Врз основа на член 21 став (1) точка 22 од Законот за спречување и заштита од дискриминација („Службен весник на Република Северна Македонија“ бр. 258/20), а во врска со член 28 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), Комисијата за спречување и заштита од дискириминација донесе

ПРАВИЛНИК
ЗА ПРОЦЕСОТ НА УПРАВУВАЊЕ СО СИСТЕМОТ НА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО КОМИСИЈАТА ЗА СПРЕЧУВАЊЕ И ЗАШТИТА ОД ДИСКРИМИНАЦИЈА

I. ОПШТИ ОДРЕДБИ

Предмет на уредување

Член 1

(1) Со овој Правилник се пропишува процесот за управување со системот за заштита на личните податоци во работењето на Државната комисија за спречување и заштита од дискриминација (во натамошниот текст: Комисијата).

(2) Комисијата врши оценка и ажурирање на техничките и организациските мерки утврдени со овој Правилник, при што секогаш ги применува оние мерки кои се соодветни на времето во кое се дизајнираат и имплементираат, а согласно најновите технолошки достигнувања.

Примена

Член 2

Овој Правилник се применуваат во сите случаи на обработка на личните податоци од страна на Комисијата, без разлика дали таа се јавува како контролор, обработувач, корисник или трето лице.

Лични податоци

Член 3

(1) Комисијата, во својата работа, врз основа на членот 5 од Законот за за спречување и заштита од дискриминација („Службен весник на Република Северна Македонија“ бр. 258/20), ги обработува следните лични податоци:

- раса,
- боја на кожа,
- потекло национална или етничка припадност,
- пол,
- род,

- сексуална ориентација,
- родов идентитет, п
- рипадност на маргинализирана група, ј
- јазик,
- државјанство,
- социјално потекло,
- образование,
- религија или верско уверување,
- политичко уверување,
- друго уверување,
- попреченост,
- возраст,
- семејна или брачна состојба,
- имотен статус,
- здравствена состојба,
- лично својство и општествен статус
- и други податоци кои можат да бидат основ за дискриминација.

(2) Заради извршување на своите законски надлежности поврзани со спречувањето на дискриминацијата утврдени со закон, Комисијата е корисник на личните податоци поврзани со утврдување на идентитетот на дискриминаторите и дискриминираните лица, како и другите учесници во постапките, а особено:

- име и презиме, ЕМБГ, адреса на живеалиште/претстојувалиште и други податоци потребни за идентификација на физичкото лице,
- назив, ЕДБ, ЕМБС, седиште и други податоци потребни за идентификација на правното лице.

(3) Во својата работа Комисијата ги воспоставува и работи со следните збирки на лични податоци:

- збирка на лични податоци поврзани со постапките и предметите за спрчеување и заштита од дискирминација во надлежност на Комисијата,
- збирка на лични податоци содржани во персоналните досијеа на членовите на Комисијата и вработените во Стручната служба и
- збирка на лични податоци поврзани со материјално финансиското работење на Комисијата.

(4) Личните податоци од ставот (1) на овој член кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето или податоци за сексуалниот живот или сексуалната

ориентација на физичкото лице, како посебни категории на лични податоци се обработуваат во секојдневната работа на Комисијата заради тоа што:

- обработката е неопходна за воспоставување, практикување или одбрана на правни барања на граѓаните;
- обработката е неопходна поради спречување и заштита од дискриминација, што претставува јавен интерес, а обработката е пропорционална на целта и почитување на суштината на правото на заштита на личните податоци, како и обезбедување соодветни и конкретни мерки за заштита на фундаменталните права и интереси на субјектот на личните податоци и
- обработката е неопходна за целите на управување со услугите и системите за социјална заштита, врз основа на закон.

Начин на обработка на личните податоци

Член 4

(1) Комисијата врши обработка на личните податоци на два начини и тоа:

- конвенционална обработка на лични податоци и
- дигитална обработка на личните податоци.

(2) Конвенционалната обработка на личните податоци опфаќа обработка на податоците во хартиена форма.

(3) Дигиталната обработка на личните податоци е обработка преку користење софтверски решенија, без оглед дали дигиталните податоци се наоѓаат на хардвер кој физички се наоѓа во простории на Комисијата или во облак (cloud), хостиран кај некој давател на услуги со кој Комисијата склучила договор за услуги согласно постоечката законска регулатива во државата.

