СЛУЖБЕН ВЕСНИК

на Република Северна Македонија

Број 122 **12 мај 2020, вторник** **година LXXVI**

www.slvesnik.com.mk **contact@slvesnik.com.mk**

С О Д Р Ж И Н А

МИНИСТЕРСТВО ЗА НАДВОРЕШНИ РАБОТИ

1607.

О Б Ј А В А

Северноатлантскиот Договор, склучен во Вашингтон на 4 април 1949 година, ратификуван со Закон од страна на Собранието на Република Северна Македонија на 11 февруари 2020 година и објавен во „Службен весник на Република Северна Македонија“ број 36/2020 од 12 февруари 2020 година, влегува во сила во однос на Република Северна Македонија на 27 март 2020 година.

Министер
10 април 2020 година за надворешни работи,
Скопје **Никола Димитров,** с.р.

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

1608.

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Предмет на уредување

Член 1

Со овој правилник се пропишуваат упатства за постапување на контролорите при применувањето на техничките и организациските мерки за обезбедување на безбедност на обработката на личните податоци.

Поимник

Член 2

Одделни изрази употребени во овој правилник го имаат следново значење:

1. Доверливост е пристап до личните податоци единствено од лица кои имаат овластување за нивна обработка од страна на контролорот;

2. Интегритет е заштита на точноста на личните податоци, при што се гарантира дека личните податоци се точни, целосни и ажурирани;

3. Достапност е непречен пристап и континуирана расположливост (business continuity) на информацискиот систем на кој се врши обработка на личните податоци од страна на овластените лица;

4. Автентикација е постапка која што овозможува потврдување на идентитетот на овластеното лице кое се најавува и пристапува на информацискиот систем на кој се врши обработка на личните податоци;

5. Неотповикливост е обезбедување на потврда на автентичноста на идентитетот на овластеното лице кое се најавува на информацискиот систем при што овластеното лице не може да ја негира преземената активност или дејствие;

6. Безбедносен ризик, е веројатност на случување на настан кој може да резултира со компромитирање, особено случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци, или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци (во натамошниот текст: ризик);

7. Управување со ризик е идентификација, оценка и негова класификација, која опфаќа координирана примена на ресурси на контролорот за минимизирање, набљудување и контрола на веројатноста и сериозноста која што може да произлезе при обработката на личните податоци, а која може да предизвика материјална или нематеријална штета врз процесите со кои се врши обработка на личните податоци;

8. Систем за заштита на личните податоци е збир од документирани политики, кодекси на практика, насоки, процедури и работни инструкции донесени од страна на контролорот, а кои се во функција на спроведување на техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци согласно прописите за заштита на личните податоци;

9. Авторизиран пристап е овластување доделено на овластеното лице за обработка на личните податоци, за користење на одредена информатичко комуникациска опрема или за пристап до одредени работни простории на контролорот;

10. Администратор на информацискиот систем е лице овластено за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;

11. Документ е секој запис кој содржи лични податоци и истиот може да биде во електронска или хартиена форма, да се чува на медиум и во информатичко комуникациската опрема која се користи за обработка на податоците, да се доставува преку пошта или да се пренесува преку електронско комуникациска мрежа.

12. Информатичка инфраструктура е целата информатичко комуникациска опрема на контролорот, во рамките на која се собираат, обработуваат и чуваат личните податоци;

13. Информациски систем е систем со кој може да се обработуваат личните податоци со цел да бидат достапни и употребливи за секој кој што има право и потреба да ги користи;

14. Инцидент е секоја аномалија која влијае или може да влијае на тајноста и заштитата на личните податоци;

15. Контрола на пристап е операција за доделување на пристап до личните податоци или до информатичко комуникациската опрема со цел проверка на овластеното лице;

16. Овластено лице е лице вработено или ангажирано кај контролорот кое има авторизиран пристап до документите и до информатичко комуникациската опрема на кои се обработуваат лични податоци;

17. Лозинка е доверлива информација составена од множество на карактери кои се користат за проверка и автентикација на овластеното лице;

18. Колаче (cookie) е информација која што се креира и испраќа од веб-серверот до веб пребарувачот, а која потоа се испраќа назад, како непроменета информација од веб-пребарувачот секогаш кога повторно ќе се пристапи до веб-серверот кој ја креирал информацијата.

19. Работна станица е секој уред (десктоп, лаптоп) кој поврзан во мрежа претставува дел од опремата на контролорот, а на кој, односно со кој се врши обработка на личните податоци во информацискиот систем;

20. Медиум е физички уред кој се користи при обработка на личните податоци во информацискиот систем, на кој податоците можат да бидат снимени или од кој истите можат да бидат повторно вратени; и

21. Сигурносна копија е копија на личните податоци содржани во електронските документи, кои се зачувани на медиум за да се овозможи нивно повторно враќање.

Примена
Член 3

Одредбите од овој правилник се применуваат и при обработка на личните податоци од страна на обработувачот на збирка на лични податоци.

Одржување на информацискиот систем
Член 4

(1) Физичките или правните лица кои вршат одржување на информацискиот систем на контролорот треба да ги применуваат прописите за заштита на личните податоци и донесената документација за технички и организациски мерки.

(2) Одредбите од ставот (1) на овој член се применуваат и ако физичките или правните лица вршат обработка на личните податоци на контролорот.

Пренос на лични податоци во трети земји
Член 5

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во трети земји само согласно условите утврдени во прописите за заштита на личните податоци.

II. БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Систем за заштита на личните податоци
Член 6

(1) Според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозноста за правата и слободите на физичките лица, контролорот е должен да воспостави систем за заштита на личните податоци преку примена на соодветни технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот.

(2) Техничките и организациските мерки од ставот (1) на овој член, особено опфаќаат:

- псевдонимизација и криптирање на личните податоци;
- способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на информацискиот систем за обработка;
- способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент; и
- процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.

(3) Контролорот врши оценка и ажурирање на техничките и организациските мерки при што секогаш ги применува оние мерки кои се соодветни на времето во кое се дизајнираат и имплементираат, а согласно најновите технолошки достигнувања (a state of the art technology).

(4) Процесот за управување со системот за заштита на личните податоци од ставот (1) на овој член е дефиниран во Политиката за системот за заштита на личните податоци на контролорот кој треба да им одговара на природата, обемот и сложеноста на активностите коишто контролорот ги врши при обработката на личните податоци и ризиците на коишто е изложен.

(5) Контролорот е должен Политиката од ставот (4) на овој член да ја ревидира и усогласува согласно промените во неговото работење.

Управување со ризик
Член 7

(1) Контролорот при утврдувањето и проценатa на ризикот (управување со ризик) ги зема во предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење, менување, неовластено откривање на личните податоци или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

(2) Управувањето со ризикот од ставот (1) на овој член ги опфаќа следните фази:

а) список (преглед) на сите процеси со кои се врши обработка на лични податоци;

б) процена на ризиците за секој процес на обработка на лични податоци;

в) спроведување и проверка на планираните мерки; и

г) спроведување на периодични безбедносни проверки.

(3) Списокот на процеси со кои се врши обработка на личните податоци од став (2) точка а) на овој член преку целосно или делумно автоматизирана обработка на личните податоци или друга обработка на лични податоци, треба најмалку да ги опфати:

- хардверот (на пример: сервери, лаптопи, хард дискови и други медиуми);
- софтверот (на пример: оперативни системи и софтверски програми развиени за потребите на контролорот);
- комуникациски канали (на пример: оптички кабли, интернет, безжична мрежна технологија – Wi-Fi);
- документи во хартиена форма (на пример: печатени документи, фотокопии).

(4) Проценатa на ризиците од став (2) точка б) на овој член, треба најмалку да ги опфати:

(а) утврдување на потенцијалните влијанија и ефекти врз правата и слободите на физичките лица на кои се однесува и тоа за следните потенцијални закани, односно настани:

- неовластен пристап до личните податоци;
- непосакувани промени на личните податоци; и
- привремена или целосна недостапност до личните податоци.

(б) идентификување на изворите на ризик кој што може да биде причина за секој непосакуван настан, а имајќи ги предвид внатрешните и надворешните човечки ресурси (на пример: администраторот на информацискиот систем, овластеното лице, надворешниот напаѓач, конкурент), како и другите внатрешни и надворешни извори (на пример: вода, опасни материјали, пожар, вирус).

(в) идентификување на можните закани кои би можеле да се случат преку медиуми од кои зависат личните податоци (на пример: хардвер, софтвер, комуникациски канали, документи во хартиена форма, итн.), а кои може да бидат:

- употребени на несоодветен начин (на пример: злоупотреба на овластувањата, грешка при ракување);
- изменети (на пример: „заразен“ софтвер или хардвер – keylogger, инсталирање на злонамерен софтвер, итн);
- изгубени (на пример: кражба на лаптоп или губење на мемориски уред – УСБ);
- набљудувани (на пример: гео-локација на опремата);
- оштетени (на пример: вандализам, деградација заради природно абење);

- преоптоварени (на пример: медиумот за складирање е целосно пополнет, denial of service attack и сл.).

(г) Утврдување на постојни или планирани мерки што овозможуваат решавање на секој ризик (на пример: контрола на пристап, сигурносни копии, информациска ревизорска трага, безбедност на просториите, криптирање или анонимизација).

(д) Оценување на сериозноста и веројатноста на ризиците, во однос на претходните елементи предвидени во овој став (на пример: скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална).

(5) Контролорот задолжително врши спроведување и проверка на планираните мерки од став (2) точка в) на овој член, а со цел да се обезбеди дека тие се применуваат и тековно се тестираат.

(6) Контролорот задолжително спроведува периодични безбедносни проверки од став (2) точка г) на овој член, за што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.

Нивоа на мерки за безбедност на обработката на личните податоци

Член 8

(1) Земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, контролорот е должен да примени соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци.

(2) Техничките и организациските мерки од ставот (1) на овој член се класифицираат во две нивоа:

- стандардно; и
- високо.

(3) Во согласност со ставот (1) од овој член, контролорот кој обработува лични податоци за помалку од 10 вработени како единствена збирка на лични податоци, нема обврска да примени технички и организациски мерки освен ако постои веројатност дека обработката која што ја врши претставува ризик за правата и слободите на субјектите на личните податоци, ако обработката не е повремена или обработката вклучува посебни категории на лични податоци или лични податоци поврзани со казнени осуди и казнени дела.

Примена на нивоа на мерки за безбедност на обработката на личните податоци

Член 9

(1) Контролорот е одговорен за усогласеноста во однос на нивото на мерки за безбедност на обработката на личните податоци кое ќе го примени во согласност со членот 8 од овој правилник, при што треба да обезбеди соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и заштита од нивно случајно губење, уништување или оштетување.

(2) Контролорот ја демонстрира примената на мерките според барањата утврдени во ставот (1) на овој член, вклучувајќи ги причините и основите за изборот на примената на стандардното, односно високото ниво.

III. СТАНДАРДНО НИВО

Документација за технички и организациски мерки

Член 10

(1) Контролорот во Политиката за системот за заштита на личните податоци ги утврдува и начелата за безбедност и заштита на личните податоци.

(2) Врз основа на Политиката за системот за заштита на личните податоци, контролорот донесува поделални политики и процедури во кои се опишани техничките и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура.

(3) Документираните процеси од ставот (2) на овој член особено се однесуваат на:

- идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);
- општ опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот;
- активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот;
- дизајнирање, развивање и одржување на софтверските програми за обработка на личните податоци, а особено од аспект на техничка и интегрирана заштита на личните податоци (Data protection by design and by default);
- начинот на обезбедување на автентикација на овластените лица во информацискиот систем;
- начинот на обезбедување на контрола на пристап до информацискиот систем;
- начинот на обезбедување евиденција за секој пристап до информацискиот систем (на пример до: оперативните системи, заштитниот sид (firewall), серверот дизајниран специјално за употреба како сервер за датотеки (file server), базите на податоци, системот (софтверот) за управување со документи (DMS System), софтверот за управување со врски со клиенти (CRM Software) и сл.);
- начинот на управување со инциденти (инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци);
- начинот на обезбедување на опремата на контролорот на која се врши обработка на личните податоци;
- начинот на обезбедување на преносливите медиуми;
- начинот на заштита на внатрешната мрежа на контролорот;
- начинот на обезбедување на серверите и веб-страницата на контролорот;
- начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци;
- начинот на обработка на личните податоци кои се псевдонимизирани;
- начинот на обработка на личните податоци кои се криптирани;
- обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;
- начинот и процесите за пријавување, реакција и санирање на инциденти;
- начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
- начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите;
- физичка безбедност;
- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);
- динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола; и
- други мерки кои контролорот ги применува врз основа на анализата на ризикот.

(4) Документацијата од ставовите (2) и (3) на овој член, контролорот ја менува и дополнува кога ќе се направат промени во информацискиот систем и информатичката инфраструктура, а најмалку еднаш годишно врши нејзино оценување, евалуација и ажурирање.

1. Технички мерки

Автентикација на овластените лица

Член 11

(1) Контролорот обезбедува најавата во информацискиот систем да се врши преку единствен идентификатор кој се поврзува само со едно овластено лице.

(2) Во согласност со ставот (1) од овој член единствениот идентификатор контролорот може да го обезбеди преку:

- информација која единствено овластеното лице ја знае (на пример: единствено корисничко име и лозинка за секое овластено лице, при што лозинката треба да биде составена од комбинација на најмалку осум алфанумерички карактери букви (мали и големи), симболи, броеви и интерпукциски знаци;
- нешто што само овластеното лице го поседува (на пример: паметна картичка – smart card);
- нешто што овластеното лице е, или го прави (на пример: дигитален потпис); и
- други начини на автентикација кои според најновите технолошки достигнувања, а во контекст на извршената анализа на ризикот обезбедуваат единствен идентификатор кој се поврзува само со едно овластено лице.

(3) Автентикацијата на овластените лица, контролорот ја врши најмалку преку еден од наведените начини од ставот (2) на овој член. Во зависност од анализата на ризикот, за одредени овластени лица или за сите, може да се примени и комбинација од два или повеќе фактори на автентикација (на пример: единствено корисничко име и лозинка во комбинација со употреба на паметна картичка).

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

(5) Кога проверката се врши врз основа на корисничко име и лозинка, контролорот секогаш ги применува правилата кои ја гарантираат нивната доверливост и интегритет при пријавување, доделување и чување на истите, при што лозинките задолжително автоматски се менуваат по изминат определен временски период врз основа на анализата на ризикот кој не може да биде подолг од три месеци.

Обезбедување на опремата на која се врши обработка на личните податоци

Член 12

(1) Контролорот е должен да обезбеди примена на технички мерки со кои се обезбедува опремата на која се врши обработка на личните податоци и тоа:

- автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути). За повторно активирање на системот, контролорот треба да обезбеди дека овластените лица пристапуваат со примена на автентикацијата во согласност со член 11 од овој правилник;
- во случај на одреден број на неуспешни обиди за најавување на информацискиот систем, кои се во спротивност со политиките за автентикација на контролорот, треба да се обезбеди автоматизирано отфрлање од информацискиот систем. Бројот на неуспешни обиди контролорот го определува соодветно на ризикот и природата на работата и работните процеси во однос на обработката на личните податоци, но не повеќе од пет последователни неуспешни обиди;
- инсталиран заштитен sид (firewall) и ограничување на овластените порти за комуникација на оние што се строго неопходни за правилна работа на софтверските програми инсталирани на работните станици на контролорот;
- редовно ажуриран антивирусен софтвер и дефинирана политика за редовни ажурирања на софтверските програми;
- конфигурирани софтверски програми така што безбедносните ажурирања да се вршат автоматски;
- зачувување на податоците на корисниците на серверите на контролорот за кои редовно се прави сигурносна копија, а во случај кога податоците се зачувуваат локално, задолжително со мерки за синхронизација или со резервни дополнителни мерки за заштита врз основа на анализа на ризикот;
- ограничување на опцијата за приклучување на преносливите медиуми (УСБ, надворешни хард дискови и сл.) кон системите со примарна важност;
- исклучен автоматски режим на работа за преносливите медиуми (Disable autorun for removable media);
- алатките за далечинска администрација мора да бидат нагодени на начин што претходно задолжително треба да обезбедат согласност од корисникот (овластеното лице) на работната станица пред каква било интервенција на самата работна станица;
- нагодување на информацискиот систем кое ќе обезбеди дека корисникот (овластеното лице) на работната станица може да забележи дали се врши далечинска администрација, како и за тоа кога истата завршила (на пример со прикажување на порака на екранот дека далечинската администрација завршила); и
- приклучување на информацискиот систем (компјутерите и серверите) на енергетска мрежа преку уред за непрекинато напојување.

(2) Покрај мерките од ставот (1) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот ги применува и следните мерки:

- забрана на работа со преземени софтверски програми кои не доаѓаат од безбедни извори;
- ограничување на употребата на софтверски програми што бараат администраторски права;
- бришење на податоците што се наоѓаат на работна станица која треба да се предаде;
- во случај работната станица да биде компромитирана, задолжително испитување и по можност пронаоѓање на изворот, како и каква било трага од упадот во информацискиот систем на контролорот, со цел откривање дали се загрозени и други елементи;
- безбедносен надзор на софтверот и хардверот што се користи во системот на контролорот, вклучувајќи и редовно следење на тимот за брза реакција (MKD-CIRT) во однос на неговите предупредувања и совети за ранливости откриени во софтверот и хардверот;
- ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;
- инсталирање на ажурирања на оперативните системи со автоматска верификација согласно проценатa на ризик, а најмалку еднаш неделно; и
- подигнување на нивото на свесност во однос на тоа, на што овластените лица треба да се посветат и податоци за контакт на лицата што треба да ги контактираат во случај на инцидент или појава на необичен настан што влијае на информациите и комуникацијата на системите на контролорот.

Сегрегација на должности и одговорности

Член 13

(1) Контролорот ги утврдува овластените лица кои треба да имаат пристап до информацискиот систем при што обезбедува јасна поделба на должностите и одговорностите според правилото „потребно е да знае“, односно дека овластеното лице ќе има пристап само до оние лични податоци за кои има неопходна потреба заради извршување на своите должности.

(2) Контролорот обезбедува повлекување на правата на пристап веднаш по престанокот на овластувањата за пристап.

(3) Контролорот врши проверка и ажурирање на привилегиите за пристап до информацискиот систем на овластените лица. Проверката се врши за периоди кои се определуваат врз основа на анализата на ризикот, а најмалку квартално.

Контрола на пристап до информацискиот систем

Член 14

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

(2) Контролорот воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема со права различни од тие за кои се авторизирани.

(3) Администраторот на информацискиот систем кој е овластен од контролорот, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на контролорот.

Обезбедување евиденција за секој пристап (logs)

Член 15

(1) Со цел да обезбеди идентификување на секој неовластен (измамнички) пристап или злоупотреба на лични податоци, како и да се утврди потеклото на овие инциденти, контролорот воспоставува и води евиденција за секој пристап до информацискиот систем – logs (на пример: од оперативните системи, од заштитниот ѕид (firewall), серверот дизајниран специјално за употреба како сервер за датотеки (file server), базите на податоци, системот (софтверот) за управување со документи (DMS System), софтверот за управување со врски со клиенти (CRM Software) и сл;

(2) Евиденцијата од ставот (1) на овој член треба да ги содржи особено следните податоци: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, лични податоци кон кои е пристапено, видот на пристапот со операциите кои се преземени при обработка на податоците, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем.

(3) Во евиденцијата од ставот (1) на овој член се внесуваат и податоци за идентификување на информацискиот систем од кој се врши надворешен обид за пристап во оперативните функции или личните податоци без потребното ниво на авторизација.

(4) Операциите кои овозможуваат евидентирање на податоците од ставовите (2) и (3) на овој член треба да бидат контролирани од страна на офицерот за заштита на личните податоци и/или од друго овластено лице од контролорот кое ги има потребните знаења и вештини, но нема администраторски привилегии и истите задолжително треба да бидат нагодени на таков начин што нема да може да се деактивираат. Во однос на евиденцијата на податоците за пристап, контролорот може да користи и алатки кои податоците ги генерираат во едноставна и лесно разбирлива форма за читање.

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

(6) Офицерот за заштита на личните податоци врши контрола на податоците од ставовите (2) и (3) на овој член, најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

(7) Контролорот ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем.

(8) Контролорот обезбедува заштита на системот за евиденција за пристап до информацискиот систем, од било каков неовластен пристап, особено на лицата чија активност се евидентира на системот за евиденција.

(9) Контролорот обезбедува дека овластените лица за управување со системот за евиденција за пристап до информацискиот систем го известуваат раководството за која било аномалија или безбедносен инцидент, веднаш, а најдоцна во рок од 12 часа од моментот на инцидентот.

(10) Контролорот ја известува Агенцијата за заштита на личните податоци за секое нарушување на безбедноста на личните податоци, а доколку постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, и субјектите на личните податоци за да можат да ги ограничат последиците од нарушувањето на безбедноста.

(11) Контролорот не смее да ги користи информациите од евиденцијата за пристап до информацискиот систем за цел различна од таа дека информацискиот систем се користи соодветно (на пример: употреба на записите за мерење на часовите на вработениот претставува злоупотреба на информацискиот систем).

Обезбедување на преносливите медиуми

Член 16

(1) Контролорот согласно анализата на ризикот од нарушување на безбедноста на личните податоци во случај на кражба или друг начин на загуба на преносливите медиуми (мобилна опрема) на кои се врши обработка на личните податоци применува соодветни технички мерки.

(2) Техничките мерките од ставот (1) на овој член го опфаќаат најмалку следното:

- подигање на свеста на овластените лица за специфичните ризици поврзани со користење на преносливи медиуми (на пример: кражба на опремата) и утврдените процедури за намалување на овие ризици;
- спроведување на мерки за правење на сигурносна резервна копија или синхронизација на мобилните работни станици, со цел да заштитат од губење на зачуваните податоци;
- мерки за криптирање за заштита на мобилни работни станици и медиуми за мобилно складирање (лаптоп, УСБ, надворешни хард-дискови, ЦД-РОМ, ДВД, итн.). На пример: повеќето лаптопи вклучуваат функционалност што овозможува да се криптира нивниот хард диск поради што секогаш кога е можно, е препорачливо да се користи оваа опција); и
- употреба на услуги во облак (cloud services) за правење на сигурносни копии само по претходна анализа на нивните услови и безбедносни гаранции.

(3) Покрај мерките од ставот (2) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, контролорот може да ги примени и следните мерки:

- поставување на филтер за приватност на екраните на мобилните работни станици што се користат на јавни места, или употреба на мобилни работни станици со интегриран филтер за приватност;
- ограничување на обемот на податоци кои може да се зачуваат на мобилните работни станици на она што е строго неопходно со дополнителна заштита и ограничување за време на патувања, особено во странство;

- спроведување на дополнителни мерки за заштита од кражба (на пример кабел за безбедност, видливо обележување на опремата итн) и мерки што ги намалуваат негативните ефекти (на пример автоматско заклучување, криптирање); и

- кога мобилните уреди се користат за собирање податоци во движење (на пример: лични асистенти, паметни телефони, лаптопи, итн.), шифрирање на податоците на самиот уред. Исто така, заклучување на уредот по неколку минути неактивност и прочистување на податоците собрани веднаш штом се пренесат во информацискиот систем на контролорот.

Заштита на внатрешната мрежа

Член 17

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

- ограничување на пристапот до интернет со блокирање на несуштински услуги и сервиси (VoIP, peer to peer, итн.);

- управување со Wi-Fi мрежата кое опфаќа користење на најсовремените методи на криптирање (на пример: WPA2 или WPA2-PSK и со употреба на комплексна лозинка која на определен временски период се менува);

- Wi-Fi мрежата која е отворена за употреба на лица кои не се овластени (на пример надворешни посетители) задолжително да биде одвоена од внатрешната мрежа;

- во случај на далечински пристап, задолжително воспоставување на VPN конекција, со задолжителна автентикација на овластеното лице (на пример: паметна картичка, уред за генерирање лозинка за еднократна употреба – OTP и слично);

- обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително да се изврши преку VPN); и

- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен sид, прокси сервери, итн (на пример: ако веб серверот користи HTTPS, да се обезбеди влезниот сообраќај да биде преку портата 443 и со блокирање на сите други пристапи).

(2) Контролорот врз основа на анализата на ризикот, покрај мерките наведени во ставот (1) од овој член, може да примени и други мерки со кои ќе ја зајакне заштитата на својата внатрешна мрежа.

Обезбедување на серверите

Член 18

(1) Контролорот согласно анализата на ризик е должен на врвот на својата листа од аспект на примената на технички и организациски мерки да ги има своите сервери на кои се централизира обработката на голема количина на лични податоци. При тоа контролорот ги применува особено (најмалку) следните мерки:

- единствено овластени лица кои ги имаат потребните знаења може да имаат пристап до алатките и административни панели на серверите;

- примена на овластувања со помалку привилегии за лицата кои не се администратори на информацискиот систем (вообичаени операции за стандардни корисници);

- примена на посебна политика за креирање и употреба на лозинките за администраторите на информацискиот систем (на пример: промена на лозинките по секое заминување на администраторот, употреба на повеќе факторска лозинка...);

- инсталирање на сите важни ажурирања (updates) за оперативните системи и за апликациите во временски интервал врз основа на анализата на ризикот, но не подолго од седмично ажурирање со нагодување на системот за автоматско ажурирање (auto update);

- правење на сигурносни копии и нивна редовна проверка; и

- примена на TLS протокол (со замена на SSL13) или друг протокол што обезбедува шифрирање и автентикација, како минимум за каква било размена на податоци преку интернет и потврда на нејзината соодветна примена преку соодветни алатки.

(2) Во случај кога се врши администрирање на базите на податоци, контролорот ги применува најмалку следните мерки:

- употреба на персонализирани профили за пристап до базите на податоци и креирање на посебно корисничко име за секоја апликација (specific account for each application); и

- примена на мерки против напади преку инјектирање на SQL код, скрипти и слично.

Обезбедување на веб-страницата на контролорот

Член 19

(1) Контролорот кој има своја веб-страница треба да примени технички мерки со кои ќе го гарантира точниот идентитет на страницата (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа особено преку следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на контролорот (ако има повеќе од една), користејќи ја единствено најновата верзија и со проверка на неговата правилна имплементација;

- задолжителна употреба на криптографски протокол (TLS) за сите страници од веб-страницата, вклучително и формулари за собирање лични податоци или овозможување автентикација на корисникот и на оние на кои се прикажани или се пренесуваат лични податоци кои не се јавно достапни;

- ограничување на портите за комуникација на оние кои се строго потребни за правилно функционирање на инсталираните апликации. Ако веб серверот прифаќа само врски со HTTPS протокол, само IP мрежен сообраќај кој влегува преку портата 443 е дозволен, а сите други пристапни порти мора да бидат блокирани;

- обезбедување дека само овластени лица ќе можат да имаат пристап до алатките и административните интерфејси, при што особено да се ограничи употребата да биде достапна само до овластените лица со администраторски привилегии кои се дел од тимот одговорен за информатичката технологија и само за административни активности што се неопходни; и

- ако се користат колачиња што не се потребни од услугата, контролорот обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето;

(2) Контролорот кој има своја веб-страница не треба да применува практики кои го зголемуваат ризикот од можна злоупотреба, несакана (случајна) или намерна неовластена обработка на личните податоци, а особено:

- да не пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);

- користење на небезбедни услуги;

- употреба на сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораки и слично;

- поставување на базите на податоци на сервери кои се директно достапни преку интернет; и
- споделување и употреба на корисничките сметки (user accounts) помеѓу две или повеќе овластени лица.

Обврски и одговорности на администраторот на информацискиот систем и на овластените лица

Член 20

(1) Контролорот врз основа на спроведената анализа на ризик, ги определува обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема, применувајќи ги најмалку мерките кои се предвидени со овој правилник.

(2) Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

(3) Во извештајот од ставот (2) се наведуваат констатираните неправилности (доколку ги има) и предложените мерки за отстранување на тие неправилности.

(4) Контролорот задолжително ги информира администраторот и овластените лица од ставот (1) на овој член за документацијата за технички и организациски мерки која се однесува на извршувањето на нивните обврски и одговорности.

Превенирање, реакција и санирање на инциденти (обезбедување континуитет)

Член 21

(1) Контролорот врз основа на анализата на ризик утврдува план за управување со континуитет на својот информациски систем, вклучувајќи и список на овластените лица кои се одговорни за превенирање, како и за навремено повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на настанат физички или технички инцидент.

(2) Согласно ставот (1) на овој член, контролорот го определува начинот на управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци.

