., PGP или S/MIME). Со користење на тој метод, примателот треба да креира јавен клуч за криптирање и јавен клуч за декриптирање. Испраќачот ја криптира е-пораката со јавниот клуч на примателот, а потоа примателот ја декриптира содржината со друг приватен клуч.

Подолу следуваат примери за други мерки кои треба да се земат предвид при испраќање е-пошта:

- текстот на самата е-порака да не содржи лични податоци кои не се однесуваат на деловни контакт податоци, и посебно да не содржи лични податоци на трети страни (лица кои не се испраќачот или примателот);
- личните податоци кои се чуваат во дигитална форма да бидат криптирани со софтверска програма за компресирање податоци која има способност за криптирање на содржината на архивата со кредибилни алгоритми за -текстот на самата е-порака да не содржи лични податоци кои не се однесуваат на деловни контакт податоци, и посебно да не содржи лични податоци на трети страни (лица кои не се испраќачот или примателот);
- личните податоци кои се чуваат во дигитална форма да бидат криптирани со софтверска програма за компресирање податоци која има способност за криптирање на содржината на архивата со кредибилни алгоритми за

6.1.13. Физичка безбедност

Кога некоја организација воспоставува заштитни мерки, таа треба да размисли и за воспоставување соодветни физички мерки за заштита од неовластено пристап до нејзините простории и до опремата што ја користи.

При воспоставување на мерки за физичка безбедност, предвид треба да се земе следново:

- обезбедување на објектот од неовластен пристап вон работните часови на организацијата (на пр., преку поставување аларми за кражба и систем за видео надзор, доколку проценката на ризикот покаже дека тоа е потребно и оправдано), и периодична проверка на нивата функционалност;
- ограничување на пристапот до опремата на која се чуваат личните податоци (компјутерски сервери, диск системи, екстерни дискови, податоци во хартиена форма, итн.) преку сместување на таквата опрема во соодветен канцелариски мебел (на пр., полици за сервери за дигиталните податоци, метални ормани за податоците во хартиена форма) и канцелариски соби (на пр., соба за сервери) или простории/ канцеларии кои се соодветно заштитени од неовластен пристап (на пр., со користење клучеви или паметни картички кои им се даваат само на овластените лица);
- ограничување на пристапот до канцелариските мебел (на пр., полици за сервери или метални ормани) и канцелариски соби (т.е. соба за сервер или архива) каде се чуваат личните и други доверливи податоци (на пр., простории кои водат до собата за сервери каде се сместени компјутерите/серверите на кои се чуваат податоци, простории/соби или ормани во кои се чуваат податоци во хартиена форма);
- водење евиденција за пристапот до просториите каде се сместени серверите кои содржат лични податоци во дигитална форма или просториите каде се чуваат податоци во хартиена форма и, кога е соодветно, водење евиденција за обидите за неовластено пристапување до овие области;

- бидејќи компјутерските сервери, дисковите и другата дигитална опрема за чување на голем обем на податоци подлежи на посериозни ризици, потребни се повеќе безбедносни мерки во просториите и собите за серверите каде е сместена таква опрема. Земајќи ги предвид најсовремените технологии, трошокот за спроведување и природата, обемот, контекстот и целта на обработката, како и ризиците со различна веројатност и сериозност по правата и слободите на физичките лица кои произлегуваат од обработката, при утврдување на средствата за обработка и при самата обработка на лични податоци контролорите применуваат соодветни технички мерки за заштита на опремата и просториите во кои е сместена опремата од природни незгоди како што се пожари, чад, вода, прашина, вибрации, хемиски супстанци, прекини во снабдувањето со електрична енергија и електромагнетско зрачење (на пр., собата за сервери треба да биде изградена со противпожарна заштита, а кога тоа не е применливо, тогаш таа треба да биде заштитена со соодветен противпожарен систем соодветен за електронска опрема; да биде изградена од водоотпорен материјал, а кога тоа не е применливо, тогаш таа треба да има покренат антистатичен под и систем за истекување; да биде опремена со систем за ладење за кој постои резервен систем, т.е. климатизација; да има непрекинато снабдување со електрична енергија за да се обезбеди континуитет или барем безбедно исклучување на целата опремата до враќање на снабдувањето со електрична енергија);

- примена на соодветни технички мерки како оние дадени погоре, но приспособени за заштита на податоците кои се чуваат во хартиена форма (на пр., просториите треба да бидат изградени од огноотпорен материјал, а кога тоа не е применливо, тогаш тие треба да бидат опремени со противпожарен систем кој е соодветен за заштита на хартија; да бидат изградени со водоотпорен материјал, а кога тоа не е применливо, тогаш треба да имаат покренат под и систем за истекување; да имаат систем за климатизирање за да се одржува соодветно ниво на влажност и температура во просториите, итн.);
- сместување на другата мрежна комуникациска опрема (на пр., интернет-рутер, мрежни прекинувачи, итн.) во соодветен канцелариски мебел (на пр., полици за сервери) и/или во простории кои се соодветно заштитени од неовластено пристапување (на пр., со клуч или паметна картичка);
- обезбедување дека целата суштинска опрема од информатичкиот систем (сервери, компјутери, опрема за локалната мрежа, мрежни уреди како што се печатачи, итн.) има непрекинато снабдување со електрична енергија за да се осигури континуитет или барем безбедно исклучување на целата опремата до враќање на снабдувањето со електрична енергија);