Евиденција на операциите на обработка на личните податоци

Член 5

(1) Комисијата води евиденција на операциите за обработка на лични податоци, при водење на постапките од своја надлежност. Оваа евиденција, особено ги содржи следните информации:

- името и презимето и контакт податоци Претседателот на Комисијата и на офицерот за заштита на личните податоци;
- целите на обработката на личните податоци;
- опис субјектите чии личните податоци се обработуваат, како и на категориите на личните податоци.

- категориите на корисници на кои Комисијата при својата работа ги открива или ќе ги открие личните податоци, вклучувајќи корисници во трети земји или меѓународни организации;
- преносот на лични податоци во трета земја или меѓународна организација, вклучувајќи идентификација на таа трета земја или меѓународна организација, документација за соодветни заштитни мерки;
- предвидените рокови за бришење на различните категории на лични податоци;
- и општ опис на техничките и организациските мерки за безбедност.

(2) Евиденцијата од ставот (1) на овој член се води во електронска форма (excel табела) и истата тековно се ажурира.

Офицер за заштита на личните податоци

Член 6

(1) Комисијата определува најмалку еден административен службеник, вработен во Стручната служба на Комисијата, кое ќе биде офицер за заштита на лични податоци во Комисијата.

(2) Офицерот за заштита на личните податоци ги врши следните работи:

- ги информира и советува членовите на Комисијата и вработените во Стручната служба кои вршат обработка соодветно на нивните обврски според одредбите од овој закон;
- (б) ја следи усогласеноста со овој закон, со други засегнати закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на Комисијата во однос на заштитата на личните податоци, вклучувајќи распределување на одговорности, подигнување на свеста и обучување на членовите на Комисијата и вработените кои што учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци;
- каде што е потребно, дава совети во однос на проценатa на влијанието на заштитата на личните податоци и го следи извршувањето на проценатa;
- соработува со Агенцијата за заштита на личните податоци;
- дејствува како контакт точка за Агенцијата за заштита на личните податоци во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација, како и советување според потребите за сите други прашања.

Информирање и едуцирање за заштитата на личните податоци

Член 7

(1) Членовите, лицата кои се вработуваат или се ангажираат во Комисијата, 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 со договор се ангажираат за извршување на работа во Комисијата во договорот за нивното ангажирање се наведуваат обврските и одговорностите за заштита на личните податоци.

(3) Комисијата пред непосредното започнување со работа на новоименуваните членови, вработените и ангажираните лица, дополнително ги информира за непосредните обврски и одговорности за заштита на личните податоци.

(4) Членовите, лицата кои се вработуваат или се ангажираат во Комисијата, 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 Комисијата, 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 членовите, лицата кои се вработуваат или се ангажираат во Комисијата.

(7) Изјавата од ставот (4) на овој член е дадено во Прилог 2 кој е составен дел на овој Правилник.

Овластување и изјава за обработка на лични податоци

Член 8

(1) Членовите на Комисијата и вработените во Стручната служба вршат обработка на личните податоци врз основа на дадено овластување од страна на Комисијата, и е должно да постапува согласно законските и подзаконските акти кои ја регулираат заштитата на личните податоци, како и согласно упатствата дадени од Комисијата, и содржани во внатрешните политики и правила.

(2) Овластувањето од ставот (1) на овој член е дадено во Прилог 1 кој е составен дел на овој Правилник.

II. БЕЗБЕДНОСТ НА ПРОЦЕСОТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

II.1. ЗАЕДНИЧКИ ПРАВИЛА

Систем за заштита на личните податоци

Член 9

(1) Комисијата воспоставува систем на 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;
- обезбедување на континуирана доверливост, интегритет, достапност и отпорност на документите и електронските системи кои содржат лични податоци;
- способност за навремен поврат и достапноста на личните податоци и пристапот до нив во случај на физички или технички инцидент; и
- редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката на личните податоци.

(3) Процесот за управување со системот за заштита на личните податоци е дефиниран во Политиката за системот за заштита на личните податоци која ја утврдува Комисијата.

(4) Комисијата редовно ја ажурира и ревидира Политиката од ставот (34) на овој член и ја усогласува истата со промените во секојдневното работење.

Управување со ризик

Член 10

(1) Комисијата при утврдување и процена на ризикот 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:

- список (преглед) на сите процеси со кои се врши обработка на лични податоци;
- процена на ризиците за секој процес на обработка на лични податоци;

- спроведување и проверка на планираните мерки; и
- спроведување на периодични безбедносни проверки.

(3) Списокот на процеси со кои се врши обработка на личните податоци од став (2) алинеја 1 на овој член, без оглед дали се работи за конвенционална или дигитална обработка на личните податоци треба најмалку да ги опфати:

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

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

- 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.