(3) Управувањето со инциденти од ставот (2) на овој член, опфаќа пријавување, реакција и санирање на инцидентите, при што контролорот го определува начинот на евидентирање на секој инцидент, времето кога се појавил, овластеното лице кој го пријавило, на кого е пријавен и мерките кои се преземени за негово санирање.

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

(5) Контролорот обезбедува дека овластените лица, обработувачите и подобработувачите знаат кого да го известат и предупредат во случај на настанат инцидент.

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

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

Член 22

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

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

(3) Контролорот врз основа на анализата на ризикот, обемот и временската динамика на промена на податоците, прави сигурносни копии во интервали кои го минимизираат ризикот врз ефектот на податоците за кои при инцидент би настапило нивно непосакувано губење или оштетување. Притоа, контролорот прави фрагментирана (incremental back-up), односно поединечна копија на дневна основа во однос на сите настанати промени во текот на денот, а целосна сигурносна копија (full back-up) во редовни временски интервали по негова оценка, а најмалку еднаш месечно, на начин кој ќе гарантира повторно воспоставување на достапноста до личните податоци во случај на настанат физички или технички инцидент.

(4) Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци.

(5) Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.

(6) Контролорот во однос на сигурносните копии го применува истото безбедносно ниво на технички и организациски мерки како и за податоците кои се зачувани на оперативните сервери на кои врши обработка на личните податоци (на пример: со криптирање на сигурносните копии, со чување на безбедно место на сигурносната копија за кое се применети мерки и контроли кои го минимизираат ризикот од поплава, пожар, кражба и слично, или во случај на договорно регулирање и аутсорсирање на услугата, соодветна заштита која треба да ја примени и обработувачот).

Начин на архивирање и чување на податоците

Член 23

(1) Контролорот, во однос на личните податоци за кои сè уште не истекол рокот за нивно чување согласно закон, а за кои престанала потребата од нивна непосредна и секојдневна обработка, врши архивирање на безбеден начин, особено ако архивираните податоци се чувствителни податоци (посебни категории на лични податоци), или податоци што можат да имаат сериозно влијание врз субјектите на личните податоци, доколку бидат компромитирани.

(2) Согласно ставот (1) од овој член, контролорот определува постапка за управување со архивскиот материјал во однос на тоа кои податоци треба да се архивираат, како и каде се чуваат и кој, како и под кои услови има пристап до нив.

(3) Контролорот задолжително донесува соодветен документ „Список (преглед) со рокови на чување на личните податоци“ во кој ќе бидат содржани информации за моментот на активирање на периодот (рокот) за чување на личните податоци, идентификуваните периоди (рокови) за чување на личните податоци, причините за чување на личните податоци, законскиот основ за чување на личните податоци и сопственикот на податоците.

(4) Контролорот е должен документот од ставот (3) на овој член да го ревидира и усогласува годишно согласно промените во работењето на контролорот и законските услови за чување на личните податоци.

Управување со преносливи медиуми

Член 24

(1) Преносливите медиуми на кои се врши обработка на личните податоци контролорот обезбедува дека се чуваат на локација до која пристап имаат само овластени лица утврдени од негова страна.

(2) Пренесувањето на медиумите од ставот (1) на овој член надвор од работните простории се врши само со претходно овластување од страна на контролорот.

(3) По пренесувањето на личните податоци од медиумот или по истекот на определениот рок за чување, медиумот треба да се уништи, избрише или да се исчисти од личните податоци снимени на него.

(4) Уништувањето на медиумот се врши на начин кој ќе гарантира дека податоците кои биле снимени на него не можат повторно да бидат реконструирани (на пример: со механичко разделување на неговите составни делови).

(5) Бришењето или чистењето на медиумот треба да се изврши на начин што ќе оневозможи понатамошно обновување на снимените лични податоци.

(6) За случаите од ставовите (4) и (5) на овој член контролорот обезбедува информациска трага (на пример: записник), која ги содржи сите податоци за целосна идентификација на медиумот, како и за категориите на лични податоци кои биле снимени на истиот.

Криптирање на личните податоци

Член 25

(1) Кога контролорот врз основа на анализата на ризикот, а земајќи ги предвид природата, обемот, контекстот и целите на обработката на личните податоци, врши криптирање на личните податоци, секогаш применува најсовремени технички решенија за криптирање со кои го обезбедува интегритетот, доверливоста и автентичноста на личните податоци.

(2) Во согласност со ставот (1) на овој член контролорот применува единствено признати и безбедни алгоритми за криптирање (како на пример: SHA-256, SHA-512 или SHA-341 како хаш функција, HMAC користејќи SHA-256, bcrypt, scrypt или PBKDF2 за чување лозинки, AES или AES-CBC за симетрично криптирање, RSA-OAEP v2.1 за асиметрично криптирање...), а воедно обезбедува заштита на тајните клучеви за криптирање со ограничувачки права за пристап и посебно креирана безбедна лозинка за пристап.

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

Физичка безбедност

Член 26

(1) Контролорот задолжително применува зајакнато ниво на безбедност во однос на просториите во кои се сместени и се чуваат серверите и мрежната опрема преку кои се врши обработка на личните податоци со примена на соодветни мерки кои обезбедуваат дека само лица посебно овластени од контролорот имаат пристап, како и мерки со кои се намалува ризикот од потенцијални закани и тоа:

- инсталирање на алармни системи против упад и нивна периодична проверка;
- примена на мерки и контроли за превенција од кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење;
- обезбедување безбедност на клучевите и шифрите за аларми кои овозможуваат пристап до просториите;
- обезбедување на одделни области во објектот каде се чуваат серверите според анализата на ризик (на пример: употреба на посебна контрола за пристап за сервер салата);
- ажуриран список на лица или категории на лица кои се овластени да влезат во просториите каде се чува опрема на која се врши обработка на личните податоци;
- воспоставување на правила и методи за контрола на пристапот на посетителите и тоа минимум со придружба од едно лице во контролорот со посетителите надвор од областите за прием на странки;
- посебна физичка заштита на ИТ-опремата преку специфични методи (систем за спречување на пожар, поплави, електрична енергија, климатизација, итн.);
- одржување на просториите за серверите (климатизација, UPS, итн.).
- водење на евиденција за пристап до просториите каде што се чуваат серверите кои содржат лични податоци;
- обезбедување дека само овластените лица можат да пристапат до просториите со ограничен пристап (на пример: во внатрешноста на контролираните простории за пристап, сите лица да носат видлива идентификација (картичка), како и преиспитување и редовно ажурирајте на дозволите за пристап до заштитените области).

(2) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот.

(3) Во случајот од ставот (2) на овој член, меѓусебните права и обврски на контролорот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи мерки за безбедност на личните податоци согласно прописите за заштита на личните податоци.

Контрола на информацискиот систем и информатичката инфраструктура

Член 27

(1) Во документацијата за технички и организациски мерки утврдена во членот 10 од овој правилник, задолжително треба да се содржани постапките за овластување на офицерот за заштита на личните податоци, за вршење периодични контроли, заради следење на усогласеноста на работењето на контролорот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

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

Управување со обработувачи

Член 28

(1) Контролорот е должен да воспостави процес на управување при користење на услуги за обработка на личните податоци од страна на обработувачи, а со цел да се воспостават соодветни процедури за одлучување при изборот на обработувачот, управување со обработката на личните податоци, како и исполнување на договорените обврски и одговорности од страна на обработувачот.

(2) Контролорот е должен да применува процедура за одлучување за избор на обработувач со која задолжително ќе предвиди:

1. Анализа на потенцијалните обработувачи во однос на нивните технички и организациски мерки за обезбедување на гаранција дека обработката на личните податоци ќе се одвива во согласност со барањата предвидени во прописите за заштита на личните податоци, како и за обезбедување на заштита на правата на субјектите на лични податоци; и

2. Анализа на ризиците врз работењето на контролорот што можат да произлезат при обработката на личните податоци од страна на обработувачите.

Ангажирање на обработувачи

Член 29

(1) Во случај кога контролорот ќе одлучи да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувачот, должен е да обезбеди дека личните податоци се обработуваат под негов надзор над безбедноста на личните податоци, при што личните податоци мора да бидат обработувани со безбедносни гаранции.

(2) Во случаите од ставот (1) на овој член, контролорот може да пренесе работи само на обработувач кој може да обезбеди доволно гаранции, особено во однос на потребното знаење од областа на заштитата на личните податоци, сигурноста и ресурсите.

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

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

- дали и како се врши криптирање на податоците според нивната чувствителност;
- постоење на процедури кои гарантираат дека никој нема да има неовластен пристап до податоците;
- дали и како се врши криптирање на преносот на податоци;
- гаранции во однос на следливост (логови, информациска ревизорска трага...);
- управување со правата на пристап;
- автентикација; и
- други мерки за безбедност на обработката на личните податоци.

(5) Договорот од ставот (3) на овој член треба да содржи одредби особено за:

- предметот, должината и целта на обработката на личните податоци;
- обврските за обработувачот да преземе технички и организациски мерки за да обезбеди безбедност на обработката на личните податоци;
- обврските во однос на доверливоста на доверените лични податоци;
- минималните стандарди за автентикација на овластените лица;
- условите за враќање на податоците и/или нивно уништување по истекот или раскинувањето на договорот;
- правилата за управување и известување на контролорот во случај на инциденти,односно во случај на нарушување на безбедноста на личните податоци;
- обврските за обработувачот да постапува единствено во согласност со упатствата добиени од страна на контролорот; и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

2. Организациски мерки

Организациски мерки за безбедност на личните податоци (минимален стандард)

Член 30

(1) Контролорот е должен да обезбеди соодветни организациски мерки за безбедност на личните податоци врз основа на резултатите од анализата на спроведениот ризик, а особено да обезбеди:

1. Ограничен пристап со идентификација за пристап до личните податоци;
2. Организациски правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори;
3. Уништување на документи по истекот на рокот за нивно чување;
4. Мерки за физичка сигурност на работните простории и на информатичко комуникациската опрема каде што се собираат, обработуваат и чуваат личните податоци; и
5. Почитување на техничките упатства при инсталирање и користење на информатичко комуникациската опрема на која се обработуваат личните податоци.

(2) Вработеното лице кое ги врши работите за човечки ресурси кај контролорот, го известува администраторот на информацискиот систем за вработувањето или ангажирањето на секое овластено лице со право на пристап до информацискиот систем, за да му биде доделено корисничко име и лозинка, како и за престанок на вработувањето или ангажирањето за да му бидат избришани корисничкото име и лозинката, односно заклучени за натамошен пристап.

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

Информирање и едуцирање за заштитата на личните податоци

Член 31

(1) Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

(2) За лицата кои се ангажираат за извршување на работа кај контролорот во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Контролорот пред непосредното започнување со работа на овластените лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Лицата кои се вработуваат или се ангажираат кај контролорот, пред нивното отпочнување со работа своерачно потпишуваат изјава за тајност и заштита на обработката на личните податоци.

(5) Изјавата од ставот (4) на овој член особено содржи: дека лицата ќе ги почитуваат начелата за заштита на личните податоци пред нивниот пристап до личните податоци; ќе вршат обработка на личните податоци согласно упатствата добиени од контролорот, освен ако со закон поинаку не е уредено и ќе ги чуваат како доверливи личните податоци, како и мерките за нивна заштита.

(6) Изјавата од ставот (4) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.

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

Пристап до документите

Член 32

(1) Пристапот до документите треба биде ограничен само за овластени лица на контролорот.

(2) За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

(3) Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Член 33

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

Чување на документи

Член 34

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

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

(3) Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 35

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

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

Начин на чување на документите

Член 36

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

(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

IV. ВИСОКО НИВО

1. Технички мерки

Дополнителни мерки

Член 37

Контролорот врз основа на анализата на ризикот воведува и применува дополнителни мерки за безбедност на личните податоци со кои ќе демонстрира дополнителна усогласеност со прописите и добрите практики за заштита на личните податоци.

Управување со лозинки

Член 38

(1) Контролорот треба да користи алатки за управување со лозинки со кои обезбедува дека различните лозинки за секоја услуга, или софтверска програма соодветно се чуваат, при што за пристап до сите лозинки обезбедува главна лозинка (master password), која треба да биде зајакнато комплексна, односно да биде составена од комбинација на најмалку 12 алфанумерички карактери (букви /мали и големи/), симболи, броеви и специјални интерпукциски знаци) и да се менува во период не подолг од 30 дена.

(2) Контролорот во согласност со анализата на ризикот, за одредени овластени лица (на пример за администраторот на информацискиот систем или лицата кои креираат и користат главна лозинка (master password), може да изврши дисперзија на ризикот преку управување со лозинката со дополнителен фактор согласно правилото n-2 (на пример: информацијата за лозинката да биде поделена на две или повеќе лица кои заеднички ќе се најавуваат на начин што секој ќе знае само дел од информацијата која ја сочинува лозинката, или едно овластено лице ја знае лозинка, а друго ја поседува и употребува паметна картичка – smart card).

Сертификација за заштита на личните податоци

Член 39

Контролорот, покрај внатрешната контрола од член 27 на овој правилник, а на доброволна основа, може да изврши и проверка на процесите и интерните документи за заштита на личните податоци заради сертификација на процесите преку кои се обработуваат личните податоци, со цел да демонстрира усогласеност со прописите за заштита на личните податоци при операциите на обработка. Сертификацијата се врши од Агенцијата или од сертификациони тела согласно прописите за заштита на личните податоци.

Управување со преносливи медиуми

Член 40

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

(2) Одредбите од ставот (1) на овој член се применуваат и за евидентирање на медиумите кои се испраќаат од страна на контролорот.

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

Тестирање на информацискиот систем
Член 41

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

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

Сертификациони постапки
Член 42

Контролорот може да применува и други технички мерки за тајноста и заштита на обработката на личните податоци, преку примена на сертификациони постапки согласно прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги.

Пренесување на медиуми
Член 43

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

Пренесување на личните податоци преку мрежа за електронски комуникации
Член 44

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

2. Организациски мерки

Копирање и умножување на документите
Член 45

(1) Копирањето или умножувањето на документите може да се врши единствено од страна на овластени лица определени со процедура од страна на контролорот во која задолжително се утврдуваат мерките и начинот на копирањето и умножувањето на документите.

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

Пренесување на документи
Член 46

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

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Период на прилагодување
Член 47

Во смисла на член 119 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), контролорите и обработувачите се должни да го прилагодат своето работење со одредбите на овој правилник во рамките на периодот предвиден за усогласување со одредбите од Законот за заштита на личните податоци.

Престанување на важење
Член 48

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр. 98/03 и 158/10) освен за случаите предвидени во членот 117 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20).

Влегување во сила
Член 49

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-599/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

1609.

Врз основа на член 90 став (4) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К ЗА СОДРЖИНАТА И ФОРМАТА НА АКТОТ ЗА НАЧИНОТ НА ВРШЕЊЕ НА ВИДЕОНАДЗОР

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишува содржината и формата на актот за начинот на вршење на видеонадзор.

Член 2

Одредбите од овој правилник се применуваат и при обработка на личните податоци преку вршење на видеонадзор од страна на обработувачот на збирка на лични податоци.

II. СОДРЖИНА И ФОРМА НААКТОТ ЗА НАЧИНОТ НА ВРШЕЊЕ НА ВИДЕОНАДЗОР

Содржина и форма на актот
Член 3

Актот за начинот на вршење на видеонадзор содржи: правен основ за неговото донесување, наслов на актот, основни одредби со опис на системот за вршење на видеонадзор, цел, односно цели на обработка на

личните податоци, категории на лични податоци, давање и пренос на лични податоци обработени преку системот за вршење видеонадзор, технички и организациски мерки за обезбедување безбедност на обработката на личните податоци преку системот за вршење на видеонадзор, овластени лица за обработка на лични податоци преку системот за вршење на видеонадзор, изјава за безбедност на обработката на личните податоци преку системот за вршење на видеонадзор, рок на чување на снимките од видеонадзорот, известување за вршење на видеонадзор, одредби за начинот на остварување на правата на субјектот на личните податоци, технички спецификации на опремата, план каде е поставен системот за вршење на видеонадзор и преодни и завршни одредби.

Правен основ

Член 4

Во правниот основ за донесување на актот за начинот на вршење на видеонадзор, се наведува членот од Законот за заштита на личните податоци или друг закон кој е основ за донесување на актот, бројот на Службениот весник на Република Северна Македонија каде е објавен законот, кој го донесува актот, како и датумот на неговото донесување.

Наслов на актот

Член 5

Насловот на актот за начинот на вршење на видеонадзор е „Правилник за начинот на вршење на видеонадзор_____ на (назив на контролорот)“.

Основни одредби со опис на системот за вршење на видеонадзор

Член 6

(1) Во основните одредби се утврдува опис на содржината на актот за начинот на вршење на видеонадзор со опис на системот за вршење на видеонадзор (аналогни и дигитални уреди и софтвер за видеонадзор).

(2) Во согласност со ставот (1) на овој член, контролорот ги опишува компонентите на системот за вршење на видеонадзор во неколку категории:

- видеооколина (со наведување на форматот на снимање, како се пренесуваат податоците (врски и комуникации) и како се анализираат, чуваат и презентираат снимките);

- управување со системот за видеонадзор (алармирање и предупредување, врски со други безбедносни и не безбедносни системи); и

- безбедност на системот за видеонадзор која се состои од доверливост, интегритет и достапност на податоците (физичка сигурност, контрола на пристап, превенција од губење и манипулација со податоците итн.)

Цел, односно цели на обработка на личните податоци

Член 7

(1) Во актот за начинот на вршење на видеонадзор се утврдува целта, односно целите за обработка на личните податоци преку вршењето на видеонадзор во смисла на одредбите од член 90 став (1) од Законот за заштита на личните податоци.

(2) Контролорот задолжително врши анализа на целта, односно целите за која се поставува видеонадзорот пред започнување на процесот за воспоставување на систем за вршење на видеонадзор која е составен дел од документацијата за воспоставување на системот на вршење на видеонадзор.

(3) Анализата од ставот (2) на овој член задолжително содржи и мислење од офицерот за заштита на личните податоци во контролорот, во однос на воспоставувањето на системот за вршење видеонадзор.

(4) Контролорот врши периодична оценка на постигнатите резултати од системот за вршење видеонадзор на секои две години, а во случај на поголеми промени (замена или надградба) во системот за вршење на видеонадзор и на покус период, при што изработува извештај кој е составен дел на документацијата за воспоставување на системот на вршење на видеонадзор.

Категории на лични податоци, давање и пренос на лични податоци обработени преку системот за вршење на видеонадзор

Член 8

Во актот за начинот на вршење на видеонадзор се определуваат категориите на лични податоци кои што ќе бидат предмет на обработка, можноста за давање на лични податоци на користење, како и преносот на личните податоци обработени преку системот за вршење на видеонадзор.

Технички и организациски мерки за обезбедување безбедност на обработката на личните податоци преку системот за вршење на видеонадзор

Член 9

(1) Контролорот задолжително ги определува техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци преку системот за вршење на видеонадзор, како и мерките за техничка и интегрирана заштита на личните податоци (Data protection by design and by default) согласно прописите за заштита на личните податоци, со давање на опис за преземените технички и организациски мерки.

(2) Контролорот применува технички мерки за оневозможување на пристап од далечина до системот за вршење на видеонадзор, притоа земајќи ги во предвид најновите технолошки достигнувања, а според анализа на ризик.

- (3) За пристапот и увидот до личните податоци обработени преку системот за вршење на видеонадзор контролорот задолжително води евиденција, која особено ги содржи следните податоци:

- име и презиме на овластеното лице;

- датум и време на пристапување;

- цел за пристапување;

- датум и час на направената снимка кон која се пристапува;

- датум и време, назив и седиште на корисникот на кого му е дадена снимката од видеонадзорот;

- вид на медиумот во кој е содржана снимката од видеонадзорот; и

- други податоци согласно одредбите од Правилникот за безбедност на обработката на личните податоци.

Овластени лица за обработка на лични податоци преку системот за вршење на видеонадзор

Член 10

(1) Пристап и увид до личните податоци обработени преку системот за вршење на видеонадзор имаат само овластени лица од страна на контролорот.

(2) Образецот на Овластувањето од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 1).

(3) Овластените лица за обработка на личните податоци преку системот за вршење на видеонадзор пред нивното отпочнување со работа своерачно потпишуваат Изјава за безбедност на обработката на личните податоци преку системот за вршење на видеонадзор која претставува составен дел на актот за начинот на вршење на видеонадзорот.

(4) Образецот на Изјавата од ставот (3) на овој член е составен дел на овој правилник (Образец бр. 2).

Рок на чување на снимките од видеонадзорот

Член 11

(1) Снимките направени при вршење на видеонадзорот се чуваат до исполнување на целите за кои се врши, но не подолго од 30 дена при што истите по истекот на рокот автоматски се бришат од медиумот на кој што се чуваат.

(2) Снимките од видеонадзорот може да се чуваат подолг временски период од периодот наведен во ставот (1) на овој член ако со друг закон е предвиден подолг рок во кој се содржани заштитни мерки и други мерки за заштита на правата и слободите на субјектите на личните податоци, но не подолго до исполнување на целта, односно целите.

(3) Снимките од видеонадзорот може да се чуваат подолг временски период од периодот наведен во ставот (1) на овој член кога тоа е потребно за остварување на легитимниот интерес на контролорот при водење на соодветни постапки согласно закон, за што контролорот воспоставува интерни процедури за начинот на чување и бришење на снимките.

Известување за вршење на видеонадзор

Член 12

(1) Контролорот на видливо и јасно место истакнува известување дека се врши видеонадзор во смисла на одредбите на член 89 став (4) од Законот за заштита на личните податоци кое е составен дел на актот за начинот на вршење на видеонадзор.

(2) Образецот на известувањето од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 3).

Начин на остварување на правата на субјектот на лични податоци

Член 13

(1) Во актот за начинот на вршење на видеонадзор контролорот го пропишува начинот на остварување на правата на субјектите на лични податоци чии податоци се обработуваат преку системот за видеонадзор согласно членовите од 16 до 26 од Законот за заштита на личните податоци.

(2) За остварување на правата од ставот (1) на овој член, контролорот донесува Изјава за приватност која претставува составен дел на актот за начинот на вршење на видеонадзор.

(3) Образецот на Изјавата од ставот (2) на овој член е составен дел на овој правилник (Образец бр. 4).

Технички спецификации на опремата

Член 14

Контролорот задолжително ја определува техничката спецификација на опремата со која ќе се врши видеонадзор, особено бројот на камерите, резолуцијата и квалитетот на сликата, видот на камерите, бројот и идентификацијата на работните станици со кои се пристапува до системот за видеонадзор, како и бројот и идентификацијата на опремата со која се врши видеонадзорот.

План каде е поставен системот за вршење на видеонадзор

Член 15

(1) Во Планот каде е поставен системот за вршење на видеонадзор графички се прикажува начинот на поставеноста на видео камерите, просторот каде се врши видеонадзорот, аголот на покриеност на просторот опфатен со видеонадзорот, како и карта со локациите на местата каде што се поставени камерите.

(2) Планот од ставот (1) на овој член треба да претставува составен дел на актот за начинот на вршење на видеонадзор.

Преодни и завршни одредби

Член 16

Преодните и завршните одредби се состојат од два члена од кој во првиот се наведува престанокот на важноста на претходниот акт и неговите изменувања и/или дополнувања, доколку такви има, како и архивскиот број и датумот на неговото/нивното донесување, додека во вториот член се утврдува влегувањето во сила на новиот акт и местото на објавување на актот.

III. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 17

Во смисла на член 119 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), контролорите и обработувачите се должни да го прилагодат своето работење со одредбите на овој правилник во рамките на периодот предвиден за усогласување со одредбите од Законот за заштита на личните податоци.

Член 18

Со денот на влегувањето на сила на овој правилник престанува да важи Правилникот за содржината и формата на актот за начинот на вршење на видеонадзор („Службен весник на Република Македонија“ бр. 158/10).

Член 19

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-603/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1

Врз основа на одредбите од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), _____

_____

одговорно лице кај контролорот, односно обработувачот (директор, министер и сл.)

ОВЛАСТУВАЊЕ

за вршење обработка на лични податоци

во _____

назив на контролорот односно обработувачот

(1) Се овластува _____, _____

(име и презиме) (работно место)

во _____

(назив на контролорот/обработувачот (сектор/одделение)

да врши обработка на личните податоци содржани во _____

_____

(да се наведе називот на збирката/те на личните податоци на пример, збирка за вработените, збирка на ученици, збирка на корисници на социјална помош, збирка на осигуреници и сл.)

(2) Лицето од ставот (1) на ова овластување задолжително треба да:

- ги почитува начелата за заштита на личните податоци;
- врши обработка на личните податоци согласно со упатствата добиени од _____;

(назив на контролорот/обработувачот)

- ги почитува техничките и организациските мерки за обезбедување безбедност на личните податоци кои ќе ги дознае при работата во _____; и

(назив на контролорот/обработувачот (сектор/одделение)

- ги чува како доверливи личните податоци, како и мерките за нивна заштита.

(3) Обемот на овластувањето за пристап до личните податоци е:

_____.

(да се опише обемот на овластување (на пример, да внесува лични податоци, да брише, да коригира, да гледа и сл.)

(4) Начинот на пристап до лични податоци е:

_____

_____.

(да се опише дали овластеното лице има пристап до личните податоци содржани во хартиена документација или до личните податоци кои автоматски се обработуваат или има пристап и на двата начина)

(5) Рокот на важење на ова овластување е за време додека е на работното место[1] _____

_____ во _____.

(да се наведе на кое работно место е распоредено лицето) (назив на контролорот/обработувачот)

(6) Ова овластување влегува во сила со денот на донесувањето.

М.П.

Потпис на одговорното лице,

_____

[1] Доколку е вработен на определено време да се наведе и рокот (ДД.ММ.ГГ)

Образец бр. 2

Врз основа на одредбите од Закон за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20) и Правилникот за безбедност на обработка на личните податоци („Службен весник на Република Северна Македонија” бр.), на ден ____.____.202___ година ја давам следната

ИЗЈАВА
за обезбедување безбедност на обработката на личните податоци преку системот за вршење на видеонадзор

Јас долупотпишаниот/ната, _____, _____
(Име и презиме) (Звање и работно место)
во Одделението за _____, во Секторот за _____, во _____, согласно одредбите од Правилникот за безбедност на обработка на личните податоци („Службен весник на Република Северна Македонија“ бр. _____), и документацијата за технички и организациски мерки за обезбедување безбедност на обработката на личните податоци во _____, се обврзувам дека:

- **ќе ги почитувам начелата за заштита на личните податоци;**
- **ќе ги применувам техничките и организациските мерки за обезбедување безбедност на обработката на личните податоци и ќе ги чувам како доверливи личните податоци, како и мерките за нивна заштита;**
- **ќе вршам обработка на личните податоци согласно упатствата добиени од _____;**
- **на трети лица надвор од _____и на други лица од _____ нема да издавам било каков податок од збирките на лични податоци или било каков друг личен податок кој ми е достапен и кој сум го дознал или ќе го дознаам при работата во _____.**

Потпис,
_____

Образец бр.3 Известување за вршење на видео надзор[1]

Дополнителни информации ќе најдете:
- Преку известување
- На пријавница/ рецепција/ инфо пулт
- На интернет (www)...

Назив на контролорот и каде е применливо назив на претставникот на контролорот:

Контакт информации:

Контакт информациите за офицерот за заштита на личните податоци (доколку е определен):

Информации што го засегаат субјектот на личните податоци (период на чување или следење во реално време, објавување или пренесување на видео снимките на трети страни):

Цел, односно цели за вршење на видео надзорот:

Права на субјектите на лични податоци: Како субјект на личните податоци можете да остварите повеќе права, особено право да пристапите или да барате да се избришат вашите лични податоци.
Повеќе детали за видео надзорот и за вашите права може да најдете од информациите наведени од контролорот преку опциите наведени во левиот агол.

[1] ***Забелешка***:*Информациите мора да бидат бесплатни, во транспарентна, разбирлива и лесно достапна форма, напишана на едноставен јазик. Ова известување треба да биде отпечатено на А4 формат.*

Образец бр. 4

ИЗЈАВА
ЗА ПРИВАТНОСТ ПРИ ВРШЕЊЕ НА ВИДЕОНАДЗОР

Оваа Изјава за приватност го објаснува видот на лични податоци што _____ (во натамошниот текст: Контролор), ги собира од вас при посета на службените/деловните простории и како Контролорот ги користи овие податоци.

1. Зошто собираме (обработуваме) лични податоци?