- канцелариската опрема (компјутери, печатачи, машини за копирање, итн.) што се користи за интерактивна работа со клиентите на деловните услуги да биде физички одделена од корисниците или барем да се отежни пристапот на клиентите до таквата опрема и до податоците (на пр., физичка препрека меѓу корисниците и работниот простор), односно да постои шалтер кој го спречува корисникот да пристапи до опремата, печатачите, машините за копирање и канцеларискиот мебел во којшто се чуваат податоците во хартиена форма со тоа што тие ќе бидат доволно далеку за корисникот да нема увид во податоци, мониторот на компјутерот е свртен со задната страна кон корисникот, итн.);
- примена на правилото „чисто биро“ на начин кој обезбедува дека сите важни документи, доверливи писма, папки, книги, итн., се отстранети од бирото и заклучени кога не се користат или кога вработениот ја напушта неговата работна станица. Ова е една од врвните стратегии што се применуваат за намалување на ризикот од нарушување на безбедноста на личните податоци. Освен тоа, во работниот простор не треба да има самолепливи ливчиња со белешки, документи со информации како што се лична карта на корисникот, лозинки или броеви на банкарска сметка, и треба да биде ослободена од сите несуштински документи.

Контролорите може да користат услуги на обработувач за чување на личните податоци надвор од нивните простории и/или да користат програми за обработка кои може да бидат физички лоцирани, хостирани и администрирани надвор од нивните простории (на пр., веб-серверот на организацијата може да биде хостиран надвор од просториите на контролорот).

Во таков случај, контролорот треба да ги регулира взаемните права и обврски со обработувачот во форма на пишан договор кој мора да вклучи одредби за мерки за безбедност на личните податоци во согласност со прописите за заштита на личните податоци.

Пред склучувањето на договорот, контролорот треба да провери дали обработувачот применува соодветни технички и организациски мерки за заштита на личните податоци.

6.1.14. Контрола на информатичкиот систем и инфраструктура

Како што беше претходно наведено, сите технички и организациски мерки пропишани во ЗЗЛП и Правилникот, како и во интерните документи на контролорот кои се однесуваат на технички и организациски мерки, нема да имаат никаков ефект доколку сите вработени кај контролорот не ги применуваат редовно. Оттука, документацијата за технички и организациски мерки на контролорот мора да вклучи и постапка за овластување на офицерот за заштита на личните податоци за тој/таа да може да врши периодични контроли за следење на усогласеноста на контролорот со прописите за заштита на личните податоци и донесената документација за технички и организациски мерки. Информатичкиот систем и инфраструктура на контролорот мора да биде предмет на интерна контрола за да се провери дали се спроведуваат постапките и инструкциите дадени во правилата и политиките за безбедност на личните податоци и дали тие се во согласност со прописите за заштита на личните податоци.

6.1.15. Управување со обработувачи и ангажирање на обработувачи

Доколку контролорот одлучи да користи некаква обработка на лични податоци што ја нуди друг деловен субјект (обработувач), тогаш тој е должен да спроведе постапка за избор на соодветен обработувач која треба да го предвиди следново:

- анализа на потенцијалните обработувачи во однос на нивните технички и организациски мерки кои гарантираат дека обработката се врши во согласност со условите пропишани во прописите за заштита на личните податоци и нивото на заштита кое е соодветно на личните податоци што ги обработува контролорот, и гарантираат заштита на правата на субјектите на лични податоци;
- анализа на ризиците врз работењето на контролорот кои можат да произлезат од обработката на личните податоци од страна на обработувачи.

Дополнително на воспоставување постапка за избор на обработувачи, контролорите се должни да воспостават процеси за управување со користењето на услугите кои ги обезбедуваат обработувачите и во однос на управувањето со обработката и да обезбедат извршување на договорните обврски и одговорности од страна на ангажираните обработувачи.

Оттука, контролорите може да ги делегираат задачите поврзани со обработка на личните податоци во нивно име само на обработувачи кои обезбедуваат доволно гаранции, особено во однос на потребното знаење, безбедност и ресурси во областа на заштита на личните податоци.

Дури и кога делегирале задачи на обработувачот кои се дел од работата што ја извршува контролорот и се однесуваат на обработка на лични податоци, контролорите се обврзани да обезбедат контрола врз таквата обработка во однос на безбедноста на личните податоци, при што податоците се обработуваат со примена на соодветни безбедносни мерки.