- Идентификување на изворите на ризик кој што може да биде причина за секој непосакуван настан (субјективни причини - човечки фактор или објективни причини- пожар, поплава, сл.).
- 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.).

- 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).
- 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).

Нивоа на мерки за безбедност на обработката на личните податоци

Член 11

(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, Комисијата спроведува две нивоа на техничките и организациските мерки, и тоа:

- стандардно и
- високо.

Ангажирање на други субјекти кои ќе обработуваат лични податоци

Член 12

(1) Во случај кога Комисијата ќе одлучи да пренесе работи од нејзиниот делокруг на работа поврзани со обработка на лични податоци на други физички или правни лица, должна е да се осигура дека личните податоци ќе се обработуваат под нејзин 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, Комисијата може да пренесе работи од свој делокруг само доколку ангажираното правно или физичко лице 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 Комисијата и ангажираниот субјект мора да бидат уредени со посебен договор или во рамки на договорот со кој се ангажира субјектот за определан услуга, при што Комисијата пред да го склучи договорот е должна да побара од ангажираниот субјект, 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 Комисијата.

(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 Комисијата 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 Комисијата; и
- другите обврски и одговорности согласно со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

Анонимизирање и псевдонимизирање на личните податоци

Член 13

(1) Заради заштита на личните податоци и спречување на нивната злоупотреба, при објавување на одлуките на Комисијата се користат следниве два методи на заштита на личните податоци:

- анонимизација - целосно отстранување на сите лични податоци, а по барање на странка во постапка, и податоците за настаните и доказите и изјавите презентирани во постапката пред Комисијата кои би можеле да го откријат идентитетот на лицето и
- псевдонимизација - замена на личните податоци на таков начин што тие повеќе не можат да се поврзат со одредено лице (субјект на лични податоци) без употреба на дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски

мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува.

(2) Минималниот стандард за анонимизација и псевдонимизацијата на личните податоци во одлуката на Комисијата подразбира изоставување, односно замена на податоци врз основа на кои е можно да се идентификува странката во постапката пред Комисијата или со него поврзано лице врз основа на чији лични податоци би можел да биде откорен идентитетот на странката.

(3) Во одлуката на Комисијата се анонимизираат следниве податоци за странката учесниците во постапката:

- Име и презиме, датум, година и место на раѓање, адреса (живеалиште или престојувалиште), единствен матичен број (ЕМБГ), број на лична карта, пасош, возачка дозвола, регистарски таблички на возила или други лични документи и онлајн податоци кои би можеле да доведат до откривање на идентитетот, биометриски податоци, генетски податоци, здравствени податоци и други лични податоци за физички лица кои самостојно или во комбинација со други лични податоци го идентификуваат физичкото лице.
- Називот и седиштето на правните лице, единствен даночен број, банкарска сметка, е-пошта, веб страна, телефонски број и други податоци кои самостојно или во комбинација со други лични податоци го идентификуваат правното лице.

II.1. КОНВЕНЦИОНАЛНА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

II.1.1. СТАНДАРДНО НИВО ТЕХНИЧКИ И ОПЕРАТИВНИ МЕРКИ ЗА КОНВЕНЦИОНАЛНА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Пристап до документите

Член 14

(1) Пристапот до документите кои содржат лични податоци треба биде ограничен само за лица кои дале изјава и имаат овластување за обработка на лични податоци .

(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 што содржат лични податоци, Комисијата треба да обезбеди изјава и да даде овластување за обработка на личните податоци.

Правило „чисто биро“

Член 15

Членовите, вработените и ангажираните лица во Комисијата задолжително го применува правилото „чисто биро“, односно забрана за било какво отворено и незаштитено изложување и пристап на неовластени лица до документи кои содржат лични податоци, за време на целиот процес на обработка.

Чување на документи

Член 16

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

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, Комисијата 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 Комисијата треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

(4) 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.

(5) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (4) на овој член, Комисијата треба да примени други мерки за да се спречи секој неовластен пристап до документите.

Архивирање на документи

Член 17

(1) Комисијата, 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, Комисијата 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. За таа цел Комисијата,

согласно Законот за архивски материјал („Службен весник на Република Македонија“ бр. 95/12, 41/14, 72/15, 148/15, 169/15, 53/16 и 11/18) и Уредбата за канцелариско и архивско работење (“Службен весник на Република Македонија” бр. 1/14), еднаш годишно донесува:

- -План на архивските знаци на Комисијата;
- -Листа на документарен материјал со рокови за негово чување и
- -Листа на архивски материјал на Комисијата.