Контролорот собира лични податоци преку системот за видеонадзор од следните причини (цели):

- да се контролира пристапот до објектот (зграда, влез, простории..) и да се обезбеди сигурност на објектот, безбедноста на вработените во Контролорот и посетителите, како и на имот и информациите кои се лоцирани или се чуваат во просториите;
- за да се спречи, одврати и, доколку е потребно, да се испита неовластен физички пристап, вклучително и неовластен пристап до безбедносни и заштитени простории, ИТ инфраструктура или оперативни информации; и
- да се спречи, открие и да се испита кражба на опремата или средства во сопственост на Контролорот, посетителите или вработените, или закани по безбедноста на персоналот кој работи во просториите (на пример: пожар, физички напад).

Системот за видеонадзор не се користи за ниту една друга цел, како на пример да се следи работата на вработените или нивното присуство. Видео камерите се поставени така што не го покриваат околниот јавен простор. Камерите имаат за цел да дадат општ преглед на она што се случува на одредени места, но не и да се препознаат лица.

Системот за видеонадзор исто така не се користи како истражна алатка или за да се добијат докази при внатрешни истраги или дисциплински постапки, освен ако не е во прашање безбедносен инцидент заради кој е воспоставен видеонадзорот согласно Законот за заштита на личните податоци. (Во исклучителни околности, податоците може да бидат пренесени до истражните органи во рамките на формална дисциплинска или кривична истрага).

Камерите за видеонадзор се инсталираат на _____ и се поставени и фокусирани така што се снимаат само лица кои ќе пристапат до службените/деловните простории (објекти), вклучително и имотот (на пример за паркирање).

Системот со видеонадзор ја опфаќа областа на: да се даде детален опис (на пример: влезните и излезните места на зградата, влезните места во зградата, гаража и надворешна површина на зградата...)

2. Какви податоци собира Контролорот?

Контролорот собира само слики фатени на камерите, при што не се врши тонско снимање.

3. Кој е одговорен за обработка на податоците?

Контролорот е субјект кое ја врши обработката на личните податоци и кое ги утврдува целите на обработка, единствено во согласност со Законот за заштита на личните податоци. Покрај тоа, _____ е лице за контакт и одговорно за видеонадзорот.

4. Кој е правниот основ за обработка на личните податоци преку системот за видеонадзор?

Контролорот користи опрема за видеонадзор за (да се неведе една или повеќе од наведените цели):

- заштита на животот или здравјето на луѓето;
- заштита на сопственоста;
- заштита на животот и здравјето на вработените поради природата на работата; или

- обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории.

Затоа, обработката е законска согласно член 90 од Законот за заштита на личните податоци.

Покрај тоа, на влезот на _____, има видливо и јасно истакнато известување за видеонадзорот кое им овозможува на субјектите на лични податоци да се запознаат со вршењето на видеонадзорот, како и за називот на контролорот кој го врши видеонадзорот и за начинот на кој може да се добијат информации за тоа каде и колку време се чуваат снимките од системот за видеонадзор.

5. Кој може да ги види моите лични податоци?

До видео записите може да се пристапи само од страна на овластените лица за видеонадзор (на пример: членовите на безбедносниот персонал на Контролорот или од ангажираната Агенција за приватно обезбедување). Пристапот до дигиталниот уред или дискот на кој се чуваат видео записите е ограничен, заштитен со примена на технички мерки за безбедност на податоците (лозинка, запис за секој настан или акција од вработените, односно овластените лица). До податоците, односно видео записите не може да се пристапи без овластување од страна на _____.

6. Како да ги контролирате вашите податоци?

Може да испратите барање на _____ (на пример: е-пошта на _____@____.mk, адреса _____).

7. Можам ли да пристапам до моите податоци?

Вие имате право да пристапите до вашите податоци во секое време и бесплатно, со испраќање на барање до _____, или преку е-пошта до: _____@____.mk.

8. Можам ли да ги менувам моите податоци?

Не е дозволено изменување на видео записот за видеонадзор.

9. Може ли да побарам ограничување на обработката на моите податоци?

Вие имате право да ја ограничите обработката на вашите лични податоци во секое време со испраќање на барање на _____ (на пример: е-пошта на _____@____.mk, адреса _____.), кога ја оспорувате точноста на вашите лични податоци, или кога на Контролорот повеќе не му се потребни податоците за извршување на неговите задачи. Вие исто така можете да ја блокирате обработка и кога работењето е незаконско и вие се спротивставувате на бришење на податоците. Сепак, блокирањето не е можно во секој случај на службена истрага.

10. Дали можам да ги избришам моите податоци?

Вие имате право да ги избришете вашите податоци во секое време со испраќање на барање на _____ (на пример: е-пошта на _____@____.mk, адреса _____.), кога обработката е незаконска.

11. Дали се споделуваат моите лични податоци со други лица?

Вашите податоци се чуваат во Контролорот, освен ако не побарате од Контролрот или пак дадете согласност истите да бидат споделени. Во случај на споделување на Вашите податоци со трети страни, ќе бидете известени на кого се откриени, за која цел и врз кој законски основ.

12. Дали имам право на приговор?

Да, имате право на приговор и да се спротивставите на обработката во кое било време со испраќање на барање на _____ (на пример: е-пошта на _____@____.mk, адреса

_____.), кога имате легитимни причини во врска со вашата конкретна ситуација. Контролорот ќе постапи по вашето барање во рок од 15 дена од денот на поднесување на барањето.

13. Што можам да направам во случај на проблем?

а) Првиот чекор е да го известите Контролорот со испраќање е-пошта до _____@____.mk и да побарате да преземе акција.

б) Вториот чекор, ако не добиете одговор од нас или ако не сте задоволни од тоа, контактирајте со нашиот офицер за заштита на личните податоци на dpo@_____.мк.

в) Во секое време можете да поднесете барање до Агенцијата за заштита на личните податоци www.azlp.mk, која ќе постапи по вашето барање и ќе ги донесе потребните мерки.

14. Кога ќе започне обработката на моите лични податоци преку системот за видеонадзор?

Обработката започнува во моментот кога ќе ги посетите просториите на Контролорот.

15. Безбедност на личните податоци

Контролорот е посветен на заштита на вашите лични податоци. Затоа, користи безбедносни технологии и процедури со кои се заштитуваат вашите лични податоци пред се од неовластен пристап, употреба или откривање. Ние ги чуваме вашите податоци на компјутерски системи со ограничен пристап и во контролирана околина.

16. Колку долго ги чуваме вашите податоци?

Контролорот ќе ги чува вашите лични податоци _____ календарски денови по вашата посета во нашите простории, по што сите снимени видеозаписи автоматски се бришат.

1610.

Врз основа на член 92 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА СОДРЖИНАТА НА АНАЛИЗАТА НА ЦЕЛТА, ОДНОСНО ЦЕЛИТЕ ЗА КОЈА СЕ ПОСТАВУВА ВИДЕОНАДЗОРОТ И ИЗВЕШТАЈОТ ОД ИЗВРШЕНА ПЕРИОДИЧНА ОЦЕНКА НА ПОСТИГНАТИТЕ РЕЗУЛТАТИ ОД СИСТЕМОТ ЗА ВРШЕЊЕ ВИДЕОНАДЗОР

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишува содржината на анализата на целта, односно целите за која се поставува видеонадзорот пред започнување на процесот за воспоставување на систем за вршење на видеонадзор, како и содржината на извештајот од извршена периодична оценка на постигнатите резултати од системот за вршење видеонадзор.

Член 2

Одредбите од овој правилник се применуваат и при обработка на личните податоци преку вршење на видеонадзор од страна на обработувачот на збирка на лични податоци.

II. СОДРЖИНА НА АНАЛИЗАТА НА ЦЕЛТА, ОДНОСНО ЦЕЛИТЕ ЗА КОЈА СЕ ПОСТАВУВА ВИДЕОНАДЗОРОТ

1. Процес на изработување анализа

Член 2

(1) Во смисла на член 92 став (1) од Законот за заштита на личните податоци, контролорот е должен да изврши анализа на целта, односно целите за која се поставува видеонадзорот пред започнување на процесот за воспоставување на систем за вршење на видеонадзор.

(2) Анализата од ставот (1) на овој член се доставува на мислење до офицерот за заштита на личните податоци во контролорот.

(3) Врз основа на изготвената анализа, а по добиеното мислење од офицерот за заштита на личните податоци, од страна на функционерот, или на одговорното лице на контролорот се донесува одлука по однос на воспоставувањето на систем за вршење видеонадзор.

(4) По исклучок од став (2) на овој член, во случај кога се воспоставува систем за вршење на видеонадзор, а не е определен офицер за заштита на личните податоци, најдоцна до завршувањето на анализата, а пред донесувањето на одлуката по однос на воспоставувањето на системот за вршење видеонадзор, контролорот е должен да определи и офицер за заштита на личните податоци, во кој случај офицерот доставува мислење за анализата во разумен рок, но не подолго од 30 дена од денот на добиената анализа.

2. Содржина на анализата

Член 3

(1) Анализата од членот 2 на овој правилник ги содржи најмалку следните податоци:

- законски основ, односно цел или цели во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кои се воспоставува видеонадзорот;
- причини за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите;
- дали поставувањето на видеонадзор е обврска согласно друг закон (со образложение);
- опис на недвижните и движните ствари, односно простор кои ќе се заштитуваат со поставувањето на видеонадзорот;
- други мерки кои се разгледани за исполнување на целта, односно целите заради која се воведува системот за вршење на видеонадзор и причините поради кои овие мерки не се доволни односно не се прифатени од контролорот за да се исполни целта односно целите заради кои се воспоставува систем за вршење на видеонадзор;
- категории на субјекти на лица кои ќе се снимаат (на пример: вработени, клиенти...);
- дали со видеонадзорот ќе се обработуваат лични податоци на деца;
- категории на лични податоци кои ќе се обработуваат преку системот за видеонадзор;
- начин за информирање дека се врши видеонадзор на различните категории на субјекти на лични податоци кои ќе бидат опфатени со видеонадзорот (на пример: посебно информирање на вработените, истакнување на известување за видеонадзор...);
- начин за остварување на правата на субјектите на лични податоци;
- начин на обука на овластените лица кои ќе имаат пристап до системот за видеонадзор;
- начин на доделување на привилегии за пристап до системот за видеонадзор;
- период за кој ќе биде поставен видеонадзор (постојано, за определен период);
- временски период во кој биде активен видеонадзорот (24/7, по завршување на работното време и сл.);
- дали преку видеонадзорот ќе се обработуваат лични податоци само во реално време (мониторирање) или ќе се врши и снимање;
- период на чување на снимките соодветен на целта, односно целите, заради која/кои се поставува видеонадзорот;
- кој ќе има пристап до видеонадзорот (лица вработени во контролорот, односно обработувачот) и број на лица кои ќе имаат пристап до видеонадзорот;
- информации за предвидена обука за заштита на личните податоци за лицата кои ќе имаат пристап до видеонадзорот;
- примена на мерки за техничка и интегрирана заштита на личните податоци (Data protection by design and by default);
- оценка на нивото на технички и организациски мерки кои треба да се применат;
- проценка на бројот на потребни камери кои ќе се постават;
- тип/вид на камери (подвижни, статични, резолуција, опција за зумирање, ноќно снимање...);
- доколку повеќе контролори заеднички вршат видеонадзор (заеднички контролори), тогаш се утврдуваат целите и начините на обработка преку системот за видеонадзор, како и податоци за начинот на кој што е уреден нивниот меѓусебен однос (на пример: со договор, закон којшто се применува на тие контролори, итн);
- период до кога ќе се донесе актот во кој што ќе се уреди начинот на вршење на видеонадзорот;
- име, презиме и потпис на лицата кои ја вршеле анализата на целта, односно целите заради кои се воспоставува системот за вршење на видеонадзор;
- датум (период) кога е вршена анализата;
- дали е консултиран офицерот за заштита на личните податоци на контролорот за воспоставувањето на систем за видеонадзор;
- оценка/мислење од офицерот за заштита на личните податоци (дадено врз основа на анализата за: потребата од воспоставување на видеонадзор, степенот на

влијание врз приватноста на субјектите на лични податоци кои ќе бидат опфатени со видеонадзорот - лица кои ќе се снимаат, соодветноста на целите/основите за кои се поставува видеонадзорот, мерките за техничка и интегрирана заштита на личните податоци, техничките и организациските мерки кои треба да се применат...);

- име, презиме и потпис на офицерот за заштита на личните податоци;

- одлука на функционерот, или на одговорното лице на контролорот за воспоставување на систем за видеонадзор;

- име, презиме и потпис на функционерот, или на одговорното лице на контролорот; и

- други податоци согласно проценката на контролорот.

(2) Образецот на Анализата на целта, односно целите за кои се поставува видеонадзорот е составен дел на овој правилник Образец бр.1.

III. СОДРЖИНА НА ИЗВЕШТАЈОТ ОД ИЗВРШЕНА ПЕРИОДИЧНА ОЦЕНКА НА ПОСТИГНАТИТЕ РЕЗУЛТАТИ ОД СИСТЕМОТ ЗА ВРШЕЊЕ ВИДЕОНАДЗОР

Член 4

(1) Во смисла на член 92 став (3) од Законот за заштита на личните податоци, контролорот е должен да врши периодична оценка на постигнатите резултати од системот за вршење видеонадзор на секои две години, а особено за:

- понатамошната потреба од користење на системот за вршење на видеонадзор;

- целта, односно целите за вршење на видеонадзор; и

- можните технички решенија за замена на системот за вршење на видеонадзор.

(2) Од извршената оценка од ставот (1) на овој член, контролорот е должен да изработи извештај како составен дел на документацијата за воспоставениот систем за вршење на видеонадзор.

(3) Во извештајот од ставот (2) на овој член, контролорот задолжително ги внесува и статистичките показатели за пристапот до снимките направени при вршење на видеонадзорот, како и начинот на искористување на снимките.

(4) Извештајот од периодичната оценка се доставува до офицерот за заштита на личните податоци и до функционерот, односно до одговорното лице на контролорот.

(5) Покрај податоците од ставовите (1) и (3) на овој член, во извештајот се внесуваат најмалку и следните податоци:

- датум на воспоставување на системот за вршење на видеонадзорот;

- датум (период) кога е извршена периодичната оценка;

- датум на претходно извршената периодична оценка;

- оценка дали видеонадзорот ја исполнува односно соодветствува на целта или целите во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кој е воспоставен видеонадзорот;

- оценка дали причините за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите, сеуште се релевантни;

- оценка дали начинот за информирање дека се врши видеонадзор на различните категории на субјекти на лични податоци кои се опфатени со видеонадзорот (на пример: посебно информирање на вработените, истакнување на известување за видеонадзор...) е соодветен;

- статистички показатели за поднесени барања за остварување на правата на субјектите на лични податоци од видеонадзорот;

- податоци од евиденција на корисници, за снимки кои се дадени на користење (статистички податоци, корисници, правен основ, причини);

- статистички податоци од пријавени инциденти поврзани со системот за вршење на видеонадзор;

- статистички податоци за нарушување на безбедноста на личните податоци кои се обработуваат преку системот за вршење видеонадзор;

- оценка на периодот на чување на снимките дали истиот е соодветен со предлог истиот да се скрати или продолжи (но не повеќе од законски утврдениот рок);

- оценка дали има потреба од намалување или зголемување бројот на лица кои ќе имаат пристап до видеонадзорот;

- потреба од континуирана обука на овластените лица (предлог тема на обуката, број на лица што треба да бидат обучени);

- оценка дали целосно се применети мерките за техничка и интегрирана заштита на личните податоци (Data protection by design and by default);

- оценка дали нивото на технички и организациски мерки кои се применуваат е соодветно;

- предлог за намалување/зголемување на број камери соодветно на нивото на исполнување на целта/целите заради кои е поставен видеонадзорот;

- понатамошната потреба од користење на системот за вршење на видеонадзор;

- за спроведената проценка на влијанието на заштитата на личните податоци;

- дали редовно се преиспитува проценката на влијанието на заштитата на личните податоци, особено кога има значајни промени во системот за видеонадзор;

- можни технички или други решенија за замена на системот за вршење на видеонадзор;

- име, презиме и потпис на лицата кои ја вршеле периодична оценка на постигнатите резултати од системот за вршење видеонадзор;

- датум на доставување на извештајот од периодичната оценка до офицерот за заштита на личните податоци во контролорот;

- мислење и предлози од офицерот за заштита на личните податоци во контролорот;

- датум на доставување на извештајот од периодичната оценка до функционерот, односно до одговорното лице во контролорот; и

- други податоци согласно проценката на контролорот.

(6) Замена или надградба на веќе воспоставен систем за видеонадзор на период пократок од две години се врши по задолжително претходно направена периодична оценка на постигнатите резултати од системот за вршење видеонадзор.

(7) Образецот на Извештајот од ставот (2) на овој член е составен дел на овој правилник Образец бр. 2.

IV. ЗАВРШНА ОДРЕДБА

Член 4

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-604/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1

Анализа на целта, односно целите за која/кои се поставува видеонадзорот во

_____

(контролор)
I

1.	Датум (период) кога е вршена анализата	
2.	Законски основ, односно цел или цели во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кои се воспоставува видеонадзорот	
3.	Дали поставувањето на видеонадзор е обврска согласно друг закон (со образложение)	
4.	Опис на недвижните и движните ствари, односно простор кои ќе се заштитуваат со поставувањето на видеонадзорот	
5.	Други мерки кои се разгледани за исполнување на целта заради која се воведува системот за вршење на видеонадзор и причините поради кои овие мерки не се доволни за да се исполни целта односно целите заради кои се имплементира систем за вршење на видеонадзор	
6.	Категории на субјекти на лични податоци кои ќе се снимаат	
7.	Дали со видеонадзорот ќе се обработуваат лични податоци на деца	
8.	Категории на лични податоци кои ќе се обработуваат преку системот за видеонадзор	
9.	Начин за информирање дека се врши видеонадзор на различните категории на субјекти на лични податоци кои ќе бидат опфатени со видеонадзорот (пр. посебно информирање на вработените, истакнување на известување за видеонадзор...)	
10.	Начин за остварување на правата на субјектите на лични податоци	
11.	Начин на доделување на привилегии за пристап до видеонадзор	
12.	Период за кој ќе биде поставен видеонадзор (неопределен период/определен период)	
13.	Временски период во кој биде активен видеонадзорот (24/7, по завршување на работното време и сл.)	
14.	Дали преку видеонадзорот ќе се обработуваат лични податоци само во реално време (мониторирање) или ќе се врши и снимање	
15.	Период на чување на снимките соодветен на целта/целите заради која/кои се поставува видеонадзорот	
16.	Кој ќе има пристап до видеонадзорот (лица вработени во контролорот, односно обработувачот) и број на лица кои ќе имаат пристап до видеонадзорот	
17.	Информации за предвидена обука за заштита на личните податоци за лицата кои ќе имаат пристап до видеонадзорот	
18.	Примена на мерки за техничка и интегрирана заштита на личните податоци (Data protection by design and by default)	
19.	Оценка на нивото на технички и организациски мерки кои треба да се применат	
20.	Проценка за број на потребни камери кои ќе се постават	
21.	Тип/вид на камери (подвижни, статични, резолуција, опција за зумирање, ноќно снимање...)	
22.	Доколку повеќе контролори заеднички вршат видеонадзор (заеднички контролори), тогаш се утврдуваат целите и начините на обработка преку системот за видеонадзор, како и податоци за начинот на кој што е уреден нивниот меѓусебен однос (на пример: со договор, закон којшто се применува на тие контролори, итн)	
23.	Период до кога ќе се донесе акт во кој што ќе се уреди начинот на вршење на видеонадзорот	
24.	Други податоци согласно проценката на контролорот	

II

1. Дали е консултиран офицерот за заштита на личните податоци на контролорот за воспоставувањето на систем за видеонадзор?

   ДА / НЕ (да се заокружи)

2. Оценка/мислење од офицерот за заштита на личните податоци

   _____
   _____
   _____
   _____
   _____
   _____
   _____

4. Име, презиме и потпис на лицата кои ја вршеле анализата на целта односно целите заради кои се воспоставува системот за вршење на видеонадзор

   _____
   _____
   _____
   _____
   _____

5. Име, презиме и потпис на офицерот за заштита на личните податоци

   _____
   _____
   _____

6. Одлука на функционерот, или на одговорното лице за воспоставување на систем за видеонадзор (дадено врз основа на анализата за: потребата од воспоставување на видеонадзор, степенот на влијание врз приватноста на субјектите на лични податоци кои ќе бидат опфатени со видеонадзорот – лица кои ќе се снимаат, соодветноста на целите/основите за кои се поставува видеонадзорот, мерките за техничка и интегрирана заштита на личните податоци, техничките и организациските мерки кои треба да се применат...):

   _____
   _____
   _____
   _____
   _____

7. Име, презиме и потпис на функционерот, или на одговорното лице во контролорот

   _____
   _____
   _____
   _____

Образец бр. 2

Извештај од извршена периодична оценка на постигнатите резултати од системот за вршење видеонадзор во

_____

(Контролор)

I

1.	Датум на воспоставување на системот за вршење на видеонадзор	
2.	Датум (период) кога е извршена периодичната оценка	
3.	Датум од претходно извршена периодична оценка	
4.	Оценка дали видеонадзорот ја исполнува односно соодветствува на целта или целите во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кој е воспоставен видеонадзорот	
5.	Оценка дали причините за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите, сеуште се релевантни	
6.	Статистички показатели за пристапот до снимките направени при вршење на видеонадзорот	
7.	Статистички показатели за начинот на искористување на снимките	
8.	Оценка дали начинот за информирање дека се врши видеонадзор на различните категории на субјекти на лични податоци кои се со видеонадзорот (пр. посебно информирање на вработените, истакнување на известување за видеонадзор...) е соодветен;	
9.	Статистички показатели за поднесени барања за остварување на правата на субјектите на лични податоци од видеонадзорот	
10.	Податоци од евиденцијата на корисници, за снимки кои се дадени на користење (статистички податоци, корисници, правен основ, причини)	
11.	Статистички податоци од пријавени инциденти поврзани со системот за вршење на видеонадзор;	
12.	Статистички податоци за нарушување на безбедноста на личните податоци кои се обработуваат преку системот за вршење видеонадзор	
13.	Оценка на периодот на чување на снимките дали истиот е соодветен со предлог истиот да се скрати или продолжи (но не повеќе од законски утврдениот рок)	
14.	Оценка дали има потреба од намалување или зголемување бројот на лица кои ќе имаат пристап до видеонадзорот	
15.	Потреба од континуирана обука на овластените лица (предлог тема на обуката, број на лица што треба да бидат обучени)	
16.	Оценка дали целосно се применети мерките за техничка и интегрирана заштита на личните податоци (Data protection by design and by default)	
17.	Оценка дали нивото на технички и организациски мерки кои се применуваат е соодветно	
18.	Предлог за намалување/зголемување на број камери соодветно на нивото на исполнување на целта/целите заради кои е поставен видеонадзорот	
19.	Целта, односно целите за вршење на видеонадзор	
20.	Оценка дали причините за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите сеуште се релевантни	
21.	Оценка дали видеонадзорот ја исполнува односно соодветствува на целта или целите во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кој е воспоставен видеонадзорот	

22.	Податоци за спроведената проценка на влијанието на заштитата на личните податоци	
23.	Дали редовно се преиспитува проценката на влијанието на заштитата на личните податоци, особено кога има значајни промени во системот за видеонадзор	
24.	Дали има понатамошната потреба од користење на системот за вршење на видеонадзор	
25.	Можни технички или други решенија за замена на системот за вршење на видеонадзор	
26.	Други податоци согласно проценката на Контролорот	

II

1. Име, презиме и потпис на лицата кои ја вршеле периодична оценка на постигнатите резултати од системот за вршење видеонадзор

_____
_____
_____
_____
_____

2. Датум на доставување на извештајот од периодичната оценка до офицерот за заштита на личните податоци во контролорот

_____
_____
_____
_____

3. Мислење и предлози од офицерот за заштита на личните податоци во контролорот

_____
_____
_____
_____
_____

4. Датум на доставување на извештајот од периодичната оценка до функционерот, или до одговорното лице во контролорот

_____
_____
_____
_____
_____

1611.

Врз основа на член 104 став (7) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА НАЧИНОТ НА ВРШЕЊЕ НА СУПЕРВИЗИЈА

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишува начинот на вршење на супервизија од страна на супервизорот за заштита на личните податоци (во натамошниот текст: супервизор) кај контролорите, како и формата, содржината и начинот на водење на евиденција за извршените супервизии.

Член 2

Одредбите од овој правилник се применуваат и при вршењето на супервизија над обработувачот на збирка на лични податоци.

II. ПЛАНИРАЊЕ НА СУПЕРВИЗИЈАТА

Член 3

(1) Супервизијата се врши согласно Годишната програма за вршење на супервизија и месечните планови за вршење на супервизија, донесени од страна на директорот на Агенцијата за заштита на личните податоци (во натамошниот текст: директор на Агенцијата).

(2) По исклучок од ставот (1) на овој член, во случај кога директорот на Агенцијата е отсутен или кога поради болест и други причини не е во можност да ја врши својата функција, месечните планови за вршење на супервизија ги донесува заменик директорот на Агенцијата, односно раководниот административен службеник кој раководи со Секторот за супервизија.

Член 4

Годишната програма за вршење на супервизија се изработува врз основа на проценка на ризикот со цел пропорционално идентификување на областите и контролорите со висок ризик преку анализирање на:

- случаите од нарушувањата на безбедноста на личните податоци;
- статистичките податоци од претходно извршените супервизии;
- бројот и природата на поднесени иницијативи за вршење на супервизија;
- бројот и природата на поднесени барања за утврдување на повреда на правото за заштита на личните податоци;
- податоците во однос на поднесени претставки и предлози по вид, број и области; поднесени барања за одобрение за обработка на матичен број на граѓанинот; поднесени барања за одобрение за обработка на посебни категории на лични податоци; поднесени барања и пријави за пренос на лични податоци; како и пријавени збирки на лични податоци со висок ризик.

Член 5

(1) Предлогот на Годишна програма за вршење на супервизија, Секторот за супервизија го доставува до директорот на Агенцијата, најдоцна до 20 декември во тековната година.

(2) Годишната програма за вршење на супервизија директорот на Агенцијата ја донесува најдоцна до 31 декември во тековната година.

(3) По донесувањето на Годишната програма за вршење на супервизија за наредната година, истата се објавува на веб страницата на Агенцијата.

Член 6

(1) Месечните планови за вршење на супервизија се изработуваат врз основа на проценка на ризикот за секој контролор според потенцијалното влијание или веројатноста за ризик врз правата и слободите на физичките лица.

(2) Ризикот од ставот (1) на овој член, се проценува врз основа на следните специфични фактори:

- „историјата“ на усогласеност на контролорот, а врз основа на барања за утврдување на повреда на правото за заштита на личните податоци или иницијативи за вршење на супервизија поднесени до Агенцијата и одговорите на контролорот;
- „самоиницијативното“ пријавување на нарушувања на безбедноста на личните податоци и активности кои што ги идентификувал контролорот за справување со нарушувањета;
- комуникациите со контролорот кои што укажуваат на недостаток на контроли за усогласеност и/или слабо разбирање на прописите за заштита на личните податоци;
- јавно достапни информации, а кои потенцираат проблеми во обработката на личните податоци од контролорот и информации од други органи од државната власт, државни органи и институции;
- изјави за внатрешна контрола и/или други информации објавени од контролорот кои ги потенцираат проблемите при обработката на личните податоци;
- внатрешна или надворешна ревизија спроведена кај контролорот поврзани со заштитата на податоците и обработка на лични податоци;
- имплементација на нови системи или процеси од страна на контролорот, а кога постои јавна загриженост дека приватноста може да биде во опасност;
- обемот и природата на личните податоци што се обработуваат;
- почитувањето на одобрен кодекс на однесување или на одобрен механизам за сертификација од страна на контролорот;
- согледаното влијание врз физичките лица од какво било потенцијално непочитување на прописите за заштита на личните податоци; и
- други релевантни информации, како на пример: проценки на влијанието на заштитата на личните податоци извршени од контролорот.

(3) При утврдување на потенцијалното влијание на неусогласеноста врз физичките лица, се земаат во предвид особено следните фактори: бројот на лицата кои се потенцијално засегнати; природата и чувствителноста на личните податоци кои што се обработуваат,како и природата и степенот на евентуалната штета или вознемиреноста предизвикана од таа неусогласеност.

Член 7

(1) Изборот на контролорите кои ќе бидат опфатени со месечните планови за вршење на супервизија се врши од страна на директорот на Агенцијата, а по предлог на Секторот за супервизија.