Взаемните права и обврски на контролорот и обработувачот мора да бидат регулирани преку пишан договор, а пред потпишувањето на таквиот договор контролорот е должен од давателот на услугата (обработувачот) да побара увид во неговата политика за безбедност која се однесува на информатичкиот систем и инфраструктура кои се користат за обработка на лични податоци во име на контролорот, при што таквата политика за безбедност треба да содржи информации кои гарантираат безбедност на личните податоци, односно:

- дали и како се криптираат личните податоци според нивната осетливост;
- дали постојат постапки кои гарантираат дека ниту едно лице нема да има неовластен пристап до податоците;
- дали и како се криптираат личните податоци кои се пренесуваат;
- гаранции во однос на следливоста (логови, информациски траги, итн.)ч
- управување со овластувања за пристап;
- автентикација;
- други безбедносни мерки за обработката на лични податоци кои се соодветни за предметната обработка на лични податоци.

Потоа, контролорот и обработувачот склучуваат договор кој содржи одредби што се однесуваат на следново:

- предмет, времетраење и цел на обработката на лични податоци;
- обврските на обработувачот за примена на технички и организациски мерки за да се осигури безбедност на обработката;
- обврски поврзани со доверливоста на дадените лични податоци;
- минимум стандарди за автентикација на овластените лица;
- услови за враќање на податоци и/или уништување на податоците по истекувањето или прекинувањето на договорот;
- правила за управување со инциденти и поднесување известување до контролорот во случај на нарушување на безбедноста на личните податоци;
- обврската на обработувачот да преземе дејство по инструкциите дадени од страна на контролорот;
- други обврски и одговорности во согласност со прописите за заштита на личните податоци и усвоената документација за технички и организациски мерки.

6.2. Високо ниво на технички мерки

Освен стандардното ниво на технички мерки, врз основа на спроведената анализа на ризици, контролорите применуваат и дополнителни безбедносни мерки со цел да покажат дополнителна усогласеност со прописите и добрите практики за заштита на личните податоци.

Високото ниво на технички мерки е пропишано во член 38 од Правилникот и се однесува на дополнителни мерки поврзани со управувањето со лозинки. Имено, првата мерка од високо ниво се однесува на користење на алатки за управување со лозинки за да се обезбеди дека различните лозинки за различни услуги или софтверски програми соодветно се чуваат и за таа цел треба да користи главна лозинка за пристап до сите лозинки којашто треба да биде од зајакната сложеност, т.е. треба да претставува комбинација од најмалку 12 алфанумерички карактери (големи и мали букви, симболи, бројки и специјални интерпункциски знаци) и треба да се менува во редовен интервал кој не е подолг од 30 дена. Друга мерка од високо ниво која се базира на спроведената анализа на ризици се однесува на случаи кога одредени овластени лица имаат повисоко ниво на привилегии (на пр., администраторот на информатичкиот систем или лицата кои креираат и користат главна лозинка), при што контролорите може да го дисперзираат ризикот преку управување со лозинки со дополнителни фактори на повеќе овластени лица со пониско ниво на привилегии согласно правилото н-2 (на пр., информацијата за лозинката се споделува со две или повеќе лица за заедничка најава, а секој од нив знае само дел од лозинката, или едно овластено лице ја знае лозинката, а друго лице ја поседува и ја користи паметната картичка).

Член 39 од Правилникот уредува уште една техничка мерка од високо ниво која се однесува на сертификација на заштитата на личните податоци. Дополнително на интерната контрола, контролорите може -на доброволна основа - да направат и оценка на процесите и интерните документи за заштита на личните податоци заради сертификација на нивната обработка на лични податоци со цел да покажат усогласеност

со прописите за заштита на личните податоци. Процесот на сертификација го врши АЗЛП или друго тело за сертификација во согласност со прописите за заштита на личните податоци.

Во член 40 од Правилникот се пропишуваат мерки кои се однесуваат на управување со преносните медиуми. Според одредбата од овој член, како техничка мерка од високо ниво контролорите се должни да воспостават систем за евидентирање на преносните медиуми кои ги примаат со цел да се овозможи директна или индиректна идентификација на таквите медиуми, датум и место на прием, испраќач, број на применот медиум, вид на документи кои се снимени на медиумот, начин на кој се испратени медиумите, име/презиме на лицето овластено за прием на такви медиуми. Истиот систем може да се примени и за водење евиденција за медиумите коишто ги испраќа контролорот.

Техничката мерка од високо ниво дадена во член 41 од Правилникот подразбира задолжително тестирање на информатичкиот систем пред неговата примена и по извршени промени во информатичкиот систем за да се провери дали системот обезбедува безбедност на личните податоци во согласност со прописите за заштита на личните податоци. Тестирањето на информатичкиот систем не смее да се врши со обработка на реални лични податоци, туку за таа цел се користат имагинарни лични податоци.

Член 42 од Правилникот пропишува дека контролорите може да применуваат и други технички мерки за да обезбедат тајност и заштита на обработката на лични податоци преку примена на постапки за сертификација во согласност со прописите кои ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги.

.

Оваа публикација е изработена како дел од твининг-проектот „Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“, финансиран од Европската Унија. Содржината на публикацијата е единствена одговорност на авторите и на проектните партнери, и не може да се смета дека ги одразува ставовите на Европската Унија.

+389 2 3230 635

info@privacy.mk

бул. „Гоце Делчев“ бр 18
Скопје

www.azlp.mk

SCAN ME

Овој проект е финансиран од Европската Унија