(3) Комисијата води „Список (преглед) со рокови на чување на личните податоци“ во кој ќе бидат содржани информации за моментот на активирање рокот за чување на личните податоци, должината на роковите за чување на личните податоци, причините за чување на личните податоци, законскиот основ за чување на личните податоци и сопственикот на податоците.

(4) Овој список Комисијата го ревидира и усогласува годишно, односно согласно промените во работењето и законските услови за чување на личните податоци.

Уништување на документи

Член 18

(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.

II. 1.2. ВИСОКО НИВО ТЕХНИЧКИ И ОПЕРАТИВНИ МЕРКИ ЗА КОНВЕНЦИОНАЛНА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Дополнителни мерки

Член 19

(1) Комисијата врз основа на анализата на ризикот може да воведе и примени дополнителни мерки за безбедност на личните податоци со кои ќе демонстрира дополнителна усогласеност со прописите и добрите практики за заштита на личните податоци.

(2) Комисијката на доброволна основа, може да изврши и проверка на процесите и интерните документи за заштита на личните податоци заради сертификација на процесите преку кои конвенционално 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 за заштита на личните податоци или од сертификациони тела согласно прописите за заштита на личните податоци.

Копирање и умножување на докумнети

Член 20

(1) Копирањето или умножувањето на документите може да се врши единствено од страна на лица овластени за тоа од страна на Комисијата.

(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 21

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

(2) При изнесување на документите, заради вршење на увид, заради нивна обработка и решавање на предметите или заради други оправдани причини, членовите и вработените на Комисијата мора да ги преземат сите мерки за нивна физичка безбедност, не смеат да ги оставаат необезбедени ниту да дозволат пристап до нив од страна на неовластени лица.

II.2. ДИГИТАЛНА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

II.2.1. СТАНДАРДНО НИВО НА ТЕХНИЧКИ И ОПЕРАТИВНИ МЕРКИ ЗА ДИГИТАЛНА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Автентикација на овластените лица

Член 22

(1) Комисијата 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 Комисијата 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, Комисијата 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) Комисијата задолжително води евиденција за овластените лица кои имаат авторизиран пристап до документите во 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, Комисијата 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 23

(1) Комисијата е должна да обезбеди примена на една или повеќе од следните технички мерки со кои се обезбедува опремата на која се врши обработка на личните податоци:

- автоматизирано одјавување од информацискиот систем после изминување на определен период на неактивност (не подолго од 15 минути). За повторно активирање на системот, Комисијата треба да обезбеди дека овластените лица пристапуваат со примена на повторна автентификација
- во случај на три последователни неуспешни обиди за најавување на информацискиот систем, треба да се обезбеди автоматизирано отфрлање на лицето кое се најавува од информацискиот систем.
- инсталиран заштитен ѕид (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 Комисијата;
- редовно ажуриран антивирусен софтвер и редовни ажурирања на софтверските програми;

- конфигурирани софтверски програми така што безбедносните ажурирања да се вршат автоматски;
- зачувување на податоците на корисниците на серверите на Комисијата 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, Комисјата може да применува една или повеќе од 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 Комисијата, со цел откривање дали се загрозени и други елементи;
- безбедносен надзор на софтверот и хардверот што се користи во системот на Комисијата, вклучувајќи и редовно следење на тимот за брза реакција (MKDCIRT) 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 Комисијата.

Сегрегација на должности и одговорности

Член 24

(1) Комисијата 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) Комисијата обезбедува повлекување на правата на пристап веднаш по престанокот на овластувањата за пристап.

(3) Комисијата 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 ендаш квартално.

Контрола на пристап до информацискиот систем

Член 25

(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) Комисијата воспоставува механизми за да се оневозможи пристап на овластените лица до личните податоци и информатичко комуникациската опрема кои не се опфатени со нивното овлстување.

(3) Администраторот на информацискиот систем кој е овластен од комисијата, ги доделува, менува или одзема привилегиите на авторизираниот пристап до личните податоци и информатичко комуникациската опрема само во рамките на овластувањата кои ги дала Комисјата.

Обезбедување евиденција за секој пристап (logs)

Член 26

(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, Комисијата 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 Комисијата 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, Комисијата 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) Комисијата ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем.

(8) Комисијата 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) Комисијата 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) Комисијата 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) Комисијата 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 27

(1) Комисијата применува соодветни технички мерки за спречување на кражба или друг начин на загуба на преносливите медиуми (мобилна опрема) на кои се врши обработка на личните податоци.