(2) Предлог-месечниот план за вршење на супервизија од ставот (1) на овој член, се доставува до директорот на Агенцијата на одобрување најдоцна до 15-ти во тековниот месец за наредниот месец.

Член 8

Месечните планови за вршење на супервизија содржат: број и вид на супервизии по контролори, област која ќе биде опфатена со супервизијата, опсег на супер-

визијата, збирки на лични податоци (ако е применливо), број на предвидени супервизии за секој супервизор, датум на отпочнување на супервизијата и забелешка.

Член 9

(1) Измени и дополнувања на Месечниот план за вршење на супервизија може да се вршат до денот на отпочнување на супервизијата по предлог, односно барање на:

- контролорот кај кој се врши супервизијата;
- супервизорот кој ја врши супервизијата;
- раководниот административен службеник кој раководи со Секторот за супервизија;
- директорот на Агенцијата; или
- како и по добивање на нови вонредни супервизии (поднесени барања за утврдување на повреда на правото на заштита на личните податоци и/или иницијативи за вршење на супервизија, односно пријавени случаи за нарушување на безбедноста на личните податоци).

(2) Измените и дополнувањата на Месечниот план за вршење на супервизија се одобруваат од страна на директорот на Агенцијата.

(3) По исклучок од ставот (2) на овој член, во случај кога директорот на Агенцијата е отсутен или кога поради болест и други причини не е во можност да ја врши својата функција, измените и дополнувањата на Месечниот план за вршење на супервизија се одобруваат од страна на заменик директорот на Агенцијата, односно раководниот административен службеник кој раководи со Секторот за супервизија.

III. НАЧИН НА ВРШЕЊЕ НА СУПЕРВИЗИЈА

Член 10

Заради извршување на супервизија над контролорот, супервизорот пред започнување на супервизијата презема подготвителни активности во зависност од случајот или од контролорот, и тоа:

1) разгледување на предметот (доколку има) од последната извршена супервизија кај контролорот и констатираните состојби;

2) разгледување на пријавените збирки на лични податоци со висок ризик (ако е применливо);

3) разгледување на мислења, укажувања, одобренија и друга кореспонденција со контролорот, кој е предмет на супервизија;

4) проучување на прописите од областа која е релевантна за извршување на супервизија;

5) преземање на неопходни технички и организациски мерки за подготвување и реализирање на супервизијата;

6) разгледување на основната листа за проверка; и

7) разгледување на јавно достапни информации.

Член 11

Со опсегот на супервизијата можат да бидат опфатени следните процеси од воспоставениот систем за заштита на личните податоци кај контролорот, и тоа:

- управување со системот за заштита на личните податоци и отчетност;
- обука и свесност за заштита на личните податоци;
- безбедност на личните податоци;
- права на субјектот на лични податоци и преносливост на податоците;
- управување и ангажирање на надворешни субјекти (обработувачи);
- управување со збирките на лични податоци; и
- проценка и управување со ризикот при обработката на личните податоци.

Член 12

(1) Редовната супервизија се врши во форма на ревизија над работењето на контролорот, а вонредната супервизија се спроведува како истражување (истрага) со цел да се идентификуваат пропусти и слабости во воспоставениот систем за заштита на личните податоци при собирањето, обработката и чувањето на личните податоци од страна на контролорот.

(2) Супервизијата може да биде: најавена или ненајавена, а по својот обем целосна или делумна.

(3) Супервизијата се врши во просториите на контролорот и во просториите на Агенцијата.

(4) За денот, видот, обемот и опсегот на вршење на супервизија, директорот на Агенцијата или од него овластениот раководен административен службеник кој раководи со Секторот за супервизија, го известува контролорот кај кој се врши супервизијата.

(5) Известувањето од ставот (4) на овој член содржи инструкции за начинот на електронско преземање на основната листа за проверка.

(6) Контролорот задолжително ја доставува до супервизорот пополнетата основна листа за проверка во рок од 10 дена од денот на приемот на истата.

Член 13

(1) Супервизорот е самостоен во вршењето на супервизијата и самостојно одлучува за дејствијата што треба да ги преземе при вршењето на супервизијата и за мерките кои ќе бидат изречени по извршената супервизија, согласно закон.

(2) При вршење на супервизија, супервизорот може да се користи со една или со повеќе од следните техники:

- истражување;
- користење на прашалници;
- интервјуирање;
- собирање на докази и друг начин на документирање;
- увид;
- набљудување; и
- користење на детална листа за проверка.

Член 14

(1) Супервизијата по правило се врши од еден супервизор, а по исклучок кога тоа е предвидено со Месечниот план за вршење на супервизија или по предлог на раководниот административен службеник кој раководи со Секторот за супервизија или директорот на Агенцијата, поради обемот или сложеноста на супервизијата, истата можат да ја вршат повеќе супервизори.

(2) При вршење на супервизија од страна на повеќе супервизори се составува еден записник и се донесува едно решение кое се потпишува од сите супервизори што учествувале при супервизијата.

(3) Записникот го изработува носителот на предметот, а останатите супервизори учествуваат во неговата изработка.

Член 15

(1) При вршење на супервизија, директорот на Агенцијата може да овласти да учествуваат и други административни службеници од Агенцијата или надворешни експерти.

(2) Во овластувањето од ставот (1) на овој член се определуваат правата и обврските на административните службеници или надворешните експерти.

(3) По исклучок од ставот (1) на овој член, во случај кога директорот на Агенцијата е отсутен или кога поради болест и други причини не е во можност да ја врши својата функција, овластувањето од ставот (1) на овој член се дава од страна на заменик директорот на Агенцијата, односно раководниот административен службеник кој раководи со Секторот за супервизија.

Член 16

(1) Во смисла на член 104 став (5) од Законот за заштита на личните податоци, при вршење на супервизија кај контролорот, може да се применуваат специјализирани софтверски алатки за испитување на информацискиот систем и информатичката инфраструктура во рамки на кои се врши обработка на личните податоци.

(2) Применувањето на софтверските алатки од ставот (1) на овој член, кои содржат инвазивни методи, се врши по предходен договор со контролорот.

(3) Во согласност со ставот (1) на овој член, при вршење на супервизија кај контролорот може да се проверуваат веб страници, мобилни апликации и други технолошки решенија, и тоа: политики за приватност, изјави за приватност, механизми за обезбедување на согласност од субјектите на лични податоци, политики за колачиња, усогласеност со барањата за колачиња, формулари за собирање на лични податоци, проверка на безбедноста на обработката на личните податоци, како и друга документација, политики, механизми и процеси кои ги применува контролорот при собирањето, обработката и чувањето на личните податоци.

Член 17

(1) По извршената супервизија, супервизорот составува записник кој особено содржи: назив и седиште, односно име и презиме и адреса на живеење на контролорот каде што е извршена супервизијата, време и место на вршење на супервизијата, име и презиме на супервизорот, имиња и презимиња на претставниците од контролорот кои се присутни при вршењето на супервизијата, податоци за добиената документација, разгледаните прописи, наод на состојбата и утврдени повреди.

(2) Во записникот од ставот (1) на овој член кој се однесува на редовната супервизија се дефинираат и оценуваат и ризиците со деталните наоди и проблемите утврдени со овие ризици при што се дава оценка за уверување за секоја област на опсегот на супервизијата, како и се наведуваат приоритетните препораки што можат да ги намалат тие ризици.

(3) Дефинициите за оценка од ставот (2) на овој член, се дадени во Прилогот бр.1 кој е составен дел на овој правилник.

Член 18

(1) Примерок од записникот од секоја извршена супервизија, супервизорот задолжително доставува до контролорот над кој е спроведена супервизијата и во документацијата.

(2) Примерок од управниот акт од секоја извршена супервизија, супервизорот задолжително доставува до контролорот над кој е спроведена супервизијата, до подносителот/подносителите во случај на извршена вонредна супервизија по поднесено барање, и во документацијата.

Член 19

(1) Во случај на поведување на управен спор по добивање на тужбата, супервизорот кој ја извршил супервизијата ја разгледува тужбата, изработува одговор и истиот го доставува до надлежниот суд согласно Законот за управните спорови.

(2) Во случаите кога Агенцијата поднесува жалба на одлука од надлежен суд, супервизорот кој ја извршил супервизијата ја разгледува одлуката, изработува аргументација за жалба и истата ја доставува до надлежниот суд, преку Државното правобранителство на Република Северна Македонија согласно Законот за управните спорови.

IV. ДОКУМЕНТАЦИЈА ЗА ИЗВРШЕНИТЕ СУПЕРВИЗИИ

Член 20

(1) Супервизорот за извршената супервизија води документација, согласно прописите за архивски материјал.

(2) Документацијата се составува само за една супервизија и ги содржи сите докази (во ракопис, копии или медиуми) за извршената супервизија.

(3) Документацијата од ставот (2) на овој член може да содржи:

- извештаи од интервјуа и белешки од различни активности;
- собрани информации/документации; и
- наоди, согледувања и писмена кои се однесуваат на извршената супервизија.

(4) Документацијата се подредува од известувањето за вршење на супервизија (најдолу) се до последниот донесен акт при супервизијата (најгоре).

(5) Водењето на документацијата се врши хронолошки според бројот и датумот на прием на предметот за супервизија согласно прописите за архивски материјал.

V. ЕВИДЕНЦИЈА ЗА ИЗВРШЕНИТЕ СУПЕРВИЗИИ

Член 21

(1) Во Агенцијата се води евиденција за извршените супервизии која особено содржи: реден број; поднесено барање за утврдување на повреда на правото на заштита на личните податоци, иницијатива за вршење на супервизија или пријавен случај за нарушување на безбедноста на личните податоци; податоци за супервизорот задолжен за предметот; име и презиме, односно назив на правното лице (контролор); адреса на живеење, односно седиште на правното лице (контролор); вид и опсег на супервизијата, област, сектор (јавен/приватен), број на предметот во евиденцијата; број и датум на записникот; број и датум кога е доставен записникот до контролорот; број и датум на решението; број и датум на доставување на решението; датум кога е завршена супервизијата; број и датум на поднесена тужба до надлежниот суд; број и датум на одговор на тужба до надлежниот суд; како е одлучено по тужбата; број и датум на поднесена жалба од Агенцијата; како е одлучено по жалбата; број и датум на поднесено Барање за поведување на прекршочна постапка и број и датум на донесената одлука на Комисијата за одлучување по прекршок, како е решено по барањето и забелешки.

(2) Евиденцијата од ставот (1) на овој член се води електронски преку систем за автоматска обработка на податоците.

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 22

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за начинот на вршење на инспекцискиот надзор („Службен весник на Република Македонија“ бр. 207/16 и 59/17), освен за случаите предвидени во членот 117 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20).

Член 23

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-600/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Прилог бр. 1

Оценка на редовната супервизија

Редовната супервизија се оценува според целокупното мислење за уверувањето во однос на секоја област на опсегот, при што сите прашања и придружни препораки се класифицираат индивидуално за да ја означат нивната важност, во согласност со следниве дефиниции:

Код за боја	Мислење	Приоритетни препораки	Дефиниции
	Високо уверување	Низок приоритет	Постои високо ниво на уверување дека процесите и процедурите се воспоставени и овозможуваат усогласеност со прописите за заштита на личните податоци. Супервизијата идентификуваше само мал обем за подобрување на постојните аранжмани при што тоа нема да предизвика значителни дополнителни активности за да се намали ризикот од неусогласеност со прописите за заштита на личните податоци.
	Разумно уверување	Среден приоритет	Постои разумно ниво на уверување дека процесите и процедурите се воспоставени и овозможуваат усогласеност со прописите за заштита на личните податоци. Супервизијата идентификуваше забележлив обем за подобрување на постојните аранжмани со цел да се намали ризикот од неусогласеност со прописите за заштита на личните податоци.
	Ограничено уверување	Висок приоритет	Постои ограничено ниво на уверување дека процесите и процедурите се воспоставени и овозможуваат усогласеност со прописите за заштита на личните податоци. Супервизијата идентификуваше значителен обем за подобрување на постојните аранжмани за да се намали ризикот од неусогласеност со прописите за заштита на личните податоци.
	Многу ограничено уверување	Итен приоритет	Постои многу ограничено ниво на уверување дека процесите и процедурите се воспоставени и овозможуваат усогласеност со прописите за заштита на личните податоци. Супервизијата идентификуваше суштински ризик дека целта за усогласеност со прописите за заштита на личните податоци нема да се постигне. Потребно е итно дејствување за да се подобри контролираната околина.

1612.

Врз основа на член 56 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци, донесе

П Р А В И Л Н И К
ЗА ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ

I. ОПШТА ОДРЕДБА

Член 1

Со овој правилник се пропишува начинот на известувањето за пренос на лични податоци во земјите членки на Европската Унија и за земјите членки на Европскиот економски простор, формата и содржината на образецот на барањето за добивање на одобрение за пренос за случаите предвидени со закон, како и формата и содржината на образецот за евиденцијата на извршениот пренос на лични податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор, како и начинот на водење на евиденцијата.

II. НАЧИН НА ИЗВЕСТУВАЊЕ ЗА ПРЕНОСОТ НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЗЕМЈИТЕ ЧЛЕНКИ НА ЕВРОПСКАТА УНИЈА И ЗА ЗЕМЈИТЕ ЧЛЕНКИ НА ЕВРОПСКИОТ ЕКОНОМСКИ ПРОСТОР

Член 2

(1) Во смисла на член 48 став (3) од Законот за заштита на личните податоци, при пренос на лични податоци во земјите членки на Европската Унија и Европскиот економски простор, контролорот или обработувачот задолжително доставува пријава за пренос на лични податоци.

(2) Пријавата за пренос на лични податоци од ставот (1) на овој член, контролорот или обработувачот ја доставува до Агенцијата за заштита на личните податоци (во натамошниот текст: Агенција) електронски преку системот на е-пријави на Агенцијата или преку електронска пошта во скенирана копија, во рок од 15 дена пред денот на започнување на преносот на лични податоци.

(3) Пријавата за пренос на лични податоци од ставот (1) на овој член, треба да биде потпишана своерачно или со електронски потпис во согласност со прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги, од страна на лицето кое го претставува и застапува контролорот или обработувачот кој врши пренос на лични податоци.

(4) Образецот на пријавата за пренос на лични податоци од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 1).

III. ФОРМА И СОДРЖИНА НА ОБРАЗЕЦОТ НА БАРАЊЕТО ЗА ДОБИВАЊЕ НА ОДОБРЕНИЕ ЗА ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ ВО ТРЕТИ ЗЕМЈИ И МЕЃУНАРОДНИ ОРГАНИЗАЦИИ

1. Форма и содржина на образецот на барањето за добивање на одобрение за пренос на лични податоци во трети земји и меѓународни организации врз основа на одлука за соодветност

Член 3

(1) За пренос на лични податоци во трети земји и меѓународни организации за кој Агенцијата донесува одлука за соодветност согласно член 49 став (3) од Законот за заштита на личните податоци, контролорот или обработувачот потребно е да поднесат Барање за добивање на одобрение за пренос на лични податоци.

(2) Образецот на Барањето за добивање на одобрение за пренос на лични податоци од ставот (1) од овој член е составен дел на овој правилник (Образец бр. 2).

(3) При донесувањето на одлуката за соодветност, Агенцијата ги зема во предвид одлуките на Европската Унија со кои има утврдено дека одредени трети земји обезбедуваат соодветен степен на заштита на личните податоци како и дали третите земјите се потписнички на Конвенцијата 108 на Советот на Европа.

(4) Барањето за добивање на одобрение за пренос на лични податоци од ставот (1) на овој член, контролорот или обработувачот го доставува до Агенцијата електронски преку системот на е-пријави на Агенцијата или преку електронска пошта во скенирана копија, во рок од 15 дена пред денот на започнување на преносот на лични податоци.

(5) Барањето за добивање на одобрение за пренос на лични податоци од ставот (1) на овој член, треба да биде потпишано своерачно или со електронски потпис во согласност со прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги, од страна на лицето кое го претставува и застапува контролорот или обработувачот кој врши пренос на лични податоци.

2. Формата и содржината на образецот на барањето за добивање на одобрение за пренос на лични податоци во трети земји и меѓународни организации врз основа на предвидени соодветни заштитни мерки

Член 4

(1) Во случаите за кои се бара одобрение од страна на Агенцијата, контролорот или обработувачот потребно е да поднесат барање за добивање на одобрение за пренос на лични податоци.

(2) Кон барањето за добивање на одобрение за пренос од ставот (1) на овој член, контролорот или обработувачот потребно е да достави документација за предвидените соодветни заштитни мерки согласно членот 50 став (3) од Законот за заштита на личните податоци.

(3) Образецот на Барањето за добивање на одобрение за пренос на лични податоци согласно ставот (1) од овој член е составен дел на овој правилник (Образец бр. 3).

(4) Барањето за добивање на одобрение за пренос на лични податоци од ставот (1) на овој член, контролорот или обработувачот го доставува до Агенцијата електронски преку системот на е-пријави на Агенцијата или преку електронска пошта во скенирана копија, во рок од 15 дена пред денот на започнување на преносот на лични податоци.

(5) Барањето за добивање на одобрение за пренос на лични податоци од ставот (1) на овој член, треба да биде потпишано своерачно или со електронски потпис во согласност со прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги, од страна на лицето кое го претставува и застапува контролорот или обработувачот кој врши пренос на лични податоци.

3. Форма и содржината на образецот на барањето за одобрување на задолжителни корпоративни правила

Член 5

(1) При пренос на лични податоци врз основа на задолжителни корпоративни правила контролорот или обработувачот потребно е да поднесе барање за одобрување на задолжителните корпоративни правила.

(2) Образецот на барањето согласно ставот (1) од овој член, е составен дел на овој правилник (Образец бр. 4).

(3) Барањето од ставот (1) на овој член, контролорот или обработувачот го доставува електронски преку системот на е-пријави на Агенцијата или преку електронска пошта во скенирана копија, во рок од 15 дена пред денот на започнување на преносот на лични податоци.

(4) Барањето од ставот (1) на овој член, треба да биде потпишано своерачно или со електронски потпис во согласност со прописите што ја уредуваат употребата на електронски документи, електронска идентификација и доверливи услуги, од страна на лицето кое го претставува и застапува контролорот или обработувачот кој врши пренос на лични податоци.

(5) Кон барањето од ставот (1) на овој член, контролорот или обработувачот потребно е да достави документација со која се докажува дека се исполнети условите предвидени во членот 51 од Законот за заштита на личните податоци.

IV. ФОРМА И СОДРЖИНА НА ОБРАЗЕЦОТ ЗА ЕВИДЕНЦИЈАТА НА ИЗВРШЕНИОТ ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ ВО ТРЕТИ ЗЕМЈИ И МЕЃУНАРОДНИ ОРГАНИЗАЦИИ, ЕВРОПСКАТА УНИЈА И ЕВРОПСКИОТ ЕКОНОМСКИ ПРОСТОР

Член 6

(1) Образецот на евиденцијата на извршениот пренос на лични податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор ги содржи следниве податоци:

1. Реден број;
2. Податоци за контролорот или обработувачот кој го врши преносот и тоа:
- назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице;
- контакт-телефон;
- електронска пошта; и
- име и презиме на овластеното лице задолжено за пренесените лични податоци.
3. Држава во која ќе се врши преносот;
4. Податоци за примачот на лични податоци (контролор, обработувач или заеднички контролор)
- назив и седиште за правно лице, името и презимето и адреса на живеење за физичко лице;
- контакт-телефон;
- електронска пошта; и
- име и презиме на овластеното лице задолжено за применените лични податоци.
5. Категории на субјектите на лични податоци чии лични податоци ќе бидат предмет на пренос;
6. Цел или цели на преносот на личните податоци;
7. Категории на личните податоци кои се пренесуваат;
8. Посебни категории на лични податоци кои се пренесуваат;
9. Рок на чување на пренесените лични податоци;
10. Правен основ за пренос на личните податоци;
11. Општ опис за преземените технички и организациски мерки за безбедност на личните податоци при преносот;
12. Периоди на вршење на преносот на лични податоци;
13. Број и датум на пријавата на преносот на лични податоци во Европската Унија или Европскиот економски простор;
14. Број и датум на донесено Решение за одобрување на пренос на лични податоци согласно член 49 став (3) и член 50 став (3) од Законот за заштита на личните податоци; и
15. Број и датум на донесено Решение за одобрување на задолжителни корпоративни правила согласно член 51 од Законот за заштита на личните податоци.

(2) Образецот на евиденцијата на извршениот пренос на лични податоци од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 5).

V. НАЧИН НА ВОДЕЊЕ НА ЕВИДЕНЦИЈАТА НА ИЗВРШЕНИОТ ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ ВО ТРЕТИ ЗЕМЈИ И МЕЃУНАРОДНИ ОРГАНИЗАЦИИ, ЕВРОПСКАТА УНИЈА И ЕВРОПСКИОТ ЕКОНОМСКИ ПРОСТОР

Член 7

(1) Евиденцијата на извршениот пренос на лични податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор се води во електронска форма во Агенцијата.

(2) Во евиденцијата од ставот (1) на овој член се внесуваат податоците од членот 6 став (1) на овој правилник, како и сите промени кои ќе настанат по извршеното запишување.

Член 8

(1) Контролорот или обработувачот за секоја промена на податоците за извршениот пренос, содржани во евиденцијата од членот 6 став (1) на овој правилник, писмено ја известува Агенцијата во рок од 15 дена од денот на настанување на промената.

(2) По приемот на известувањето од ставот (1) на овој член, Агенцијата во рок од три дена ги ажурира податоците содржани во евиденцијата на извршениот пренос на лични податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор.

(3) Контролорот или обработувачот за секоја промена на податоците во однос на примачот на личните податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор, потребно е да поднесе нова пријава за пренос на лични податоци или ново барање за добивање на одобрение за пренос на лични податоци согласно прописите за заштита на личните податоци.

Член 9

Во случај на престанување на својството на контролор или обработувач согласно прописите за заштита на личните податоци, контролорот или обработувачот писмено ја известува Агенцијата во рок од 15 дена од денот на престанување на својството контролор или обработувач.

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 10

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за формата, содржината и начинот на водење на евиденција за извршен пренос на лични податоци во други држави („Службен весник на Република Македонија“ бр. 158/10).

Член 11

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-601/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1

ПРИЈАВА
за пренос на лични податоци во држава членка на Европската Унија или Европскиот економски простор согласно член 48 став (3) од Законот за заштита на личните податоци

1.	**Податоци за контролорот или обработувачот кој го врши преносот**	
1.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
1.2	Контакт-телефон	
1.3	Електронска пошта	
1.4	Име и презиме на овластеното лице задолжено за пренесените лични податоци	
2.	**Држава во кој ќе се врши преносот**	
3.	**Податоци за примачот на лични податоци во држава членка на ЕУ/ЕЕП (контролор, обработувач или заеднички контролор)**	
3.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
3.2	Контакт-телефон	
3.3	Електронска пошта	
3.4	Име и презиме на овластеното лице задолжено за примените лични податоци	
4.	**Категории на субјектите на лични податоци чии лични податоци ќе бидат предмет на пренос**	
5.	**Цел или цели на преносот на личните податоци**	
6.	**Категории на лични податоци кои се пренесуваат**	
7.	**Посебни категории на личните податоци кои се пренесуваат**	
8.	**Рок на чување на пренесените лични податоци**	
9.	**Правен основ за преносот на личните податоци**	
10.	**Општ опис за преземените технички и организациски мерки за безбедност на личните податоци при преносот**	
12.	**Периоди на вршење на преносот**	

_____, ____.____.202___ година
(место) (датум)

М.П. _____
(потпис на функционерот, односно одговорното лице)

Образец бр. 2

БАРАЊЕ
за добивање на одобрение за пренос на лични податоци во трети земји или меѓународни организации врз основа на одлука на соодветност согласно член 49 став (3) од Законот за заштита на лични податоци

1.	**Податоци за контролорот или обработувачот кој го врши преносот**	
1.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
1.2	Контакт-телефон	
1.3	Електронска пошта	
1.4	Име и презиме на овластеното лице задолжено за пренос на лични податоци	
2.	**Трета земја или меѓународна организација во кој ќе се врши преносот**	
3.	**Податоци за примачот на лични податоци во третата земја или назив на меѓународна организација (контролор, обработувач или заеднички контролор)**	
3.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
3.2	Контакт-телефон	
3.3	Електронска пошта	
3.4	Име и презиме на овластеното лице задолжено за примените лични податоци	
4.	**Категории на субјектите на лични податоци чии лични податоци ќе бидат предмет на пренос**	
5.	**Цел или цели на преносот на личните податоци**	
6.	**Категории на лични податоци кои се пренесуваат**	
7.	**Посебни категории на личните податоци кои се пренесуваат**	
8.	**Рок на чување на пренесените лични податоци**	
9.	**Правен основ за пренос на личните податоци**	
10.	**Дали Европската унија или Агенцијата за заштита на личните податоци има донесено претходно одлука за соодветен степен на заштита на личните податоци на третата земја или меѓународна организација**	
11.	**Општ опис за превземените технички и организациски мерки за заштитата на личните податоци при преносот**	
12.	**Периоди на вршење на преносот**	

_____, ____.____.202___ година
(место) (датум)

М.П. _____
(потпис на функционерот, односно одговорното лице)

Образец бр. 3

БАРАЊЕ
за добивање на одобрение за пренос на лични податоци во трети земји или меѓународни организации врз основа на предвидени соодветни заштитни мерки согласно член 50 став (3) од Законот за заштита на лични податоци

1.	**Податоци за контролорот или обработувачот кој го врши преносот**	
1.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
1.2	Контакт-телефон	
1.3	Електронска пошта	
1.4	Име и презиме на овластеното лице задолжено за пренос на лични податоци	
2.	**Трета земја или меѓународна организација во која ќе се врши преносот**	
3.	**Податоци за примачот на лични податоци во третата земја или назив на меѓународната организација (контролор, обработувач или заеднички контролор)**	
3.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
3.2	Контакт-телефон	
3.3	Електронска пошта	
3.4	Име и презиме на овластеното лице задолжено за примените лични податоци	
4.	**Категории на субјектите на лични податоци чии лични податоци ќе бидат предмет на пренос**	
5.	**Цел или цели на преносот на личните податоци**	
6.	**Категории на лични податоци кои се пренесуваат**	
7.	**Посебни категории на личните податоци кои се пренесуваат**	
8.	**Рок на чување на пренесените лични податоци**	
9.	**Правен основ за пренос на личните податоци**	
11.	**Општ опис за превземените технички и организациски мерки за заштитата на личните податоци при преносот**	
12.	**Периоди на вршење на преносот**	
13.	**Договор помеѓу контролорот или обработувачот, како и контролорот, обработувачот или корисникот на личните податоци во третата земја или меѓународната организација со клаузули за соодветни заштитни мерки, како и применлива и достапна судска заштита за субјектите на лични податоци**	
14.	**Склучен управен (административен) договор меѓу јавните органи или тела со соодветни заштитни мерки и применливи и ефикасни права на субјектите на лични податоци**	

_____, ____.____.202___ година
(место) (датум)

М.П. _____
(потпис на функционерот, односно одговорното лице)

Образец бр. 4

БАРАЊЕ
за одобрување на задолжителни корпоративни правила врз основа на член 51 од Законот за заштита на личните податоци

1.	**Податоци за контролорот или обработувачот (подносител на барањето)**	
1.1	Назив и седиште контролорот или обработувачот	
1.2	Име и презиме или функција на овластеното лице задолжено за контакт за задолжителните корпоративни правила	
1.3	Контакт-телефон	
1.4	Електронска пошта	
1.5	Правен статус на подносителот на барањето (корпорација, партнерство итн.)	
1.6	Опис на позицијата на подносителот на барањето во рамките на групата на правни лица или на групата на правни лица кои вршат заедничка економска дејност (седиште на групата или член на групата со делегирани обврски за заштита на личните податоци)	
2.	**Назив на групата на правни лица или на групата на правни лица кои вршат заедничка економска дејност и локација на нивното седиште**	
3.	**Дали задолжителните корпоративни правила предвидуваат дека се правно обврзувачки и се применуваат на секој заинтересиран член на одредена група на правни лица или на група на правни лица кои вршат заедничка економска дејност и каде е тоа предвидено**	
4.	**Дали задолжителните корпоративни правила обезбедуваат применливи права за субјектите на лични податоци и каде е тоа предвидено**	
5.	**Дали задолжителните корпоративни правила ги исполнуваат условите утврдени во член 51 став (2) на Законот за заштита на личните податоци и каде е тоа предвидено**	

_____, ____.____.202___ година
(место) (датум)

М.П. _____
(потпис на функционерот, односно одговорното лице)

Образец бр. 5

ЕВИДЕНЦИЈА
на извршениот пренос на лични податоци во трети земји и меѓународни организации, Европската Унија и Европскиот економски простор

1.	**Податоци за контролорот или обработувачот кој го врши преносот**	
1.1	Назив и седиште за правно лице/име и презиме и адреса на живеење за физичко лице	
1.2	Контакт-телефон	
1.3	Електронска пошта	
1.4	Име и презиме на овластеното лице задолжено за пренос на лични податоци	
2.	**Држава во кој ќе се врши преносот**	
3.	**Податоци за примачот на лични податоци (контролор, обработувач или заеднички контролор)**	
3.1	Назив и седиште за правно лице, името и презимето и адреса на живеење за физичко лице	
3.2	Контакт-телефон	
3.3	Електронска пошта	
3.4	Име и презиме на овластеното лице задолжено за примените лични податоци	
4.	**Категории на субјектите на лични податоци чии лични податоци ќе бидат предмет на пренос**	
5.	**Цел или цели на преносот на личните податоци**	
6.	**Категории на лични податоци кои се пренесуваат**	
7.	**Посебни категории на личните податоци кои се пренесуваат**	
8.	**Рок на чување на пренесените лични податоци**	
9.	**Правен основ за пренос на личните податоци**	
11.	**Општ опис за преземените технички и организациски мерки за заштитата на личните податоци при преносот**	
12.	**Периоди на вршење на преносот**	
13.	**Број и датум на пријава за преносот на лични податоци е во Европската унија или Европскиот економски простор**	
14.	**Број и датум на донесено Решение за одобрување на пренос на лични податоци согласно член 49 став (3) и член 50 став (3) од Законот за заштита на личните податоци**	
15.	**Број и датум на донесено Решение за одобрување на задолжителни корпоративни правила согласно член 51 од Законот за заштита на личните податоци**	

_____, ____.____.202___ година
(место) (датум)

М.П. _____
(потпис на функционерот, односно одговорното лице)

1613.

Врз основа на член 69 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К ЗА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТА ОДРЕДБА

Член 1

Со овој правилник се пропишува начинот на спроведување на обука за вработените во контролорите, односно обработувачите, како и за офицерите за заштита на личните податоци од страна на Агенцијата за заштита на личните податоци (во натамошниот текст: Агенција), програмата за обука за заштита на личните податоци, формата и содржината на образецот за сертификатот, како и начинот на водење на евиденција за издадените сертификати.

II. НАЧИН НА СПРОВЕДУВАЊЕ НА ОБУКАТА

Член 2

Обуките утврдени согласно Годишната програма за обуки за заштита на личните податоци (во натамошниот текст: Годишна програма) ги организираат, подготвуваат и спроведуваат вработени административни службеници во Агенцијата (во натамошниот текст: обучувачи) определени од страна на директорот на Агенцијата.

Член 3

(1) Барањето за обука за заштита на личните податоци, контролорот, обработувачот, односно офицерот за заштита на личните податоци може да го поднесе:

- во писмена форма по пошта;
- на електронската пошта obuki@privacy.mk; или
- во писарницата на Агенцијата.

(2) Барањето за обука за заштитата на личните податоци ги содржи особено следните податоци:

- назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци;
- бројот на учесниците што се пријавуваат за обуката;
- име и презиме на пријавените учесници за обуката и работно место;
- видовите на обука и модулите за обуката за која се пријавуваат учесниците;
- терминот на бараната обука;
- име и презиме на одговорното лице;
- телефон за контакт; и
- електронска пошта.

(3) По исклучок од ставот (2) на овој член, контролорот, односно обработувачот, податоците за учесниците може да ги достави и дополнително, но најдоцна до денот на отпочнување на обуката.

(4) Доколку контролорот, обработувачот, односно офицерот за заштита на личните податоци сака да присуствува на посебни обуки според барана програма, во барањето за обука за заштитата на личните податоци наместо модулите ги наведува темите, односно прашањата што бара да бидат предмет на обуката.

(5) Секое добиено барање за обука за заштита на личните податоци во Агенцијата се заведува во писарницата и се доставува до обучувачите.

(6) Образецот на барањето за обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 1).

Член 4

(1) Агенцијата ги евидентира податоците за пријавените контролори, обработувачи, односно офицери за заштита на личните податоци и го следи бројот на пријавени учесници за секој од модулите на обуките наведени во Годишната програма.

(2) Доколку контролорот, обработувачот, односно офицерот за заштита на личните податоци сака да присуствува на посебна обука според барана програма терминот за обуката договорно се утврдува.

(3) Контролорот, обработувачот, односно офицерот за заштита на личните податоци кој се пријавил за обука, најдоцна три работни дена пред одржувањето на обуката се известува за:

- терминот за одржување на обуката; и
- крајниот рок во кој треба да се уплати надоместокот за обуката.

(4) Известувањето од ставот (3) на овој член до контролорот, обработувачот, односно офицерот за заштита на личните податоци се доставува по електронски пат.

Член 5

Агенцијата за секој од модулите што се предмет на обука обезбедува презентација во електронска форма (медиум), како и канцелариски материјали за учество на обуката (прописи за заштитата на личните податоци, папка, хартија, пенкало и др.) кои на учесниците им се даваат пред отпочнување на обуката.

Член 6

(1) Уплатата на надоместокот за обуката се врши само преку трезорската сметка на Агенцијата. Правилно пополнетиот образец ПП-50 за плаќање на надоместокот за обуката се објавува на веб-страницата на Агенцијата.

(2) Контролорите, обработувачите, односно офицерите за заштита на личните податоци се должни да го извршат плаќањето на трошоците за обуката пред отпочнување на обуката за нивните пријавени учесници, но не подоцна од денот на одржување на обуката.

(3) Ако учесникот од било кои причини не присуствува на обуката и/или најмногу два пати го одложува присуството на обуката, Агенцијата определува нов термин за одржување на обуката.

(4) Во случаите од ставот (3) на овој член, доколку и на новиот термин учесникот не се појави на обуката, уплатените средства не се враќаат на контролорот, обработувачот, односно офицерот за заштита на личните податоци.

Член 7

(1) Агенцијата склучува договор за спроведување обука за заштита на личните податоци со контролорот, обработувачот, односно офицерот за заштита на личните податоци, а кои доставиле барање за спроведување на обука согласно Годишната програма.

(2) Образецот на Договорот за спроведување обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 2).

(3) По исклучок од ставот (1) на овој член, обуките за вработените во министерствата, органите на државната управа, управните организации и другите државни

органи кои се целосни буџетски корисници, а кои доставиле барање за спроведување на обука согласно Годишната програма, се вршат без надомест, а по претходно склучен меморандум за соработка помеѓу Агенцијата и заинтересираниот контролор.

Член 8

(1) На обуката може да учествуваат само пријавените учесници за кои е уплатен надоместокот за обуката или кои биле ослободени од плаќањето на надоместокот.

(2) Доколку пријавениот учесник не се јави на определениот термин за одржување на обуката, истиот се вклучува во следните обуки што се одржуваат за истите модули.

(3) Пред отпочнување на обуката, секој учесник на обуката во евиденциониот лист за присуство ги внесува своите лични податоци (лично име) и своерачно се потпишува.

(4) Евиденциониот лист за присуство од ставот (3) на овој член ги содржи следните рубрики: реден број, контролор/обработувач, офицер за заштита на личните податоци, име и презиме, контакт телефон/електронска пошта и потпис. Во евиденциониот лист за присуство се внесува и датата и местото на одржување на обуката.

(5) Образецот на евиденциониот лист за присуство е составен дел на овој правилник (Образец бр. 3).

Член 9

(1) По завршување на обуката секој од учесниците анонимно пополнува прашалник за евалуација.

(2) Податоците од прашалникот за евалуација се користат само за анализи, извештаи, како и за унапредување на процесот за обука во Агенцијата.

(3) Образецот на прашалникот за евалуација е составен дел на овој правилник (Образец бр. 4).

III. ПРОГРАМА ЗА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 10

(1) Обуката за заштита на личните податоци се спроведува во согласност со:

- Програма за обука за заштита на личните податоци (Прилог бр. 1); и
- Програма за обука за офицерите за заштита на личните податоци (Прилог бр. 2).

(2) Програмите од ставот (1) на овој член се составен дел на овој правилник.

IV. ФОРМА И СОДРЖИНА НА ОБРАЗЕЦОТ ЗА СЕРТИФИКАТ

Член 11

(1) На секој учесник по завршувањето на обуката му се издава сертификат за учество на обука за заштита на личните податоци (во натамошниот текст: сертификат) од страна на директорот на Агенцијата.

(2) Во сертификатот се внесуваат податоци за: името и презимето на учесникот што учествувал на обуката, назив на контролорот, односно обработувачот, назив на обуката, место на одржување на обуката, период на важење на сертификатот, број и датум на сертификатот, место за печат и потпис на директорот на Агенцијата.

(3) Сертификатот се издава во случај ако учесникот присуствувал на генеричка обука и/или специјализирана обука.

(4) Сертификатот се издава и за учесниците на посебните обуки што се спроведуваат согласно Годишната програма.

(5) Образецот на сертификатот е составен дел на овој правилник (Образец бр. 5).

V. НАЧИН НА ВОДЕЊЕ НА ЕВИДЕНЦИЈА ЗА ИЗДАДЕНИ СЕРТИФИКАТИ

Член 12

(1) Евиденцијата за издадените сертификати ги содржи следните податоци:

- реден број;
- име и презиме на учесникот на обуката;
- назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци;
- вид на обуката;
- место на одржување на обуката;
- датум и број на издадениот сертификат;
- датум и број на издадена потврда;
- контакт-телефон и електронска адреса; и
- забелешка.

(2) Образецот на евиденцијата за издадените сертификати е составен дел на овој правилник (Образец бр. 6).

(3) Евиденцијата од ставот (1) на овој член се води електронски согласно прописите за архивски материјал.

Член 13

(1) На барање на контролорот, обработувачот, односно офицерот за заштита на личните податоци или на учесникот на обуката, директорот на Агенцијата или од него овластено лице им издава Потврда за учество на обука за заштита на личните податоци.

(2) Во Потврдата за учество на обука за заштита на личните податоци се внесуваат податоци за: името и презимето на учесникот што учествувал на обуката, назив контролорот, односно обработувачот, место каде е одржана, датум на спроведување на обуката, по чие барање се издава потврдата и причини за издавање.

(3) Образецот на Потврдата за учество на обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 7).

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 14

Со денот на влегувањето во сила на овој правилник престанува да важи Упатството за начинот на организирање и спроведување на обуки за контролори и обработувачи бр. 02-283/1 од 8.2.2012, бр. 02-283/2 од 7.3.2012, бр. 01-283/3 од 6.4.2012 и бр. 02-2852/1 од 20.12.2013 година.

Член 15

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-602/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 1

БАРАЊЕ ЗА ОБУКА
за заштита на личните податоци

1. Назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци
_____;
2. Број на учесници што се пријавуваат за обуката _____;
3. Име и презиме на пријавените учесници за обуката и работно место:
   1. _____;
   2. _____;
   3. _____;
   4. _____;
   5. _____
4. Видови на обуки[1] и модули за обуки за кои се пријавувате:
   1. Генерички[2] модул 1, 2, 3 ☐
   2. Генерички и специјализирани обуки – 1 модул ☐
   3. Генерички обуки модул 4 (офицер за заштита на личните податоци) ☐
   4. Посебни обуки ☐
      - на тема _____;
5. Термин за бараната обука – ваш предлог _____;
6. Име и презиме на одговорното лице _____;
7. Телефон за контакт _____;
8. Електронска пошта _____.

Барањето за обука може да се поднесе:
- на obuki@privacy.mk;
- во писмена форма по пошта; или
- во писарницата на Агенцијата за заштита на личните податоци.

Скопје _____._____.202__ М.П. _____ (Одговорно лице)

[1] Генерички; Специјализирани и Посебни обуки согласно Годишната програма за обука на контролори и обработувачи

[2] **Генерички обуки** – сите модули се задолжителни: Модул: 1 Правни основи (Законот за заштита на личните податоци и подзаконските акти) во домашното законодавство и право на Европската Унија; Модул: 2 Поимник (објаснување на поимите од Законот за заштита на личните податоци); Модул: 3 Обврски и одговорности на контролорот и обработувачот; и Модул: 4 Положба, статус и работи кои ги врши офицерот за заштита на лични податоци.

[3] **Специјализирани обуки**: Модул: 1 – Органи за спроведување на законот; Модул: 2 – Правосудство; Модул: 3 – Државна безбедност и одбрана; Модул: 4 – Здравство; Модул: 5 – Образование; Модул: 6 – Социјална заштита; Модул: 7 – Финансии; Модул: 8 – Комунални дејности и енергетика; Модул: 9 – Локална самоуправа; Модул: 10 – Работни односи; Модул: 11 – Индустрија и транспорт; Модул: 12 – Градежништво; Модул: 13 – Телекомуникации и пошти; Модул: 14 – Медиуми; Модул: 15 – Маркетинг; Модул: 16 – Трговија; Модул: 17 – Туризам и угостителство; Модул: 18 – Лотарија и игри на среќа; Модул: 19 – Здруженија на граѓани; Модул: 20 – Политички партии; Модул: 21 – Осигурување; Модул: 22 - Технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци (генерално и посебно според област); Модул: 23 – Видеонадзор; Модул: 24 – Биометриски податоци; Модул: 25 – Пренос на лични податоци; Модул: 26 – Обработка на посебни категории на лични податоци; и Модул: 27 – Вршење на внатрешна контрола; или Посебен модул 1, 2, 3, 4 и 5.

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 2

Бр. ____-_____/____
_____._____.2020

ДОГОВОР
за спроведување обука за заштита на личните податоци

Склучен во Скопје, на ден ____.____.2020 година, помеѓу:

1. **Агенцијата за заштита на личните податоци**, со седиште во Скопје на бул. „Гоце Делчев“ бр. 18, застапувана од директорот Имер Алиу, во својство на давател на услугата за спроведување обука за заштита на личните податоци (во натамошниот текст: Давател на услугата), од една страна и

2. _____, со седиште во _____ на адреса _____, застапуван/а од _____, во својство на корисник на услугата за обука за заштита на личните податоци (во натамошниот текст: Корисник на услугата), од друга страна.

Член 1

Предмет на овој договор е спроведувањето обука за заштита на обработката на личните податоци (генерички и специјализиран модул), која ќе се одржи во просториите на Давателот на услугата, на ден ____.____.202__ година, во траење од 6 часа.

Член 2

Давателот на услугата, за спроведување обука за заштита на личните податоци, согласно Годишната програма за обуки на контролори и обработувачи, преку определените вработени лица за спроведување обуки за заштита на личните податоци, се обврзува договорената обука да ја реализира совесно и во согласност со барањето на Корисникот на услугата, со вклучување на компетентни експерти од Давателот на услугата.

По исклучок од ставот 1 на овој член, Давателот на услугата може да вклучи и надворешни експерти од земјата или странство.

Член 3

Давателот на услугата за спроведената обука го определува надоместокот според висината на трошоците, зависно од видот и модулот на обуката, согласно одредбите од Одлуката за определување на висината на надоместоците за организирање и спроведување на обука за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 58/2020).

Член 4

Корисникот на услугата е должен да му го плати надоместокот на Давателот на услугата за спроведување на обуката: ___.000,00 денари за 1 (еден) пријавен учесник, односно вкупно ____._____,00 денари за ____ (_____) пријавени учесници.

Надоместокот за обуката од став 1 на овој член се уплатува најдоцна до денот на одржувањето на обуката за која Корисникот на услугата се пријавил.

Средствата треба да се уплатат на Буџетот на РСМ на трезорската сметка со број 100-0000000630-95 која се води на НБРСМ, сметка на буџетски корисник број 0200660143-631-14 на Агенцијата за заштита на личните податоци, приходна шифра 723612, потпрограма 20.

Член 5

Во случај да настанат спорови во врска со реализацијата на овој договор, договорните страни се согласни да ги решат спогодбено.

Доколку не се постигне спогодбено решавање на спорот/вите, надлежен е Основниот граѓански суд Скопје.

Член 6

Овој договор влегува во сила со денот на потпишувањето.

Член 7

Овој Договор е составен во два истоветни примероци, од кои еден примерок за Давателот на услугата и еден примерок за Корисникот на услугата.

Давател на услугата,
Директор,
Imer Aliu

Корисник на услугата,

ЕВИДЕНЦИОНЕН ЛИСТ ЗА ПРИСУСТВО НА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

_____, ___.___.20___ година

Образец бр. 3

Ред. бр.	Контролор/обработувач, офицер за заштита на личните податоци	Име и презиме	Контакт-телефон Електронска пошта	Потпис
1.			_____ _____	
2.			_____ _____	
3.			_____ _____	
4.			_____ _____	
5.			_____ _____	
6.			_____ _____	
7.			_____ _____	
8.			_____ _____	
9.			_____ _____	
10.			_____ _____	

Обука за заштита на личните податоци
_____, ___.___.20___ година

Образец бр. 4

ПРАШАЛНИК ЗА ЕВАЛУАЦИЈА

Ред. бр.	Содржина на прашањето	Оценка				
I Евалуација за обуките						
1.	Која е Вашата оценка за организацијата на обуката?	1	2	3	4	5
2.	Колку обуката ги исполни предвидените цели?	1	2	3	4	5
3.	Колку обуката ги исполни вашите очекувања?	1	2	3	4	5
4.	Во која мера сте задоволни од методологијата на обуката?	1	2	3	4	5
5.	Колку сте задоволни со времетраењето на обуката?	1	2	3	4	5
6.	Колку сте задоволни од добиените материјали за обуката (презентации, прописи и др.)	1	2	3	4	5
7.	Колку сте задоволни од условите за одржување на обуката (сала, опрема, техничка поддршка)?	1	2	3	4	5
8.	Со која оценка ја оценувате можноста за поставување на прашања?	1	2	3	4	5
II Евалуација за обучувачите (име и презиме на обучувачот)						
1.	I	1	2	3	4	5
2.	II	1	2	3	4	5
3.	III	1	2	3	4	5
4.	IV	1	2	3	4	5
5.	V	1	2	3	4	5
6.	VI	1	2	3	4	5
III Евалуација за трансферот на знаења						
1.	Дали стекнатите знаења може да ги примените за подобрување на вашето работење?	да	не	делумно		
2.	Дали добиените материјали ќе ги доставите на вашите колеги?	да	не	делумно		
3.	Дали планирате да одржите презентација за стекнатото искуство пред вашите колеги ?	да, за _____ лица			не	
4.	Дали имате обврска за подготвување извештај од учеството на обуката	да	не			

Ваши дополнителни забелешки, коментари или предлози:

_____
_____
_____

Ви благодариме на соработката

Образец бр. 5

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на член 69 став (5) од Законот за заштита на личните податоци, а во врска со член 11 од Правилникот за обука за заштита на личните податоци, директорот на Агенцијата за заштита на личните податоци

ИЗДАВА

СЕРТИФИКАТ

за учество на обука за заштита на личните податоци

На лицето _____ кое во својство на претставник на контролорот, односно обработувачот _____, учествуваше на обука за заштита на личните податоци _____ во_____

Овој сертификат е со важност од три години од денот на неговото издавање.

Бр. _____ М.П. Директор,

Дата _____ Imer Aliu

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

ЕВИДЕНЦИЈА ЗА СПРОВЕДЕНИ ОБУКИ

Образец бр. 6

Ред. бр.	Име и презиме на учесникот на обуката	Контролор, обработувач, односно офицер за заштита на личните податоци (назив и седиште, име и презиме и адреса на живеење)	Вид на обуката	Место на одржување на обуката	Датум и број на издадениот сертификат	Датум и број на издадена потврда	Контакт-телефон и електронска адреса	Забелешка
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 7

Бр. ____-_____/____
_____._____.202___

Врз основа на член 63 став (1) алинеја 8 од Законот за заштита на личните податоци, а во врска со член 13 од Правилникот за обука за заштита на личните податоци, Агенцијата за заштита на личните податоци издава

П О Т В Р Д А
за учество на обука за заштита на личните податоци

На лицето _____, кое во својство на претставник на контролорот, односно обработувачот _____ присуствуваше на обука за заштита на личните податоци во период од __ до __ на ден _____.20__ година, одржана во просториите на Агенцијата за заштита на личните податоци.

Потврдата се издава на барање на _____.

Потврдата се издава заради _____.

Директор,
Imer Aliu

Прилог бр. 1

Програма за обука за заштита на личните податоци

Модул еден		
Име на модулот	**Преглед на правната рамка за заштита на личните податоци**	
Придобивка од учењето	Учесникот: • го разбира значењето на клучните поими дефинирани со Законот • подготвен е да ги почитува начелата за заштита на лични податоци и да ги примени во пракса, како и да ги запознае соработниците со нив преку внатрешни обуки • способен е да ја анализира усогласеноста на обработката на податоците со Законот • запознаен е со обврската на контролорт да демонстрира почитување на овие начела • детално е запознаен со статусот, надлежностите, задачите и овластувањата на Агенцијата • способен е да го застапува контролорот при вршење на надзор од страна на надзорниот орган • запознаен е со управните постапки што контролорот ги покренува пред надзорниот орган и со управните постапки што субјектот на лични податоци ги поведува пред надзорниот орган против контролорот	
Тема	**Што ќе опфати темата?**	**Материјал[1]**

• Општа регулатива за заштита на лични податоци на Европскиот парламент и Советот на ЕУ и нејзино транспонирање во новиот Закон за заштита на личните податоци	• Воведен краток осврт на:
	  • Европска конвенција за заштита на човековите права
	  • Конвенција 108/81 на Совет на Европа
	  • Конвенција 108/81+
	• Преглед на Општата регулатива за заштита на податоци
	• Закон за заштита на личните податоци
		• Европска конвенција за заштита на човековите права (ЕКЧП)
		• Судска практика во однос на член 8 од ЕКЧП (CASE OF TYRER v. THE UNITED KINGDOM, чување на податоци за приватниот живот CASE OF LEANDER v. SWEDEN, надзор и пресретнување на телефонска и писмена комуникација CASE OF KLASS AND OTHERS v. GERMANY, надзор на работно место Copland v. the United Kingdom, примена на CCTV (видеонадзор) Chamber judgment Peck v. United Kingdom, заштита на нечиј имиџ Grand Chamber judgments Springer and Von Hannover v. Germany - German и Von Hannover v. Germany, репутација PFEIFER v. AUSTRIA, NIEMIETZ v. GERMANY,
		Ограничување на правото да е утврдено со закон AMANN v. SWITZERLAND, ROTARU v. ROMANIA, ограничување во однос на легитимната цел PECK v. THE UNITED KINGDOM, мешањето во правото е неопходно во едно демократско општество LEANDER v. SWEDEN, позитивни обврски на државата K.U. v. FINLAND, поле на слободна проценка GARDEL v. FRANCE.
		• Конвенција 108/81 на Совет на Европа
		• Повелба на Европската унија за основните права
		Ограничување на повелбата
		• Општа регулатива за заштита на лични податоци (ОРЗЛП)
		• EC What does the General Data Protection Regulation (GDPR) govern?
		• Реформски пакет 2018
		• Закон за заштита на личните податоци
		• Мислења и препораки на Работната група 29
		• Мислења на Европскиот супервизор за заштита на личните податоци
		• ICO Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now
		• FRA Прирачник за европското законодавство за заштита на податоците
		• Protecting the right to respect for private and family life under the European Convention on Human Rights
		Судска практика – Европски суд за човекови права
		• ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data)

[1] Во програмата, во колоната „Материјал“, за Општата регулатива за заштита на лични податоци се користи кратенката ОРЗЛП.

			• ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Примена на законот	• Територијална примена на Законот • Исклучоци од примена на Законот	• Закон за заштита на личните податоци	
Клучни поими и дефиниции	• Главни аспекти на поимот личен податок • Обработка на личните податоци • Контролор на лични податоци • Посебни категории на лични податоци • Нови поими и дефиниции • Анономизирани и псевдонимизирани податоци	• Закон за заштита на личните податоци • Судска практика обработка на личните податоци Bodil Lindqvist • Судска практика за опфатот на поимот личен податок AMANN v. SWITZERLAND, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) • Судска практика: здравствени податоци Z v. FINLAND, • ICO Anonymization code • EC What is personal data? • EC Rules for business and organisations • WP29 Opinion 1/2010 on the concepts of "controller" and "processor" • WP29 Working Document on Genetic Data WP 91 • WP29 Working document on biometrics WP 80 • EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies	
Начела за заштита на личните податоци и нивното значење	• „Законитост, правичност и транспарентност“ • „Ограничување на целите“ • „Минимален обем на податоци“ • „Точност“ • „Ограничување на рокот на чување“ • „Интегритет и доверливост“ • Демонстрирање усогласеност со начелата за заштита на личните податоци (отчетност)	• Закон за заштита на личните податоци • Судска практика: правична и транспарентна обработка на податоците HARALAMBIE v. ROMANIA, K.H. AND OTHERS v. SLOVAKIA, период на чување S. AND MARPER v. THE UNITED KINGDOM • Водич за ОРЗЛП • Отчетност ИКО • EDPS обука • ENISA Privacy, Accountability and Trust – Challenges and Opportunities • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • WP 29 Opinion 3/2010 on the principle of accountability WP 173 • EDPS Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies Summary • EDPS Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments • EDPS Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation • WP 29 Guidelines on transparency under Regulation 2016/679 WP260	
Агенција за заштита на лични податоци како надзорен орган	• Надлежности, задачи и овластувања ○ Супервизија над заштитата на личните податоци	• Закон за заштита на личните податоци • ОРЗЛП чл. 51, 52, 53, 54, 55, 57, 58 • EC What are Data Protection Authorities (DPAs)?	

Модул два		
Име на модулот	**Комуникација на контролорот со субјектот на лични податоци**	
Придобивка од учењето	Учесникот: • ги познава правата на субјектот • способен е да води постапки и да одлучува за правата на субјектот на лични податоци • знае да процени како треба да биде формулирана секоја одделна согласност за обработка на лични податоци со јасно дефинирање на целта на обработката на личните податоци и обезбедување на лесен начин за нејзино повлекување • знае да даде конкретни насоки и работни инструкции на вработените кај контролорот кој што вршат директен маркетинг	
Тема	**Што ќе опфати темата?**	**Материјал**
Права на субјектите на лични податоци	• Информираност (транспарентност) • Пристап и исправка на личните податоци • Бришење („право да се биде заборавен“) • Ограничување на обработката на личните податоци • Преносливост на личните податоци • Право на приговор • Автоматска обработка на податоците (вклучително и профилирање)	• Закон за заштита на личните податоци • ОРЗЛП чл. 17, 20, 22 • Прашања и одговори поврзани со реформскиот пакет • Едукативно видео за правото на пристап до личните податоци • Образец на барање за пристап и исправка на личните податоци • Fact sheet EU Data Protection Reform: better data protection rights for European citizens • I-scoop Data subject rights and personal information: data subject rights under the GDPR • Matheson GDPR in Context: Data Subject Rights • ICO - Guide to the General Data Protection Regulation (GDPR) • Обрасци EU GDPR Academy Managing Data Subject Rights • ICO subject-access-request-checklist • ICO privacy-notices-transparency-and-control • EC Rights for citizens • ENISA The right to be forgotten - between expectations and practice • ICO Personal information online small business checklist • ICO Protecting personal data in online services: learning from the mistakes of others • WP 29 Guidelines on transparency under Regulation 2016/679 WP260 • WP 29 Guidelines on Consent under Regulation 2016/679 WP259 • EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data • ОРЗЛП- чл. 20 и рец. 68 • WP242 ANNEX –Frequently Asked Questions • WP29 WP 242 rev.01 Guidelines on the right to data portability • ОРЗЛП – чл. 22, рец.71, рец. 91 • Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling • WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 WP251 Судска практика – Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)

Услови за согласност	• Условите што треба да бидат исполнети за да се смета за валидна согласноста на субјектот за обработка на неговите лични податоци	• Закон за заштита на личните податоци Судска практика: • Согласност за обработка на здравствени податоци во поставка за вработување European Data Protection Supervisor, represented by M. V. Pérez Asinari and by H. Kranenborg, acting as Agents, intervener, v European Parliament, represented by K. Zejdová and S. Seyr, acting as Agents • Недостиг на согласност за медицински податоци L.L. v. FRANCE, RADU v. THE REPUBLIC OF MOLDOVA • Јавен интерес AVILKINA AND OTHERS v. RUSSIA • Fact sheet EU Data Protection Reform: better data protection rights for European citizens • I-sccop Data subject rights and personal information: data subject rights under the GDPR • Matheson GDPR in Context: Data Subject Rights • ICO - Guide to the General Data Protection Regulation (GDPR) Практични примери • Обрасци EU GDPR Academy Managing Data Subject Rights
Услови кои што се применуваат за согласност на дете во однос на услугите на информатичкото општество	• Користење на услугите на информатичкото општество од страна на децата е појава која што е застапена на глобално ниво. Во овој сегмент, неопходно е нормирање на обработката на личните податоци на децата.	• Закон за заштита на личните податоци • ОРЗЛП чл. 8 • ICO – Guide to the General Data Protection Regulation (GDPR) • Обрасци EU GDPR Academy Managing Data Subject Right • WP 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160 • WP 29 Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools) WP 147

Модул три		
Име на модулот	**Информациска сигурност**	
Придобивка од учењето	Учесникот: • свесен е за значењето на техничките аспекти за безбедност на обработката на личните податоци • знае кои информации му се потребни за да ги идентификува операциите на обработка на лични податоци • способен е да препознае ризик при одредени операции на обработка на личните податоци • знае што е безбедносен инцидент • запознат е со обврската за известување за нарушување на безбедноста на личните податоци • способен е да напише правилник за технички и организациски мерки за сигурност и тајност при обработката на личните податоци • способен е да подготви Договор за обработка на лични податоци со вклучени одредби кои гарантираат дека обработувачот ќе преземе потребни технички и организациски мерки за заштита и тајност на личните податоци • способен е да оцени кои области треба да бидат предмет на внатрешна или надворешна ревизија/контрола, • способен е да настапи со свој совет при спроведување на „Data Protection Impact Assesment“ • го разбира концептот на Privacy by design & by default и способен е да дава совети за негова примена	
Тема	**Што ќе опфати темата?**	**Материјал**
Безбедност на обработката	• Технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • Едукативно видео за техничките и организациски мерки за заштита и тајност на личните податоци • ICO IT_security_practical_guide • UK GOV Cyber security guidance for business • HM Government Small businesses: What you need to know about cyber security • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • EDPS Guidance Security Measures for Personal Data Processing Article 22 of Regulation 45/2001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance Судска практика - Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Нивоа на техничките и организациски мерки за заштита и тајност на личните податоци и	• Воспоставување одговорност за средства кои се во сопственост на контролорот • Нивоа на техничките и организациски мерки за заштита и тајност на личните	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци

контроли	податоци треба да се применат во зависност од категориите на личните податоци кои се обработуваат • Воспоставување контроли соодветни за секое ниво на техничките и организациски мерки за заштита и тајност на личните податоци	• ICO IT security practical guide • UK GOV Cyber security guidance for business • HM Government Small businesses: What you need to know about cyber security • ENISA Handbook on Security of Personal Data Processing • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Безбедносни инциденти и Известување за нарушување на безбедноста на личните податоци	• Обврските за безбедност и тајност на личните податоци да се опфатени во описот на работното место и во договорот за работа • Да се следи почитувањето на овие обврски во процесот на оценување на вработените • Како и каде да се пријави инцидент-нарушување на безбедноста на личните податоци • Обрасци и постапка за известување на нарушувањето на безбедноста на личните податоци • Лекција која може да се научи од настанат инцидент • Санкции и дисциплински постапки кај контролорот поврзани со инциденти	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Recommendations for a methodology of the assessment of severity of personal data breaches • ENISA Recommendations for technical implementation of Art.4 • ENISA Data breach notifications in the EU • WP 29 Opinion 03/2014 on Personal Data Breach Notification WP 213 • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance • WP 29 Guidelines on Personal data breach notification under Regulation 2016/679
Безбедност и приватност за услуги кои се пренесуваат на обработувачи (аутсорсинг)	• Примена на техничките и организациски мерки за заштита и тајност на личните податоци и во случаи кога тие се обработуваат од страна на обработувачот • Обврската за примена на техничките и организациски мерки за обезбедување заштита и тајност на личните податоци помеѓу контролорот и обработувачот да се предвиди со Договор.	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • CNIL General Data Protection Regulation GUIDE FOR PROCESSORS SEPTEMBER 2017 EDITION • DPC Data security guidance
Физичка безбедност	• Процедури и механизми за физичка безбедност • Физичка контрола на влезовите • Обезбедување на канцелариите, просториите и објектите • Работење во безбедна околина • Обезбедување на компјутерската опрема	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Безбедност и приватност на работното место	• Заштита на просториите каде се обработуваат личните податоци со цел да се спречи нивно откривање или модификација од страна на неовластени лица или кражба • Контроли што треба да бидат поставени за да се минимизира загубата или штетата	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing

	• Политиката за чисто биро и чист екран	• ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Оперативни постапки и одговорности	• Воспоставување на одговорности и постапки за управување и работи со сите компјутери и мрежи • Документирани оперативни процедури • Процедури за управување со инциденти • Сегрегација на должности	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Планирање и прифаќање на системот	• Заштита од злонамерен софтвер • Контроли против малициозен софтвер • Процедури за сомневање за малициозен код (како на пример со е-пошта) • Заштита од злонамерен софтвер при користење на сајтовите за социјално вмрежување, инстант пораки, текстуални пораки и други технологии • Процедури за откриен и потврден малициозен код	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Сигурносни копии и логови	• Процедури за правење сигурносни копии на податоци • Процедури за логирање на настани и грешки • Логови на администратори • Пријавување на грешки • Постапка за периодично тестирање на ефикасноста на сигурносните копии	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance • DPC Back-up systems
Сигурност на мрежа и контрола на приватноста	• Управување со безбедноста на компјутерските мрежи • Заштита на информациите и на придружната инфраструктура • Одржување на безбедноста на мрежата и контрола на приватноста • Тестирање на ефикасноста на безбедноста на мрежата и на приватност	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO Wi-Fi location analytics • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Управување и безбедност на	• Контрола и физичка заштита на компјутерските медиуми, документи,	• Законот за заштита на личните податоци

медиуми	влезните и излезните податоци за да се спречи кражба, оштетување на средствата и прекин на деловните активности • Управување со преносливи медиуми • Ништење на медиумите • Постапки за ракување со податоци • Безбедност на документацијата	• ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Давање и размена на информации	• Контрола на давањето и размената на податоци за да се спречи загуба, модификација или злоупотреба на податоци • Барање за користење или размена на податоци • Безбедност на медиумите кои се пренесуваат • Безбедност на електронските пораки • Други форми на размена на информации	• Закон за заштита на личните податоци • Правилник за безбедност на личните податоци • ICO data sharing code of practice • ICO Data sharing checklists • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Контрола на пристап на системи	• Контрола на пристапот до компјутерски услуги и податоци • Политики за дисеминација на податоците и информациите • Политика за контрола на пристап	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Управување со корисниците	• Процедури за контрола на правата на пристап до ИТ системите и услугите • Регистрација на корисниците • Управување со привилегии • Управување со корисничките лозинки • Преглед на правата на пристап на корисниците • Процедури за отстранување на неактивни корисници и корисници кои повеќе не се потребни	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • CNIL Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords • DPC Data security guidance

Следење на системот за пристап и користење	• Следење на системот
	  ○ за да се обезбеди усогласеност со политиката за пристап
	  ○ за откривање на неовластени активности
	  ○ за да се утврди ефективноста на безбедносни мерки
	• Логирање на настани
		• Законот за заштита на личните податоци
		• ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83
		• Правилник за безбедност на личните податоци
		• ENISA Guidelines for SMEs on the security of personal data processing
		• ICO IT security practical guide
		• ISO/IEC 27001:2013(E)
		• Academy27001 Clause-by-clause explanation of ISO 27001

		• CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Криптирање на податоците	• Употреба на криптографски системи и техники за заштита на доверливоста, автентичноста или интегритетот на податоците и за заштита на информациите што се сметаат за ризични (посебни категории на личните податоци и ЕМБГ) • Дигитален потпис • Управување со клучеви	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Study on cryptographic protocols • ENISA Recommended cryptographic measures - Securing personal data • ENISA Algorithms, Key Sizes and Parameters Report - 2013 • ENISA Algorithms, key size and parameters report 2014 • ENISA The Use of Cryptographic Techniques in Europe • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Алатки за приватност и безбедност на податоците (PETs - Технологии кои треба да ја подобрат приватноста)	• Криптирање • Систем за контрола на пристап • Печат за приватност на веб страниците • Дигитален потпис • Биометрија • Фаервол • Спам филтри • HTML филтри • Системи за псеводонимизација и анонимизација	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA On the security, privacy and usability of online seals • ENISA Study on cryptographic protocols • ENISA Recommended cryptographic measures - Securing personal data • ENISA Algorithms, Key Sizes and Parameters Report - 2013 • ENISA Algorithms, key size and parameters report 2014 • ENISA The Use of Cryptographic Techniques in Europe • ENISA Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies • ENISA Privacy Enhancing Technologies: Evolution and State of the Art • ENISA PETs controls matrix - A systematic approach for assessing online and mobile privacy tools • ENISA Recommendations on European Data Protection Certification • ENISA Challenges of security certification in emerging ICT environments • ENISA Privacy and data protection in mobile applications • ENISA Privacy considerations of online behavioural tracking • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • WP29 Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC WP 90 • WP29 Opinion 1/2008 on data protection issues related to search engines WP 148 • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Технологии кои се опасни по приватност	• Cookies (Колачиња) • Лог фајлови • Спајвеар • Спам и фишинг	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • COOKIE SWEEP COMBINED ANALYSIS – REPORT

		• Working Document 02/2013 providing guidance on obtaining consent for cookies • Opinion 04/2012 on Cookie Consent Exemption • ICO Guide to the Privacy and Electronic Communications Regulations • Directive 2009/136/EC (ePrivacy Directive) • Factsheet – Stronger ePrivacy rules • Proposal for a Regulation on Privacy and Electronic Communications • Directive 2002/22/EC of the European Parliament and of the Council • ENISA Bittersweet cookies. Some security and privacy considerations • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • ENISA Smartphones: Information security risks, opportunities and recommendations for users • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • DPC Data security guidance
Социјален инженеринг	• Заеднички методи и цели на социјалниот инженеринг • Проверка на идентитетот на барателите • Признавање на можни напади на социјален инженеринг • Процедури за реагирање на потенцијални обиди за социјално инженерство	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • US-CERT Avoiding Social Engineering and Phishing Attacks • WEBROOT What is Social Engineering? • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Бришење на податоци	• Безбедно уништување на доверливите и посебните категории на лични податоци во хартиена форма • Неповратно бришење на податоците кои електронски се чуваат • Безбедно уништување на електронските медиуми за складирање на податоци	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Проценка на влијанието на планираните операции на обработка на податоците врз заштитата на личните податоци „Data Protection Impact Assesment"	• Идентификување и разрешување на проблеми во раните фази на развој на нови системи и продукти, како и дефинирање на улогата на офицерот во овој процес – давање конкретни совети и следење дали истите се прифатени при неговото спроведување.	• ОРЗЛП чл. 35 • WP 29 WP 248 rev.01 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 • WP 29 Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force WP209 • ICO PIA-Code-of-practice • Smart Grid Task Force 2012-14 - Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems • CNIL PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA) • CNIL PRIVACY IMPACT ASSESSMENT (PIA) Tools (templates and knowledge bases) • CNIL Good practices MEASURES FOR THE PRIVACY RISK TREATMENT • CNIL INFOGRAFICS - DPIA • DPC Data Protection Impact Assessments (DPIA)
Privacy by design & by default	• Пренесување на главната порака до учесниците во однос на овој нов	• ОРЗЛП чл. 25

	концепт, а тоа е дека Privacy by design & by default се реализира преку техничките и организациски мерки, како компонента на "Data Protection Impact Assessment" • **Privacy by design** - примена на соодветни технички и организациски мерки при дизајнирање на системите во кои се врши обработка на лични податоци и при самата обработка на лични податоци, како што е псевдонимизацијата, сведувањето на минимален обем на податоците и вклучување на потребните заштитни мерки во процесот на обработка, со цел да се исполнат барањата од Закон и да се обезбеди заштита на правата на субјектите на личните податоци. • **Privacy by default** - примена на соодветни технички и организациски мерки со кои се обезбедува интегрирана обработка само на оние лични податоци кои се неопходни за конкретна цел на обработката, како и гаранција дека интегрираните лични податоци без индивидуална интервенција не се автоматски достапни за неограничен број на физички лица.	• Privacy by Design – Information & Privacy Commissioner of Ontario • ENISA Privacy and Data Protection by Design • ENISA Privacy by design in big data • ENISA Study on data collection and storage in the EU • ENISA Privacy Enhancing Technologies: Evolution and State of the Art • ENISA PETs controls matrix – A systematic approach for assessing online and mobile privacy tools • ENISA Online privacy tools for the general public • ENISA Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies

Модул четири		
Име на модулот	**Обврски и одговорности на контролорот**	
Придобивка од учењето	• запознаен е со постапката за водење на Евиденција за активностите на обработка на лични податоци и знае кои информации му се потребни за проверка на оваа евиденција • запознаен е со воспоставените механизми за сертификација на контролорите • има претстава кои елементи треба да ги содржат Кодексот на однесување и Задолжителните корпоративни правила за заштита на приватност • го разбира системот на прекршочни санкции на полето на заштитата на личните податоци	
Тема	**Што ќе опфати темата?**	**Материјал**
Евиденција на активностите на обработка	• Обврска на контролорот да води евиденција на операциите на обработка на лични податоци • Информации што ги содржи евиденцијата	• ОРЗЛП чл. 30, рец. 13
Кодекси на однесување	• Потреба од донесување на Кодекси на однесување, нивно одобрување од Агенцијата и мониторинг на одобрените кодекси	• ОРЗЛП чл. 40, 41
Сертификација	• Услови и начин на сертификација на контролорите за демонстрирање усогласеност со Законот • Сертификациони тела	• ОРЗЛП чл. 42, 43 • ENISA Recommendations on European Data Protection Certification • ENISA Challenges of security certification in emerging ICT environments • ENISA Security certification practice in the EU – Information Security Management Systems - A case study • Законот за заштита на личните податоци • Упатство за начинот на вршење на надворешна контрола 1, 2, 3
Задолжителни корпоративни правила	• Задолжителните корпоративни правила кои се почитуваат од страна на контролорот при пренос на лични податоци во трети земји во рамките на група на друштва (поврзани друштва) или група на правни лица кои вршат заедничка економска дејност	• WP 29 Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules WP 155 rev.04 • WP 29 Working Document Setting up a framework for the structure of Binding Corporate Rules WP 154 • WP 29 Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents WP 212 • WP 29 Explanatory Document on the Processor Binding Corporate Rules WP 204 rev.01 • WP 29 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules WP 256 • WP 29 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules WP 257
Прекршоци за постапување спротивно на одредбите на Закон	• Прекршоците, одмерувањето на глоба, надлежност за водење на прекршочна постапка и судската заштита во прекршочната постапка	• WP29 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

Модул пет		
Име на модулот	**Пренос на лични податоци**	
Придобивка од учењето	Учесникот: • Запознаен е со основните претпоставки и постапката за пренос на лични податоци	
Тема	**Што ќе опфати темата?**	**Материјал**
• Општо начело за пренос	• Услови за пренос во земји членки на ЕУ и ЕЕП • Услови за пренос во трети земји	• Законот за заштита на личните податоци • ОЗЛП чл. 44, 45, 46, 47 • Decision (EU) 2016/1250 • Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop • OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data • OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 2013 • THE OECD PRIVACY FRAMEWORK
• Пренос врз основа на одлука за соодветност	• Елементи врз основа на кои се врши оценка на степенот на соодветност на заштита на личните податоци • Пренос на лични податоци врз основа на одлука за соодветност	• Decision (EU) 2016/1250 • Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop
• Пренос кој подлежи на соодветни заштитни мерки	• Соодветни заштитни мерки што треба да се обезбедат за да се изврши пренос на лични податоци без одлука за соодветност.	• Decision (EU) 2016/1250 • Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop

Модул шест		
Име на модулот	**Видеонадзор**	
Придобивка од учењето	Учесникот: • Запознаен е со условите под кои може да се врши обработка на личните податоци преку систем за вршење на видеонадзор	
Тема	**Што ќе опфати темата?**	**Материјал**
Видеонадзор	• Целите заради кои може да се врши обработка на лични податоци преку системот за вршење видеонадзор • Обврски на контролорот при поставување на систем за вршење на видеонадзор	• Законот за заштита на личните податоци • Правилник за видеонадзор • Судска практика: Снимки од домашен видеонадзор во František Ryneš • Видеонадзор од страна на полиција • Видеонадзор и судска практика PECK v. THE UNITED KINGDOM, • Nevenka ANTOVIĆ and Jovan MIRKOVIĆ against Montenegro • Working Document on the Processing of Personal Data by means of Video Surveillance • Opinion 4/2004 • The EDPS video-surveillance guidelines • Едукативно видео за видеонадзор • Едукативно видео за правото на пристап до личните податоци • ICO CCTV Code of practice (In the picture: A data protection code of practice for surveillance cameras and personal information • WP29 Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance WP 89 • DPC Data Protection and CCTV Судска практика – Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Барање за утврдување повреда на правото на заштита на личните податоци преку вршење на видеонадзор	• Специфики на Барањето • Постапување по истото	• Образец на барање • Е-пријава

Модул седум		
Име на модулот	**Улогата на офицерот за заштита на личните податоци – „Размислувај и постапувај како офицер“**	
Придобивка од учењето	Учесникот: • запознаен е со новата положба што треба да ја има кај контролорот • способен е да го информира, советува и да му дава соодветни препораки на контролорот • способен е самостојно да ја организира работата и да ги извршува задачите пропишани со Закон • способен е да организира и спроведе обука за вработените и менаџерите, како и да процени каков вид на обука да се обезбеди и на кои операции на обработка да посвети најмногу време и ресурси • стекнува поголемо искуство, пракса и вештини за вршење на оваа функција односно го продлабочува стекнатото искуство	
Тема	**Што ќе опфати темата?**	**Материјал**
Критериуми за определување на офицер	Оваа тема ги опфаќа персоналните и професионалните квалитети што треба да ги исполнува офицерот во согласност со Закон	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци
Положба и статус на офицерот (гарантирање на независност)	Оваа тема е срцето на модулот, заради што треба да и се посвети особено внимание. • Темата ги опфаќа сите важни аспекти врз основа на кои се гарантира независната положба на офицерот.	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци
Работи што ги врши офицерот согласно новиот Закон	Оваа тема е исто така клучна за сите учесници во обуката. • Детален опис на работите односно задачите што ги врши офицерот согласно Закон	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци • Е-пријава
„Размислувај и постапувај како офицер“ • Организирање на работата • Управна и судска пракса во областа на заштитата на личните	Организирање на работата од страна на офицерот • Да се даде одговор на прашањата: ○ Како да се зајакне функцијата на офицерот? ○ Како да се организира работата на офицерот за да биде поефикасен? Обучувачите да ги упатат на редовна посета на Катчето за офицери на интернет страницата на ДЗЛП, накратко да ги запознаат и со обрасците наменети за офицерите, но и да им препорачаат да ги користат алатките е-форум и е-конференција. • Анализа на управна и судска пракса во областа на заштитата на личните податоци	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (cArticle 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци • Е-форум • Е-пријава • Е-конференции • Катче за офицери Судска практика - Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)

Прилог бр. 2

Програма за обука за офицерите за заштита на лични податоци

Број	Модул	Придобивка од обуката	Теми
1	**Преглед на правната рамка за заштита на личните податоци**	Учесникот: • го разбира значењето на клучните поими дефинирани со Законот • подготвен е да ги почитува начелата за заштита на лични податоци и да ги примени во пракса, како и да ги запознае соработниците со нив преку внатрешни обуки • способен е да ја анализира усогласеноста на обработката на податоците со Законот • запознаен е дека контролорот има обврска да демонстрира почитување на овие начела • детално е запознаен со статусот, надлежностите, задачите и овластувањата на Агенцијата • способен е да го застапува контролорот при вршење на надзор од страна на надзорниот орган • запознаен е со управните постапки што контролорот ги покренува пред надзорниот орган и со управните постапки што субјектот на лични податоци ги поведува пред надзорниот орган против контролорот	Општа регулатива за заштита на лични податоци на Европскиот парламент и Советот на ЕУ и нејзино транспонирање во новиот Закон за заштита на личните податоци
			Примена на Законот
			Клучни поими и дефиниции
			Начела за заштита на личните податоци и нивното значење
			Агенција за заштита на лични податоци како надзорен орган • Надлежности, задачи и овластувања ○ Супервизија
2	**Комуникација на контролорот со субјектот на лични податоци**	Учесникот: • ги познава правата на субјектот • способен е да води постапки и да одлучува за правата на субјектот на лични податоци • знае да процени како треба да биде формулирана секоја одделна согласност за обработка на лични податоци со јасно дефинирање на целта на обработката на личните податоци и обезбедување на лесен начин за нејзино повлекување • знае да даде конкретни насоки и работни инструкции на вработените кај контролорот кој што вршат директен маркетинг	Права на субјектите
			Услови за согласност
			Услови кои што се применуваат за согласност на дете во однос на услугите на информатичкото општество
3	**Информациска сигурност**	Учесникот: • свесен е за значењето на техничките аспекти за безбедност на обработката на личните податоци • знае кои информации му се потребни за да ги идентификува операциите на обработка на лични податоци • способен е да препознае ризик при одредени операции на обработка на личните податоци • знае што е безбедносен инцидент • запознат е со обврската за известување за нарушување на безбедноста на личните податоци • способен е да напише правилник за технички и организациски мерки за сигурност и тајност при обработката на личните податоци • способен е да подготви Договор за	Безбедност на обработката (Технички и организациски мерки за обезбедување заштита и тајност на обработката на личните податоци)
			Нивоа на техничките и организациски мерки за заштита и тајност на личните податоци и контроли
			Безбедносни инциденти и известување за нарушување на безбедноста на личните податоци
			Безбедност и приватност за услуги кои се пренесуваат на обработувачи (аутсорсинг)
			Физичка безбедност
			Безбедност и приватност на работното место
			Оперативни постапки и одговорности

		• обработка на лични податоци со вклучени одредби кои гарантираат дека обработувачот ќе преземе потребни технички и организациски мерки за заштита и тајност на личните податоци • способен е да оцени кои области треба да бидат предмет на внатрешна или надворешна ревизија/контрола, • способен е да настапи со свој совет при спроведување на „Data Protection Impact Assesment" • го разбира концептот на Privacy by design & by default и способен е да дава совети за негова примена	Планирање и прифаќање на системот Сигурносни копии и логови Сигурност на мрежа и контрола на приватноста Управување и безбедност на медиуми Давање и размена на информации Контрола на пристап на системи Управување со корисниците Следење на системот за пристап и користење Криптирање на податоците Алатки за приватност и безбедност на податоците Технологии кои се опасни по приватност Социјален инженеринг Бришење на податоци Проценка на влијанието на планираните операции на обработка на податоците врз заштитата на личните податоци "Data Protection Impact Assesment" Privacy by design & by default
4	**Обврски и одговорности на контролорот**	Учесникот: • запознаен е со постапката за водење на Евиденција за активностите на обработка на лични податоци и знае кои информации му се потребни за проверка на оваа евиденција • запознаен е со воспоставените механизми за сертификација на контролорите • има претстава кои елементи треба да ги содржат Кодексот на однесување и Задолжителните корпоративни правила за заштита на приватност • го разбира системот на прекршочни санкции на полето на заштитата на личните податоци	Евиденција на активностите на обработка Кодекси на однесување Сертификација Задолжителни корпоративни правила за заштита на приватност Прекршоци за постапување спротивно на одредбите на Законот
5	**Пренос на лични податоци**	Учесникот: • запознаен е со основните претпоставки и постапката за пренос на лични податоци	Општо начело за пренос Пренос врз основа на одлука за соодветност Пренос кој подлежи на соодветни заштитни мерки
6	**Видеонадзор**	Учесникот: • запознаен е со условите под кои може да се врши обработка на личните податоци преку систем за вршење на видеонадзор	Видеонадзор Барање за утврдување повреда на правото на заштита на личните податоци преку вршење на видеонадзор

			Критериуми за определување на офицер (професионални и персонални квалитети)
7	**Улогата на офицерот за заштита на личните податоци** - **„Размислувај и постапувај како офицер“**	Учесникот: • запознаен е со новата положба што треба да ја има кај контролорот • способен е да го информира, советува и да му дава соодветни препораки на контролорот • способен е самостојно да ја организира работата и да ги извршува задачите пропишани со Закон • способен е да организира и спроведе обука за вработените и менаџерите, како и да процени каков вид на обука да се обезбеди и на кои операции на обработка да посвети најмногу време и ресурси • стекнува поголемо искуство, пракса и вештини за вршење на оваа функција односно го продлабочува стекнатото искуство	Положба и статус на офицерот (гарантирање на независност) Работи што ги врши офицерот согласно Законот **„Размислувај и постапувај како офицер“**: • читање и анализирање на управна и судска пракса во Македонија, но и меѓународна пракса – одлуки на Судот на правдата на ЕУ и Европскиот суд за човекови права • студија на случаи • вежби • споделување на индивидуални искуства • организирање на работата од страна на офицерот

1614.

Врз основа на член 103 став (2) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К ЗА ФОРМАТА И СОДРЖИНАТА НА СЛУЖБЕНАТА ЛЕГИТИМАЦИЈА И ЗА НАЧИНОТ НА НЕЈЗИНОТО ИЗДАВАЊЕ И ОДЗЕМАЊЕ

I. ОПШТА ОДРЕДБА

Член 1

Со овој правилник се пропишува формата и содржината на службената легитимација на супервизорите (во натамошниот текст: легитимација), како и начинот на нејзиното издавање и одземање.

II. ФОРМА И СОДРЖИНА НА ЛЕГИТИМАЦИЈАТА

Член 2

(1) Образецот на легитимацијата е изработен на пластифицирана бела хартија со димензии 6 x 9 см, на која што од двете страни, по целата должина е отпечатен грбот на Република Северна Македонија.

(2) На предната страна на легитимацијата е отпечатен меморандумот на Агенцијата за заштита на личните податоци (во натамошниот текст: Агенцијата), под него, во средината, испишани се зборовите „СЛУЖБЕНА ЛЕГИТИМАЦИЈА“, под овие зборови на левата страна има место за фотографија на супервизорот на кој му се издава легитимацијата со димензии 3 x 3,5 см. На десната страна се испишува името и презимето и називот на работното место на супервизорот. Во средината на долниот раб има место за печат, а во долниот десен дел има место за потпис на директорот на Агенцијата.

(3) На задната страна на легитимацијата е содржан следниот текст: „При вршење на супервизија, супервизорот постапува согласно член 105 од Законот за заштита на личните податоци“. Под текстот на десната страна се испишува регистарскиот број на легитимацијата, а под него на левата страна се испишува дата на издавање на легитимацијата.

(4) Образецот на легитимацијата содржи посебна заштита, и тоа:

- треба да биде изработена од хартија со тежина од 200 г; и
- на задната страна треба да има воден печат.

(5) Образецот на легитимацијата од ставот (1) на овој член е сместен во дводелна црна кожна обвивка со димензии 11 x 17 см, која се превиткува на средината.

(6) Образецот на легитимацијата е составен дел на овој правилник (Прилог 1).

III. НАЧИН НА ИЗДАВАЊЕ И ОДЗЕМАЊЕ НА ЛЕГИТИМАЦИЈАТА

Член 3

(1) Легитимацијата се издава од страна на директорот на Агенцијата.

(2) Легитимацијата се издава за периодот додека административниот службеник има својство на супервизор.

Член 4

(1) Легитимацијата се одзема во сите случаи кога супервизорот повеќе не ја врши должноста на супервизор по било која основа.

(2) Легитимацијата се одзема и во случај кога против супервизорот се води постапка за дисциплинска, прекршочна или кривична одговорност во врска со вршењето на должноста на супервизор.

(3) Во случаите од ставовите (1) и (2) на овој член, супервизорот веднаш ја враќа легитимацијата на овластеното лице за човечки ресурси и истата се чува во неговото досие.

(4) Кога легитимацијата не е вратена во согласност со ставот (3) на овој член, истата се одзема со решение донесено од страна на директорот на Агенцијата.

Член 5

(1) Во случај на промена на личните податоци содржани во легитимацијата, по претходно барање на супервизорот, од страна на директорот на Агенцијата се издава нова легитимација, која ги содржи ажурираните лични податоци.

(2) Легитимацијата се заменува со нова и кога поради оштетување или дотраеност ќе стане неупотреблива.

(3) Новата легитимација од ставовите (1) и (2) на овој член, содржи нов регистарски број.

Член 6

За случаите предвидени во член 4 став (4) и член 5 ставови (1) и (2) на овој правилник, легитимацијата се уништува од комисија формирана од страна на директорот на Агенцијата.

Член 7

(1) Во случај на губење на легитимацијата, се известува директорот на Агенцијата и истата се огласува за неважечка во „Службен весник на Република Северна Македонија“.

(2) Изгубената легитимација се заменува со нова која што содржи нов регистарски број.

(3) Трошоците за издавање на нова легитимација заради губење на легитимацијата, супервизорот ја надоместува од сопствени средства.

IV. ПОСЕБНИ ОДРЕДБИ

Член 8

(1) За секое издавање, одземање, заменување, уништување и губење на легитимацијата, во Агенцијата се води евиденција.

(2) Евиденцијата од ставот (1) на овој член се води по електронски пат на посебен образец кој содржи податоци за: реден број, име и презиме на супервизорот, звање на супервизорот, дата на издавањето на легитимацијата, регистарскиот број на легитимацијата, дата на враќање на легитимацијата, дата на заменување на легитимацијата, број и дата на решение за одземање на легитимацијата, број и дата на решение за формирање на комисија за уништување на легитимацијата, дата на уништување на легитимацијата, дата на известување за губење на легитимацијата и забелешки.

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 9

(1) Легитимациите издадени согласно одредбите на Правилникот за образецот, формата и содржината на легитимацијата и за начинот на нејзиното издавање и одземање („Службен весник на Република Македонија“ бр. 143/08 и 158/10) ќе се заменат со нови во рок од 180 дена од денот на влегувањето во сила на овој правилник.

(2) Старите легитимации од ставот (1) на овој член се уништуваат од комисија формирана од страна на директорот на Агенцијата.

Член 10

Со денот на влегувањето на овој правилник престанува да важи Правилникот за образецот, формата и содржината на легитимацијата и за начинот на нејзиното издавање и одземање („Службен весник на Република Македонија“ бр.143/08 и 158/10).

Член 11

Овој правилник влегува во сила наредниот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-605/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Прилог 1

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ
С Л У Ж Б Е Н А Л Е Г И Т И М А Ц И Ј А

М.П. Директор,

Предна страна

При вршење на супервизија, супервизорот постапува согласно член 105 од Законот за заштита на личните податоци

Воден печат

Дата на издавање _____ **Регистарски број** _____

Задна страна

1615.

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), а во врска со Насоките за проценка на влијанието врз заштитата на личните податоци (ПВЗЛП) и утврдување дали обработката „веројатно ќе резултира со висок ризик“ за целите на Регулативата 2016/679 (WP 248 rev.01) од Работната група 29 за заштита на личните податоци при Европската унија, директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К ЗА ПРОЦЕСОТ НА ПРОЦЕНКА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишуваат упатства за контролорот при процесот на спроведување на проценката на влијанието на заштитата на личните податоци.

Член 2

Проценката на влијанието на заштитата на личните податоци во смисла на овој правилник претставува процес дизајниран да ја опише обработката на личните податоци, да ја процени нејзината неопходност и пропорционалност и да помогне во управувањето со ризиците за правата и слободите на физичките лица кои ќе настанат со обработката преку нивна проценка, како и да се предвидат мерки за справување со тие ризици (во натамошниот текст: ПВЗЛП).

II. СЛУЧАИ ВО КОИ Е ЗАДОЛЖИТЕЛНА ПВЗЛП

Член 3

(1) Во смисла на член 39 став (1) од Законот за заштита на личните податоци, контролорот задолжително спроведува ПВЗЛП кога постои веројатност обработката да предизвика висок ризик за правата и слободите на физичките лица, а особено кога се воведуваат нови технологии за обработка на личните податоци, според природата, обемот, контекстот и целите на обработката, како и кога обработката е вклучена во Листата на видовите операции на обработка за кои се бара ПВЗЛП воспоставена од Агенцијата за заштита на личните податоци (во натамошниот текст: Агенцијата).

(2) Контролорот спроведува ПВЗЛП пред да започне со обработка на личните податоци, притоа обезбедувајќи техничка и интегрирана заштита на личните податоци, односно во фаза на планирање на операциите на обработка, како и кога некои од операциите на обработка се сè уште непознати.

(3) По исклучок од ставот (2) на овој член, контролорот задолжително спроведува ПВЗЛП и пред да се направат значителни промени на некои постојни операции на обработка на лични податоци, а кои претходно биле проверени од страна на Агенцијата.

Член 4

Контролорот за да определи кои операции на обработка веројатно ќе резултираат со висок ризик и за кои ПВЗЛП е задолжителна, мора да ги има во предвид најмалку еден од следните критериуми:

1. Евалуација или бодирање, вклучително и профилирање и предвидување, особено врз основа на аспекти поврзани со работењето на субјектот на лични податоци, економската состојба, здравјето, личните преференции или интереси, сигурност или однесување, локацијата или движења.

2. Автоматско донесување одлуки со правно или слично суштинско дејство, односно обработка насочена кон донесување на одлуки за субјектите на лични податоци што произведуваат правни последици за физичкото лице или на сличен начин значајно влијаат на физичкото лице.

3. Систематско набљудување, односно обработка која се користи за следење, набљудување или контрола на субјектите на лични податоци, вклучително и податоци собрани преку мрежи или „систематско набљудување на јавно достапни простори“.

4. Чувствителни податоци или податоци од изразита лична природа: ова вклучува посебни категории на лични податоци кои се определени во членот 4 став (1) точка 13 од Законот за заштита на личните податоци, како и лични податоци поврзани со казнени осуди и казнени дела.

5. Обемна обработка на податоци. При утврдување дали обработката е обемна според околностите на секој конкретен случај, се земаат предвид следниве фактори:

- број на засегнати субјекти на лични податоци, било да е конкретен број или процент од релевантното население;
- обем на податоци и/или опфат на различни видови податоци што се обработуваат;
- траење или непрекинатост на операциите на обработка на личните податоци; и
- географскиот опсег на активностите за обработка на личните податоци.

6. Сет од лични податоци што се совпаѓаат или комбинираат, на пример оние кои потекнуваат од две или повеќе операции на обработка на лични податоци кои се извршени за различни цели и/или од различни контролори на начин што ги надминува разумните очекувања на субјектот на личните податоци.

7. Податоци кои се однесуваат на ранливи субјекти на лични податоци: обработката на овој вид на податоци е критериум заради зголемената нерамнотежа на моќта помеѓу субјектите на лични податоци и контро-

лорите, при што физичките лица не можат едноставно да се согласат или да се спротивстават на обработката на нивните податоци или да ги остварат своите права. Ранливи субјекти на лични податоци може да вклучуваат деца, вработени, ранливи групи на кои им е потребна посебна заштита (лица со ментална попреченост, баратели на азил или постари лица, пациенти и др.). како и секој друг случај кога може да се идентификува нерамнотежа во односот помеѓу положбата на субјектот на личните податоци и контролорот.

8. Иновативна употреба или примена на нови технолошки или организациски решенија, како што се комбинирање на употреба на отпечаток од прст и препознавање на лице за подобрување на контролата на физичкиот пристап, итн.

9. Ситуации кога самата обработка ги спречува субјектите на лични податоци да остварат одредени права или да користат услуга или договор. Ова вклучува процедури за обработка кои се насочени кон овозможување, модифицирање или одбивање на пристапот на субјектите на личните податоци до одредена услуга или склучување на договор.

III. СЛУЧАИ КОГА ПВЗЛП НЕ Е ЗАДОЛЖИТЕЛНА

Член 5

(1) ПВЗЛП е незадолжителна во следните случаи кога:

- операциите на обработка може да одговараат на случаите наведени во членот 4 на овој правилник, но контролорот оценил дека истите нема веројатност да резултираат со висок ризик за правата и слободите на физичките лица;

- природата, обемот, контекстот и целите на обработката се слични на обработката за која била спроведена ПВЗЛП; и

- обработката е вклучена во Листата на видовите операции на обработка за кои не се бара ПВЗЛП воспоставена од Агенцијата.

(2) Контролорот задолжително ги оправдува и документира причините за неизвршување на ПВЗЛП при што го наведува и мислењето на офицерот за заштита на личните податоци (во натамошниот текст: офицерот).

IV. УЛОГИ И ОДГОВОРНОСТИ

Член 6

(1) Во смисла на член 39 од Законот за заштита на личните податоци, контролорот е исклучиво одговорен да го спроведува ПВЗЛП при што ги определува лицата задолжени за извршување на ПВЗЛП и ги документира советите и одлуките на офицерот во рамките на ПВЗЛП.

(2) Во согласност со ставот (1) на овој член, контролорот при спроведување на ПВЗЛП може да ангажира надворешни лица или да побара совет или мислење од независни експерти, а според природата на технолошките и организациските решенија кои ќе се применуваат при операциите на обработка на личните податоци.

(3) Кога обработката целосно или делумно ќе биде извршувана од страна на обработувачот, тогаш обработувачот е должен да му помогне на контролорот во спроведувањето на ПВЗЛП при што улогите, обврските и одговорностите на контролорот и обработувачот задолжително се дефинираат со договор согласно прописите за заштита на личните податоци.

V. БАРАЊЕ НА МИСЛЕЊЕ ОД СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

Член 7

(1) Според околностите на секој конкретен случај за кој се изработува ПВЗЛП, контролорот може да побара мислење од субјектите на личните податоци или нивните претставници, преку различни средства, во зависност од контекстот (на пример, општа студија поврзана со целта и средствата на процесот на обработка, со поставување на прашања до претставниците на субјектите на лични податоци, или преку анкети кои се испраќаат до идните клиенти на контролорот).

(2) Кога конечната одлука на контролорот се разликува од мислењето на субјектите на лични податоци, причините за продолжување или прекин на обработката на личните податоци задолжително треба да се документираат при процесот на ПВЗЛП.

(3) Кога контролорот ќе одлучи да не бара мислење од субјектите на лични податоци (на пример: доколку со тоа би се загрозила доверливоста на работните планови во организацијата или истото е несразмерно или неизводливо), образложението за ваквата одлука треба да се документира при процесот на ПВЗЛП.

VI. ПРЕИСПИТУВАЊЕ НА ПВЗЛП

Член 8

(1) Контролорот го преиспитува ПВЗЛП по промена на ризиците што произлегуваат од операциите на обработка (на пример, употреба на нова технологија, кога личните податоци се користат за друга цел итн.).

(2) Доколку одредени промени го намалат ризикот, во вакви ситуации, преиспитувањето на направената анализа на ризик може да покаже дека не е потребно контролорот да спроведе ПВЗЛП.

VII. ОСНОВНИ КАРАКТЕРИСТИКИ НА ПВЗЛП

Член 9

(1) ПВЗЛП задолжително содржи:

- опис на предвидените операции на обработка и целите на обработката;

- проценка на потребата и пропорционалноста на обработката;

- проценка на ризиците за правата и слободите на субјектите на личните податоци; и
- мерки предвидени за:
  - управување со ризиците; и
  - демонстрирање на усогласеност со прописите за заштита на личните податоци.

(2) Процесот на спроведување на ПВЗЛП графички е прикажан во Прилогот бр.1 кој е составен дел на овој правилник.

Методологија за спроведување на ПВЗЛП

Член 10

Контролорот задолжително донесува соодветна Методологија за спроведување на ПВЗЛП според критериумите дадени во Прилогот бр. 2 кој е составен дел на овој правилник.

Фази на спроведување на ПВЗЛП

Член 11

ПВЗЛП се спроведува во четири фази и тоа:

1. Дефинирање на контекстот – во првата фаза се дефинира контекстот на обработка и се наведуваат, односно опишуваат најмалку следниве информации:
- збирка на лични податоци;
- цел на обработката;
- движење на податоци;
- метод(и) на добивање на податоците;
- начин и средства за обработка на податоците (користена опрема, мрежи, човечки ресурси итн.);
- субјекти кои се вклучени во обработката (контролори, обработувачи, корисници итн.); и
- рок на чување.

2. Анализа на ризик – во втората фаза се идентификуваат заканите (несакани исходи), како и се одредува веројатноста и влијанието (последицата) од остварување на секој ризик.

Ризикот се изразува како функција од веројатноста да се случи несаканиот исход (заканата) и влијанието (последицата) од несаканиот исход доколку се случи.

Ризикот = (веројатност да се случи заканата) x (степен на влијанието)

Влијанието може да биде:
- ниско, кога физичките лица можат да се соочат со неколку помали непријатности, кои ќе ги надминат без проблем;
- средно, кога физичките лица можат да се соочат со значителни непријатности, кои ќе можат да ги надминат и покрај одредени тешкотии;
- високо, кога физичките лица можат да се соочат со значителни последици, кои би требало да можат да ги надминат, но со сериозни тешкотии; и
- многу високо, кога физичките лица можат да се соочат со значителни, па дури и неповратни последици, кои најверојатно нема да можат да ги надминат.

Проценката на ризикот се спроведува според начелата за заштита на личните податоци.

3. Управување со ризик – во третата фаза треба да се опфатат заштитните мерки, односно мерките на безбедност и механизмите дизајнирани да го намалат ризикот на прифатливо ниво, како и да се обезбеди заштита на личните податоци и да се прикаже усогласеност со прописите за заштита на личните податоци.

Мерките, исто како и кај проценката на ризикот треба да се поделат според начелата за заштита на личните податоци.

4. Составување извештај од спроведена ПВЗЛП – Контролорот ги документира сите фази на спроведување на ПВЗЛП, по што изработува извештај.

Извештајот од спроведената ПВЗЛП особено содржи: опис на процесот на обработка, внатрешни и надворешни лица вклучени во процесот на спроведување на ПВЗЛП, анализа на ризик, дефинирани мерки за управување со ризикот, резиме/заклучок, акциски план, мислење на офицерот и на другите лица вклучени во процесот, одобрување на ПВЗЛП од страна на функционерот или одговорното лице кај контролорот.

Објавување на ПВЗЛП

Член 12

(1) Контролорот самостојно одлучува дали јавно ќе го објави извештајот од ПВЗЛП.

(2) Контролорот демонстрира почитување на начелото на отчетност и транспарентност преку објавување на делови од извештајот, на пример преку објавување на краток преглед или заклучок од спроведената ПВЗЛП.

(3) Контролорот е должен да го достави извештајот од спроведената ПВЗЛП на барање на Агенцијата.

VIII. КОНСУЛТАЦИЈА СО АГЕНЦИЈАТА

Член 13

Кога контролорот не може да најде соодветни мерки за да го намали ризикот на прифатливо ниво (т.е. ако преостанатите ризици останат високи), задолжително се консултира со Агенцијата во смисла на член 40 од Законот за заштита на личните податоци.

IX. ЗАВРШНА ОДРЕДБА

Член 14

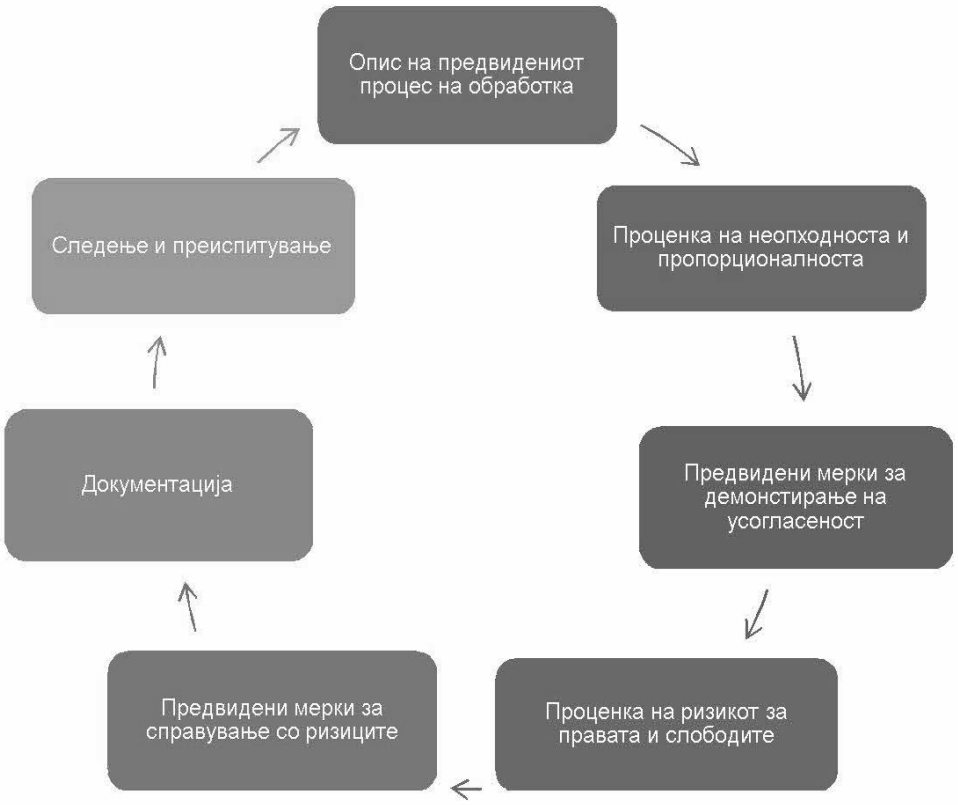
Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-606/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Прилог бр. 1

Графички приказ на процесот за спроведување на ПВЗЛП



Напомена: Секоја од фазите ќе треба да се спроведе неколку пати пред да заврши ПВЗЛП.

Прилог бр. 2

Критериуми за прифатлива ПВЗЛП

Критериумите што контролорот може да ги користи за да оцени дали ПВЗЛП или методологијата за спроведување на ПВЗЛП е доволно сеопфатна за да се усогласи со прописите за заштита на личните податоци, се следни:

- ☐ проценката содржи систематски опис на обработката:
  - ☐ земени се предвид природата, обемот, контекстот и целите на обработката;
  - ☐ евидентирани се личните податоци, примателите и периодот на чување на личните податоци;
  - ☐ даден е функционален опис на операцијата на обработка;
  - ☐ идентификувани се средства од кои зависат личните податоци (опрема, софтверски програми, мрежи, лица, документи во хартиена форма или канали за испраќање документи во хартиена форма);
  - ☐ исто така, земена е предвид усогласеноста со одобрените кодекси на однесување;
- ☐ проценета е неопходноста и пропорционалноста:
  - ☐ одредени се мерките предвидени за усогласување со прописите за заштита на личните податоци, земајќи ги предвид:
    - ☐ мерки што придонесуваат за пропорционалност и неопходност од обработка врз основа на:
      - ☐ конкретни, јасни и легитимни цели;
      - ☐ законитост на обработката;
      - ☐ соодветни и релевантни лични податоци и ограничени на она што е потребно;
      - ☐ ограничен рок на чување;
    - ☐ мерки кои придонесуваат за правата на субјектите на личните податоци:
      - ☐ информации доставени на субјектот на личните податоци;
      - ☐ право на пристап и преносливост на податоците;
      - ☐ право на исправка и бришење;
      - ☐ право на приговор и ограничување на обработката;
      - ☐ односи со обработувачите;
      - ☐ заштитни мерки кои се однесуваат на преносот;
      - ☐ претходна консултација.
- ☐ контролирани се ризиците за правата и слободите на испитаниците:
  - ☐ се проценува изворот, природата, особеноста и сериозноста на ризикот или подетално, за секој ризик (неовластен пристап, несакани промени и исчезнати податоци) од гледна точка на субјектите на личните податоци:
    - ☐ земени се предвид изворите на ризик;
    - ☐ утврдени се можните ефекти врз правата и слободите на субјектите на личните податоците, меѓу другото, во случај на неовластен пристап, несакани промени и исчезнати податоци;
    - ☐ идентификувани се закани што може да доведат до неовластен пристап, несакана промена и исчезнати податоци;
    - ☐ проценета е веројатноста и сериозноста;
  - ☐ предвидени се одредени мерки за да се отстранат овие ризици;
- ☐ вклучени се засегнатите страни:
  - ☐ побаран е совет од офицерот;
  - ☐ каде што е соодветно, побарани се мислења на субјектите на личните податоци или нивните претставници.

1616.

Врз основа на член 97 став (3) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К

ЗА ФОРМАТА И СОДРЖИНАТА НА БАРАЊЕТО ЗА УТВРДУВАЊЕ НА ПРЕКРШУВАЊЕ НА ОДРЕДБИТЕ ОД ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 1

Со овој правилник се пропишува формата и содржината на барањето за утврдување на прекршување на одредбите од Законот за заштита на личните податоци (Образец бр. 1).

Образецот од ставот 1 на овој член е составен дел на овој правилник.

Член 2

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за формата и содржината на барањето за утврдување на повреда на правото на заштита на личните податоци („Службен весник на Република Македонија“ бр. 144/11).

Член 3

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-607/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1

БАРАЊЕ

1. Податоци за подносителот на барањето:

1.1. Податоци за подносител – физичко лице
Име: _____
Презиме: _____
Адреса на живеење и место за доставување на писмена:
Контакт-телефон: _____
Електронска пошта: _____

1.2. Податоци за подносител – здружение на граѓани
(Во статутот на здружението задолжително треба да бидат наведени целите кои се од јавен интерес, неговиот непрофитен карактер и истото активно да дејствува во областа на заштитата на личните податоци и во заштитата на правата и слободите на субјектите на лични податоци – член 100 став (2) од Законот за заштита на личните податоци)

Назив: _____
Седиште: _____
Место за доставување на писмена:
_____
Контакт-телефон: _____
Електронска пошта: _____
Име и презиме и адреса на живеење на физичкото лице кое го овластило здружението да поднесе барање во негово име во однос на заштитата на неговите лични податоци:
(Во прилог на барањето, потребно е да го доставите и овластувањето со кое физичкото лице кое го овластило здружението да поднесе барање во негово име во однос на заштитата на неговите лични податоци)
_____
_____

1.3. Податоци за законскиот застапник доколку го има:
Име: _____
Презиме: _____
Контакт-телефон: _____

2. Податоци за правното/физичкото лице кое сметате дека ги повредило Вашите лични податоци:
Назив на правното лице/име и презиме на физичкото лице:

_____

Седиште на правното лице/адреса на живеење на физичкото лице:

_____

Телефон: _____
Факс (доколку знаете): _____
Електронска пошта: (доколку знаете): _____

3. Краток опис на повредата на Вашите лични податоци:

_____
_____
_____
_____

4. Специфицирајте ги документите кои ги давате во прилог како докази кои го поткрепуваат погоре наведеното барање:

_____
_____
_____
_____
_____

Тврдам дека погоре наведените податоци се точни и целосни.

Датум: Потпис на подносителот*
____.____.202__ _____

* Актите во хартиена форма се потпишуваат своерачно, додека електронските исправи се комплетираат со отпечатено име на потписникот и се поврзуваат со општо прифатен електронски потпис во согласност со прописите што ја уредуваат употребата на електронските документи, електронскиот потпис и електронскиот печат и електронските доверливи услуги во управни и судски постапки.

1617.

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), а во врска со Насоките за известување за нарушување на безбедноста на личните податоци според Регулативата 2016/679 (WP250 rev.01) од Работната група 29 за заштита на личните податоци при Европската Унија, директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА НАЧИНОТ НА ИЗВЕСТУВАЊЕ ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТИ ОДРЕДБИ

Член 1

Со овој правилник се пропишува начинот на доставување на Известувањето до Агенцијата за заштита на личните податоци (во натамошниот текст: Агенцијата) за нарушување на безбедноста на личните податоци, начинот на известување на субјектот на личните податоци за нарушувањето на безбедноста на личните податоци, како и активностите кои што контролорот треба да ги преземе при нарушување на безбедноста на личните податоци.

Член 2

Одредбите од овој правилник соодветно се применуваат и над обработувачот на збирка на лични податоци откако дознал за нарушување на безбедноста на личните податоци во смисла на одредбите од членот 37 став (2) од Законот за заштита на личните податоци.

II. ДОСТАВУВАЊЕ НА ИЗВЕСТУВАЊЕТО ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ ДО АГЕНЦИЈАТА

Член 3

(1) Во случај на нарушување на безбедноста на личните податоци, контролорот е должен во рокот предвиден во членот 37 став (1) од Законот за заштита на личните податоци да ја извести Агенцијата за нарушувањето на безбедноста на личните податоци, по електронски пат на incident@privacy.mk или на https://eprijavi.privacy.mk/. Прилогот во електронската пошта треба да биде електронски потпишан од страна на функционерот, или на одговорното лице на контролорот или истиот да биде во скенирана форма од кој јасно може да се гледа своерачниот потпис на функционерот, или на одговорното лице на контролорот.

(2) Во смисла на член 37 став (3) од Законот за заштита на личните податоци, известувањето од ставот (1) на овој член ги содржи следните податоци:

- опис на природата на нарушувањето на безбедноста на личните податоци, вклучувајќи, категориите и приближниот број на засегнати субјекти на личните податоци (во зависност од користените идентификатори, ова може да вклучува, меѓу другите, деца и други ранливи групи, лица со посебни потреби, вработени или клиенти), како и категориите и приближниот број на засегнати евидентирани лични податоци (на пример: здравствени податоци, матични броеви на граѓаните (ЕМБГ), информации за социјална помош, финансиски податоци, броеви на банкарски сметки, броеви на пасоши и слично);

- наведување на името, презимето и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации;

- опис на можните последици од нарушувањето на безбедноста на личните податоци (на пример: потенцијални последици и негативни ефекти на засегнати субјекти на лични податоци); и

- опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти (на пример: технички и организациски мерки што се преземени од контролорот со цел да ги намали можните негативни ефекти, дадени совети на засегнатите субјекти на лични податоци за да се заштитат од можните неповолни последици од нарушувањето на безбедноста на личните податоци, како што е промена на лозинки во случај кога нивните привелегии за пристап се компромитирани).

(3) Покрај податоците од ставот (2) на овој член, според околностите на секој конкретен случај, во известувањето од ставот (1) на овој член, може да се внесат и следните податоци:

- датум и време на инцидентот (доколку се знае, во спротивно може да се направи процена);

- датум и време на детектирање на инцидентот;

- услови под кои што е настанато нарушувањето на безбедноста на личните податоци (на пример: загуба, кражба...);

- име, презиме и потпис на лицата кои констатирале нарушување на безбедноста на личните податоци;

- дали во инцидентот е вклучен и обработувачот, при што ако е вклучен, се наведуваат и неговите податоци (назив и седиште, односно име и презиме и адреса на живеење, податоци за офицерот за заштита на личните податоци и други контакт податоци);

- дали е информиран офицерот за заштита на личните податоци на контролорот за нарушувањето на безбедноста на личните податоци;

- оценка/мислење од офицерот за заштита на личните податоци преку преземени или предложени мерки за справување со нарушувањето на безбедноста на личните податоци;

- сумарен преглед на нарушувањето на безбедноста на личните податоци (вклучително физичка локација и медиум на кој се складирани податоците);

- статистички податоци за нарушување на безбедноста на личните податоци, односно констатирање дали инцидентот првпат се појавува;

- известување до субјектот на личните податоци – ДА/НЕ;

- содржина на известувањето до засегнатите субјекти на лични податоци;

- комуникациска технологија преку која е испратено известувањето;

- број на субјекти на лични податоци што се известени;

- други податоци на контролорот, доколку ги има за настанатиот случај.

(4) Образецот на известувањето од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 1).

III. ИЗВЕСТУВАЊЕ НА СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 4

(1) Во смисла на член 38 ставови (1) и (2) од Законот за заштита на личните податоци, контролорот во известувањето до субјектот на личните податоци ги наведува следните податоци:

- опис на природата на нарушувањето на безбедноста на личните податоци;

- името, презимето и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации;

- опис на можните последици од нарушувањето на безбедноста на личните податоци; и

- опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти.

(2) Според околностите на секој конкретен случај, во известувањето од ставот (1) на овој член, може да се внесат и следните податоци:

- датум и време на инцидентот (доколку се знае);

- причина поради која дошло до нарушување на безбедноста на личните податоци;

- услови под кои што е настанато нарушувањето на безбедноста на личните податоци (на пример: загуба, кражба...); и

- име, презиме и потпис на функционерот, или на одговорното лице во контролорот.

(3) Образецот на известувањето од ставот (1) на овој член е составен дел на овој правилник (Образец бр. 2).

IV. АКТИВНОСТИ НА КОНТРОЛОРОТ

Член 5

(1) Во смисла на член 37 став (5) од Законот за заштита на личните податоци, контролорот е должен детално да го документира нарушувањето на безбедноста на личните податоци, како и да воспостави внатрешен процес на евидентирање на нарушувањата на безбедноста на личните податоци, без оглед дали ќе биде потребно да се извести Агенцијата според прописите за заштита на личните податоци.

(2) Процесот на евидентирање од ставот (1) на овој член, ги содржи следните податоци за:

- природата (факти и причини) за нарушување на безбедноста на личните податоци;

- категориите и приближниот број на засегнати субјекти на личните податоци;

- категориите и приближниот број на засегнати евидентирани лични податоци;

- вклученоста и улогата на обработувачот при нарушување на безбедноста на личните податоци;

- ефектите и последиците предизвикани од нарушување на безбедноста на личните податоци;

- преземените мерки за справување со нарушувањето на безбедноста на личните податоци;

- преземените превентивни мерки; и

- други информации што и овозможуваат на Агенцијата да ја провери усогласеноста на контролорот со прописите за заштита на личните податоци.

(3) Активностите кои што контролорот треба да ги преземе при нарушување на безбедноста на личните податоци се наведени во Прилогот бр.1 кој е составен дел на овој правилник.

(4) Офицерот за заштита на личните податоци задолжително треба да биде информиран и вклучен во целиот процес на управување и известување за нарушувањето на безбедноста на личните податоци преку давање совети и следење на усогласеноста со прописите за заштита на личните податоци при нарушувањето на безбедноста на личните податоци, како и за време на секоја последователно истражување од Агенцијата.

V. ЗАВРШНА ОДРЕДБА

Член 6

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-608/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1

ИЗВЕСТУВАЊЕ
за нарушување на безбедноста на личните податоци
до Агенцијата за заштита на личните податоци
(се доставува на: incident@privacy.mk или https://eprijavi.privacy.mk/)

1.	Назив и седиште на контролорот	
2.	Опис на природата на нарушувањето на безбедноста на личните податоци, вклучувајќи, категориите и приближниот број на засегнати субјекти на личните податоци, како и категориите и приближниот број на засегнати евидентирани лични податоци	
3.	Име, презиме и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации	
4.	Опис на можните последици од нарушувањето на безбедноста на личните податоци	
5.	Опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти	
6.	Датум и време на инцидентот (доколку се знае, во спротивно може да се направи процена)	
7.	Датум и време на детектирање на инцидентот	
8.	Услови под кои што е настанато нарушувањето на безбедноста на личните податоци	
9.	Име, презиме и потпис на лицата кои констатирале нарушување на безбедноста на личните податоци	
10.	Дали во инцидентот е вклучен и обработувачот, при што ако е вклучен, се наведуваат и неговите податоци (назив и седиште, односно име и презиме и адреса на живеење, податоци за офицерот за заштита на личните податоци и други контакт податоци)	
11.	Дали е информиран офицерот за заштита на личните податоци на контролорот за нарушувањето на безбедноста на личните податоци	
12.	Оценка/мислење од офицерот за заштита на личните податоци преку преземени или предложени мерки за справување со нарушувањето на безбедноста на личните податоци	
13.	Сумарен преглед на нарушувањето на безбедноста на личните податоци (вклучително физичка локација и медиум на кој се складирани податоците)	
14.	Статистички податоци за нарушување на безбедноста на личните податоци, односно констатирање дали инцидентот првпат се појавува	
15.	Известување до субјектот на личните податоци – ДА/НЕ	
16.	Содржина на известувањето до засегнатите субјекти на лични податоци	
17.	Комуникациска технологија преку која е испратено известувањето	
18.	Број на субјекти на лични податоци што се известени	
19.	Други податоци на контролорот, доколку ги има за настанатиот случај	

_____, ___.___.202___ година
(место) (датум)

Име, презиме и потпис на
функционерот, односно одговорното лице во Контролорот

_____

Образец бр. 2

ИЗВЕСТУВАЊЕ

на субјектот на личните податоци за нарушување на безбедноста на личните податоци

1.	Природа на нарушувањето на безбедноста на личните податоци	
2.	Име, презиме и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации	
3.	Опис на можните последици од нарушувањето на безбедноста на личните податоци	
4.	Опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти	
5.	Датум и време на инцидентот (доколку се знае)	
6.	Причина поради која дошло до нарушување на безбедноста на личните податоци	
7.	Услови под кои што е настанато нарушувањето на безбедноста на личните податоци	

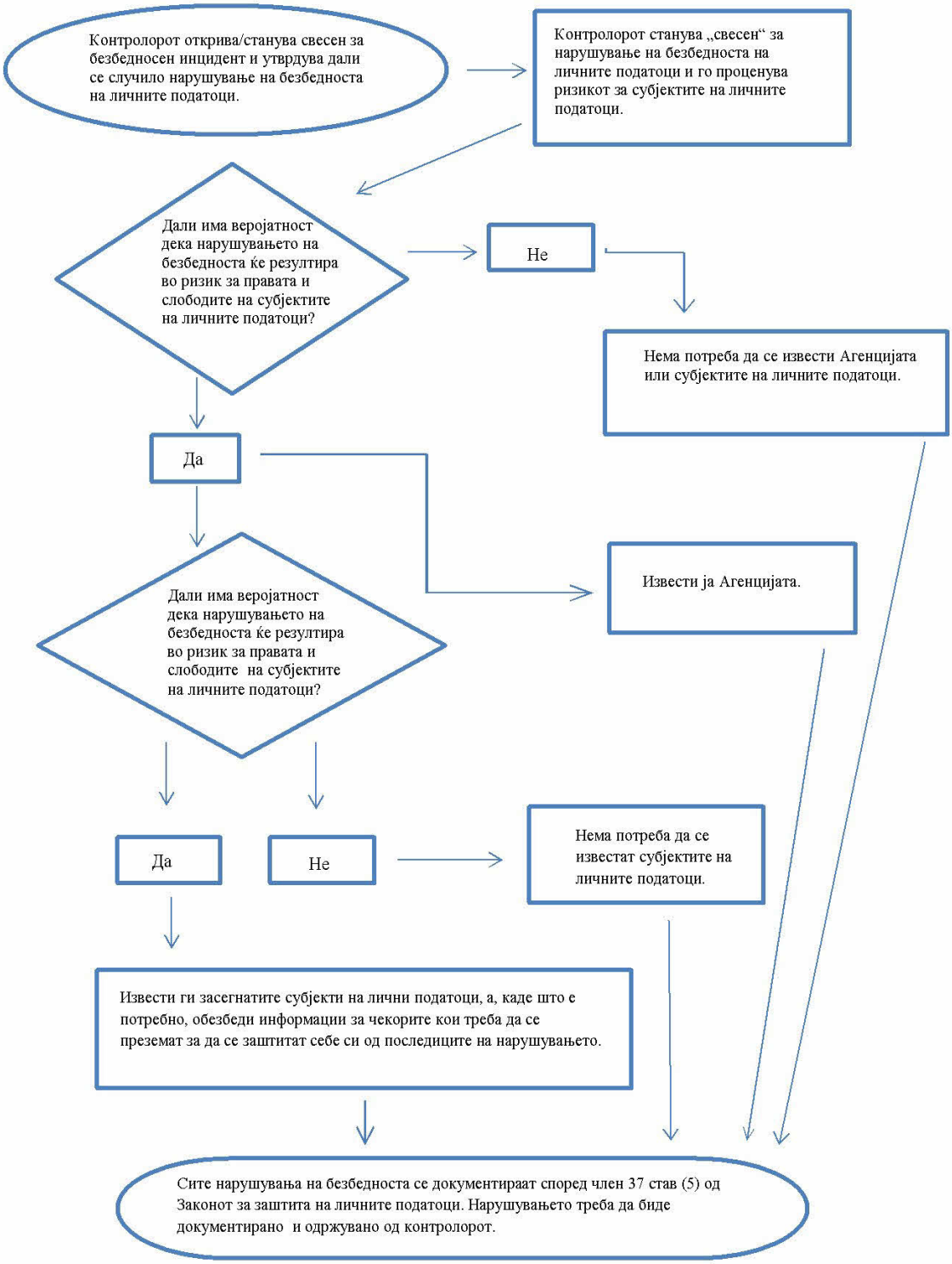
_____, ____.____.202___ година
(место) (датум)

Име, презиме и потпис на
функционерот, односно одговорното лице во Контролорот

_____

Прилог бр. 1

Дијаграм за активностите на контролорот кои ги презема за нарушување на безбедноста на личните податоци



1618.

Врз основа на член 71 став (4) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА ИЗВЕСТУВАЊЕ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ СО ВИСОК РИЗИК

I. ОПШТА ОДРЕДБА

Член 1

Со овој правилник се пропишува формата и содржината на образецот на Известувањето за обработка на лични податоци која предизвикува висок ризик за правата и слободите на физичките лица (во натамошниот текст: Известување), начинот на известување на Агенцијата за заштита на личните податоци (во натамошниот текст: Агенција), како и формата и содржината на евиденцијата на збирки на лични податоци со висок ризик.

II. ФОРМА И СОДРЖИНА НА ОБРАЗЕЦОТ НА ИЗВЕСТУВАЊЕТО

Член 2

(1) Образецот на Известувањето е составен од два дела и ги содржи податоците во смисла на член 71 од Законот за заштита на личните податоци и тоа:

1. ДЕЛ 1 – Податоци за контролорот

1.1. Правно лице, орган на државната власт, државен орган, правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело

- Назив на контролорот;
- Даночен број;
- Претежна дејност;
- Организациска форма;
- Општина;
- Населено место;
- Контакт-телефон;
- Електронска пошта;
- Факс;
- Веб-страница;
- Одговорно лице;
- Име и презиме на офицерот за заштита на личните податоци;
- Контакт телефон на офицерот на заштита на личните податоци;
- Електронска пошта на офицерот за заштита на личните податоци;
- Работно место или број и датум на договор за ангажирање на офицерот за заштита на личните податоци;
- Назив/име на овластениот претставник доколку го има; и
- Седиште/адреса на живеење на овластениот претставник.

1.2. ДЕЛ 2 – Податоци за контролорот – Физичко лице

- Име и презиме;
- Место и адреса на живеење;
- Податоци за вработување (занимање или функција што ја врши);
- Датум на раѓање;
- Место на раѓање; и
- Државјанство.

2. Назив на збирката на лични податоци;

3. Цел или цели на обработката;

4. Правна основа за воспоставување збирка на лични податоци;

5. Опис на категориите на субјектите на личните податоци и на категориите на лични податоци кои се однесуваат на нив;

6. Категориите на корисници на кои се, или ќе бидат откриени личните податоци, вклучувајќи корисници во трети земји или меѓународни организации;;

7. Рок на чување на личните податоци, односно предвидените рокови за бришење на различните категории на лични податоци;

8. Пренос на личните податоци во трета земја или меѓународна организација;

9. Општ опис на преземените технички и организациски мерки за обезбедување на безбедност на личните податоци; и

10. Број и датум на проценката на влијанието на заштитата на личните податоци.

(2) При пополнувањето на Образецот од ставот (1) на овој член, делот 1 се пополнува само од страна на контролорот – правно лице од потточката 1.1, а делот 2 се пополнува само од страна на контролорот – физичко лице од потточка 1.2.

(3) Образецот на Известувањето од ставот (1) на овој член е составен дел на овој правилник (Обрасци бр, 1 и бр.2).

III. НАЧИН НА ИЗВЕСТУВАЊЕ НА АГЕНЦИЈАТА ЗА ОБРАБОТКАТА НА ЛИЧНИ ПОДАТОЦИ КОЈА ПРЕТСТАВУВА ВИСОК РИЗИК

1. Пријавување на збирки на лични податоци со висок ризик

Член 3

Известувањето се доставува од страна на контролорот во електронска форма преку веб-страницата на Агенцијата заради евидентирање во евиденцијата на збирки на лични податоци со висок ризик.

Член 4

За доставување на Известувањето, контролорот претходно електронски се регистрира во евиденцијата на збирки на лични податоци со висок ризик преку самостојно определување на корисничко име и лозинка за пристап.

Член 5

(1) По регистрацијата, контролорот во системот на евиденцијата на збирки на лични податоци со висок ризик ги внесува следните податоци:

- назив на контролорот – правно лице, орган на државната власт, државен орган, правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело; даночен број; претежна дејност; организациска форма; општина; населено место; контакт-телефон; електронска пошта; факс; веб-страница; одговорно лице; име и презиме на офицерот за заштита на личните податоци; контакт телефон на офицерот на заштита на личните податоци; електронска пошта на офицерот за заштита на личните податоци и работно место или број и датум на договор за ангажирање на офицерот за заштита на личните податоци; назив, односно име на овластениот претставник доколку го има и седиште, односно адреса на живеење на овластениот претставник и

- контролор – физичко лице: име и презиме; место и адреса на живеење; податоци за вработување (занимање или функција што ја врши); датум на раѓање; место на раѓање и државјанство.

(2) По внесувањето на податоците од ставот (1) на овој член, контролорот го отпечатува конфирмациското писмо и врши електронско внесување на податоците за збирките на лични податоци со висок ризик преку одбирање на понудените опции или пополнување на податоците за категорија или категории на субјектите на личните податоци, односно категории на личните податоци кои се однесуваат на нив.

(3) Отпечатеното конфирмациско писмо од ставот (2) на овој член, контролорот го пополнува, заверува со печат и потпишано од функционерот, или од одговорното лице го испраќа веднаш со препорачана пратка до Агенцијата.

(4) Ако контролорот е физичко лице, отпечатеното конфирмациско писмо од ставот (2) на овој член само го пополнува и своерачно потпишано го испраќа веднаш со препорачана пратка до Агенцијата.

Член 6

(1) Агенцијата врз основа на внесените податоци од страна на контролорот, како и врз основа на добиеното конфирмациско писмо, врши евидентирање на контролорот и на неговите збирки на лични податоци со висок ризик.

(2) Известувањето заради евидентирање од ставот (1) на овој член, контролорот го врши со цел демонстрирање на негова усогласеност со прописите за заштита на личните податоци (отчетност).

(3) Агенцијата при процесот на евидентирање на контролорот и на неговите збирки на лични податоци со висок ризик, врши верификација на точноста на податоците во однос на доставеното известување, како и проверка на неговата автентичност.

2. Пријавување на промени во евиденцијата на збирки на лични податоци со висок ризик

Член 7

(1) Контролорот за секоја промена во збирките на лични податоци со висок ризик, содржана во Известувањето, писмено ја известува Агенцијата во рок од 30 дена од денот на настанување на промената.

(2) По приемот на известувањето од ставот (1) на овој член, Агенцијата веднаш ги ажурира податоците содржани во евиденцијата на збирки на лични податоци со висок ризик.

Член 8

(1) Контролорот за секоја промена во делот на контролорот и на офицерот за заштита на личните податоци согласно прописите за заштита на личните податоци, веднаш писмено ја известува Агенцијата.

(2) По приемот на известувањето од ставот (1) на овој член, Агенцијата веднаш ги ажурира податоците содржани во евиденцијата на збирки на лични податоци со висок ризик.

Член 9

(1) Во случај на престанување на својството на контролор согласно прописите за заштита на личните податоци, контролорот писмено ја известува Агенцијата во рок од 15 дена од денот на престанување на својството контролор.

(2) По приемот на известувањето од ставот (1) на овој член, Агенцијата веднаш ги брише податоците на контролорот содржани во евиденцијата на збирки на лични податоци со висок ризик.

IV. ФОРМАТА И СОДРЖИНАТА НА ЕВИДЕНЦИЈАТА НА ЗБИРКИ НА ЛИЧНИ ПОДАТОЦИ СО ВИСОК РИЗИК

Член 10

(1) Во Агенцијата се води евиденција на збирки на лични податоци со висок ризик која ги содржи податоците од членот 2 на овој правилник.

(2) Евиденцијата од ставот (1) на овој член се води електронски преку систем за автоматска обработка на податоците.

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 11

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот за формата и содржината на образецот на Известувањето за обработка на личните податоци и за начинот на известувањето во Централниот регистар на збирки на лични податоци („Службен весник на Република Македонија“ бр. 155/08 и 158/10).

Член 12

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-609/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

Образец бр. 1 (дел 1)

Врз основа на член 71 став 1 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), _____,
назив на контролорот

Ви го доставувам следното

ИЗВЕСТУВАЊЕ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ СО ВИСОК РИЗИК

1.	**Податоци за контролорот – правно лице, орган на државната власт, државен орган, правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело**	
1.1	Назив	
1.2	Даночен број	
1.3	Шифра на дејност	
1.4	Организациска форма	
1.5	Општина	
1.6	Населено место	
1.7	Контакт-телефон	
1.8	Електронска пошта	
1.9	Факс	
1.10	Веб-страница	
1.11	Одговорно лице	
2.	**Офицер за заштита на личните податоци**	
2.1	Име и презиме	
2.2	Контакт-телефон	
2.3	Електронска пошта	
2.4	Работно место или број и датум на договор за ангажирање	
3.	**Овластен претставник (доколку го има)**	
3.1	Назив/име	
3.2	Седиште/адреса на живеење	
4.	**Назив на збирката на лични податоци со висок ризик**	
5.	Цел или цели на обработката;	
6.	Правна основа за воспоставување збирка на лични податоци	
7.	Опис на категориите на субјектите на личните податоци и на категориите на лични податоци кои се однесуваат на нив	
8.	Категориите на корисници на кои се, или ќе бидат откриени личните податоци, вклучувајќи корисници во трети земји или меѓународни организации	
9.	Рок на чување на личните податоци, односно предвидените рокови за бришење на различните категории на лични податоци	
10.	Пренос на личните податоци во трета земја или меѓународна организација	
11.	Општ опис на преземените технички и организациски мерки за обезбедување на безбедност на личните податоци	
12.	Број и датум на проценката на влијанието на заштитата на личните податоци	

_____, ____.____.202___ година
(место) (датум)

Образец бр. 2 (дел 2)

Врз основа на член 71 став 1 од Законот за заштита на личните податоци („Службен Весник на Република Северна Македонија“ бр. 42/20), _____,
(име и презиме на контролорот)

Ви го доставувам следното

ИЗВЕСТУВАЊЕ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ СО ВИСОК РИЗИК

1.	**Податоци за контролорот – физичко лице**	
1.1	Име и презиме	
1.2	Место и адреса на живеење	
1.3	Податоци за вработување (занимање или функција што ја врши)	
1.4	Датум на раѓање	
1.5	Место на раѓање	
1.6	Државјанство	
2.	**Назив на збирката на лични податоци**	
3.	Цел или цели на обработката	
4.	Правна основа за воспоставување збирка на лични податоци	
5.	Опис на категориите на субјектите на личните податоци и на категориите на лични податоци кои се однесуваат на нив	
6.	Категориите на корисници на кои се, или ќе бидат откриени личните податоци, вклучувајќи корисници во трети земји или меѓународни организации	
7.	Рок на чување на личните податоци, односно предвидените рокови за бришење на различните категории на лични податоци	
8.	Пренос на личните податоци во трета земја или меѓународна организација	
9.	Општ опис со кој ќе се овозможи првична оцена на соодветноста на преземените технички и организациски мерки за обезбедување на безбедност на личните податоци	
10.	Број и датум на проценката на влијанието на заштитата на личните податоци	

_____, ____.____.202___ година
(место) (датум)

1619.

Врз основа на член 39 став (4) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

Л И С Т А
НА ВИДОВИТЕ ОПЕРАЦИИ НА ОБРАБОТКА ЗА КОИ СЕ БАРА ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I.

1. Со оваа листа се воспоставуваат видовите операции на обработка, за кои се бара проценка на влијанието врз заштитата на личните податоци согласно Законот за заштита на личните податоци.

2. Во согласност со точка 1 на оваа листа, проценка на влијанието врз заштитата на личните податоци се бара во случај на:

1) обработка на лични податоци за систематско и сеопфатно профилирање или автоматско донесување одлуки со цел да се извлечат заклучоци и да се донесат одлуки кои произведуваат правно дејство, кои во голема мера влијаат на физичкото лице и/или на повеќе лица или кои помагаат при донесување на одлуки за нечиј пристап до услуга или некој вид на услуга или некоја погодност (на пр., како што се обработка на лични информации во врска со економски или финансиски статус, здравје, лични преференции, интереси, сигурност, однесување, податоци за локација, итн.);

2) обработка на посебни категории на лични податоци со цел профилирање или автоматско донесување на одлуки;

3) обработка на посебни категории на лични податоци, т.е. податоци што откриваат расно или етничко потекло, политичко мислење, религиозно или филозофско уверување или членство во синдикат, како и обработка на генетски податоци, биометриски податоци со цел единствено идентификување на лицата, здравствени податоци или податоци за сексуалниот живот или сексуалната ориентација на индивидуата;

4) обемна обработка на посебни категории на лични податоци или на лични податоци поврзани со казнените осуди и казнените дела (член 14 од Законот за заштита на личните податоци) или прекршочната одговорност;

5) обработка на лични податоци на деца со цел профилирање, автоматско одлучување или за цели на маркетинг или за директно понудување на услуги наменети за нив;

6) обработка на лични податоци собрани од трети страни (лица), кои се земаат во предвид за донесување на одлуки поврзани со склучување, раскинување, одбивање или продолжување на договори за давање на услуги на физички лица;

7) обработка на лични податоци со користење на систематско набљудување (мониторинг) на јавно достапен простор во големи размери;

8) употреба на нови технологии или технолошки решенија за обработка на лични податоци или со можност за обработка на лични податоци што служат за анализирање или предвидување на економската состојба, здравјето, личните желби или интереси, сигурноста или однесувањето, локацијата или движењето на физичките лица;

9) обработка на лични податоци преку поврзување, споредување или вршење на проверка на сличностите од повеќе извори;

10) обработка на лични податоци на начин кој што вклучува следење на локацијата или на однесувањето на физичкото лице во случај на систематска обработка на податоците за комуникација (метаподатоци) настанати – генерирани со употреба на телефон, интернет или други средства (канали) за комуникација, како што се GSM, GPS, Wi-Fi, за следење и обработка на податоците за локацијата;

11) обработка на лични податоци преку користење на уреди и технологии, кај кои што доколку настане инцидент може да го загрози здравјето на една личност или повеќе лица (субјекти на лични податоци); и

12) обработка на посебни категории на лични податоци на вработените кои се користат за единствена идентификација на вработените од страна на работода-

вачот и во други случаи на обработка на податоци за личности – вработени од страна на работодавачот преку користење апликација или систем за следење на нивната работа, движење и комуникација и слично. (на пр. обработка на лични податоци за следење на вршењето на работната обврска, движењето, комуникација и сл.).

II.

3. Агенцијата за заштита на личните податоци потенцира дека постоењето на Листа на видовите операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци, во никој случај не ја намалува општата обврска на контролорот за операциите на обработка да спроведе соодветна проценка на ризик и управување со ризикот. Понатаму, спроведувањето проценка на влијанието врз заштитата на личните податоци не ги ослободува контролорите кои обработуваат лични податоци од обврската да ги почитуваат и другите обврски предвидени во прописите за заштита на личните податоци. Исто така, оваа листа во никој случај не е рестриктивна (ограничувачка) или ексклузивна, бидејќи спроведувањето на проценка на влијанието врз заштитата на личните податоци секогаш е неопходно доколку се исполнети условите од член 39 став (1) од Законот за заштита на личните податоци.

Во тој контекст, Агенцијата за заштита на личните податоци укажува на фактот дека оваа листа подлежи на натамошен развој и може да биде изменета во согласност со дополнително идентификувани технологии или нови ризици од обработка на лични податоци. Проценката на влијанието врз заштитата на личните податоци задолжително мора да се изврши пред да се започне со обработка на лични податоци. Обврската за консултација со Агенцијата за заштита на личните податоци пред обработката постои само ако проценката на влијанието врз заштитата на личните податоци ќе покаже дека, доколку контролорот за обработка на лични податоци не преземе соодветни мерки за ублажување, односно намалување на ризикот, самата обработка на лични податоци ќе доведе до висок ризик, а според одредбите од членот 40 од Законот за заштита на личните податоци.

4. Контролорот е должен да изврши преиспитување за да процени дали обработката се врши во согласност со проценката на влијанието врз заштитата на личните податоци најмалку во случаите кога има промена на ризикот предизвикан од операциите на таа обработка.

5. Освен во случаите наведени во точка 2 дел I од оваа листа, контролорот е должен да изврши проценка на влијанието врз заштитата на личните податоци и во други случаи доколку постои веројатност дека некој вид обработка, особено со употреба на нови технологии и земајќи ја предвид природата, обемот, контекстот и целите на обработката, може да предизвика висок ризик за правата и слободите на физичките лица.

III.

6. Оваа листа влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-610/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

_____

1620.

Врз основа на член 39 став (5) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

Л И С Т А
НА ВИДОВИТЕ ОПЕРАЦИИ НА ОБРАБОТКА ЗА КОИ НЕ СЕ БАРА ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

I.

1. Со оваа листа се воспоставуваат видовите операции за обработка на лични податоци за кои не се бара проценка на влијанието врз заштитата на личните податоци согласно Законот за заштита на личните податоци.

2. Во согласност со точка 1 на оваа листа, проценка на влијанието врз заштитата на личните податоци не се бара за одредени видови на операции на обработка, особено кога:

- операциите за обработка не резултираат со висок ризик за правата и слободите на физичките лица;

- процесите (операциите) претходно биле утврдени дека не се изложени на ризик при извршената проценка на влијанието врз заштитата на личните податоци;

- обработката е веќе одобрена од Агенцијата за заштита на личните податоци;

- за обработката веќе има постоечка јасна и специфична правна основа во правниот систем на Република Северна Македонија и кога проценката на влијанието врз заштитата на личните податоци веќе е спроведена како дел од воспоставувањето на таа правна основа според членот 10 став (3) од Законот за заштита на личните податоци;

- е изведена како дел од проценката на влијанието што произлегува од основата на јавниот интерес и кога проценката на влијанието врз заштитата на личните податоци бил елемент на таа проценка според членот 10 став (3) од Законот за заштита на личните податоци; и/или

- Агенцијата за заштита на личните податоци ќе одлучи определена обработка да ја вброи (смета) како операција за обработка во согласност со членот 39 став (5) од Законот за заштита на личните податоци.

II.

3. Оваа листа влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-611/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

КОМОРА НА ИЗВРШИТЕЛИ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

1621.

Комората на извршители на Република Северна Македонија согласно член 74 став 2 од Законот за извршување („Службен весник на РМ“ бр. 72/16, 142/16, 233/18 и 14/20), го објавува следното

И З В Е С Т У В А Њ Е

Се известуваат граѓаните кои биле странки во предметите кои се водеа во канцеларијата на извршител Весна Кавракова од Куманово, дека предметите ги презема извршител Билјана Николовска од Куманово, именуван со Решение бр. 09-5589/1 од 30.12.2019 година на Министер за правда на РСМ за подрачје на Основен суд Куманово, Основен суд Крива Паланка и Основен суд Кратово.

Комората на извршители на РСМ известува дека извршител Билјана Николовска од Куманово започна со работа на ден 20.2.2020 година на адреса ул. „Ленинова“ бр. 20А/1-1.

Комора на извршители
на Република Северна Македонија
Претседател,
Зоран Димов, с.р.

Бр. 03-271/1
5 мај 2020 година
Скопје

ДРЖАВЕН ЗАВОД ЗА СТАТИСТИКА

1622.

Врз основа на член 44 став 1 од Законот за државната статистика „Службен весник на Република Македонија“ бр. 54/97, 21/07, 51/11, 104/13, 42/14, 192/15, 27/16, 83/18, 220/18 и „Службен весник на Република Северна Македонија“ бр. 31/20), Државниот завод за статистика го утврдува и објавува

ДВИЖЕЊЕТО НА ИНДЕКСОТ НА ЦЕНИТЕ НА МАЛО ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА ЗА МЕСЕЦ АПРИЛ 2020 ГОДИНА

Индексот на цените на мало во Република Северна Македонија во периодот јануари-април 2020 година во однос на просечните цени на мало во 2019 година изнесува -0.4%.

Директор,
Апостол Симовски, с.р.

СЛУЖБЕН ВЕСНИК
на Република Северна Македонија

www.slvesnik.com.mk contact@slvesnik.com.mk

Издавач: ЈП СЛУЖБЕН ВЕСНИК НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА, ц.о. – Скопје
бул. „Партизански одреди" бр. 29. Поштенски фах 51.
Директор и одговорен уредник – Мартин Костовски
телефон: +389-2-55 12 400
телефакс: +389-2-55 12 401

Претплатата за 2020 година изнесува 12.200,00 денари.
„Службен весник на Република Северна Македонија" излегува по потреба.
Рок за рекламации: 15 дена.
Жиро-сметка: 300000000188798.
Депонент на Комерцијална банка, АД – Скопје.

ISSN 0354-1622
2020122