(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) 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, Комисијата 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.

Заштита на внатрешната мрежа

Член 28

(1) Комисијата 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.

(2) Комисијата 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 29

(1) Комисијата согласно анализата на ризик е должна 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 Комисијата 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, Комисијата може да 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 Комисијата

Член 30

(1) Комисијата треба да примени технички мерки со кои ќе го гарантира точниот идентитет на својата Веб страница (pharming prevention), како и доверливоста на информациите што ги испраќа или ги собира преку веб-страницата, и тоа преку примена на една или повеќе од следните мерки:

- имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на Комисијата (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, Комисијата обезбедува претходна согласност од интернет корисникот откако ќе го извести корисникот, а пред да се депонира колачето.

(2) Комисијата во однос на својата 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:

- не треба да пренесува лични податоци преку URL без примена на протокол за криптирање (на пример идентификатори или лозинки);
- не треба да користи небезбедни услуги;
- не треба да употребува сервери кои хостираат бази на податоци или сервери како работни станици, особено не за пребарување на веб-страници, пристап до електронски пораци и слично;
- не треба да ги поставува базите на податоци на сервери кои се директно достапни преку интернет; и
- не смее да споделува кориснички сметки (user accounts) помеѓу две или повеќе овластени лица.

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

Член 31

(1) Комисијата 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) Офицерот за заштита на лични податоци при Комисијата 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) Комисијата 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 32

(1) Секое овластено лице е должно веднаш да го пријави на администраторот на информацискиот систем секој инцидент што ќе настане во процесот на обработување на личните податоци.

(2) Пријавувањето на инцидентот од став 1 на овој член се врши во електронска форма, а доколку тоа не е возможно, пријавувањето се врши во писмена форма, при што се наведуваат следните податоци за инцидентот:

- време на настанување на инцидентот;
- траење и престанок на инцидентот;
- место во информацискиот систем каде се појавил инцидентот;
- податок или проценка за обемот, односно опсегот на инцидентот;
- име и презиме на овластеното лице кое го пријавило инцидентот;
- име и презиме на овластените лица до кои е доставена пријавата за инцидентот.

(3) По приемот на пријавата за инцидент, администраторот на информацискиот систем веднаш започнува да врши проценка на причините за појавување на инцидентот, како и за тоа дали и кои мерки треба да се преземат за негово санирање и за спречување на негово повторување во иднина. Доколку се работи за инцидент кој се повторува, администраторот на информацискиот систем е должен да преземе мерки кои ќе гарантираат трајно отстранување на ризикот од негово повторување.

(4) Доколку како последица на инцидент дојде до губење или бришење на дел или сите лични податоци содржани во информацискиот систем, истите ќе бидат повторно внесени – вратени во информацискиот систем, со користење на сигурносните копии кои што се чуваат во Комисијата.

(5) Постапката од став (5) на овој член ќе се примени и доколку бришењето или губењето на дел или сите лични податоци содржани во информацискиот систем е неопходно заради отстранување на последиците од инцидентот или за преземање на мерки за спречување на негово повторување во иднина.

(6) При повторното внесување – враќање на личните податоци во информацискиот систем, задолжително и во електронска форма се врши евидентирање на овластените лица кои ги извршиле операциите за повторно враќање на податоците, категориите на лични податоци кои биле вратени и кои биле рачно внесени при враќањето. Повторното враќање на личните податоци во информацискиот систем се врши од страна на овластените лица/администратор на информацискиот систем врз основа на претходно издадено писмено овластување од страна на Комисијата.

(7) Во случај на нарушување на безбедноста на личните податоци, за кое постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, Комисијата ја известува Агенцијата за заштита на личните податоци за нарушувањето на безбедноста на личните податоци, веднаш или најдоцна во рок од 72 часа откако се дознало за нарушувањето.

(8) Известувањето за нарушување на безбедноста на личните податоци, кое е достапно на https://dzlp.mk/mk/content/%D0%BE%D0%B1%D1%80%D0%B0%D1%81%D1%86%D0%B8 се доставува на е-маил адресата: incident@privacy.mk или а https://eprijavi.privacy.mk.

(9) Во случај на нарушување на безбедноста на личните податоци, за кое постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, Комисијата веднаш го известува субјектот на личните податоци за нарушувањето на безбедноста на личните податоци. Образецот на ова известување исто така е достапен на веб страната на Агенцијата за заштита на личните податоци на горенаведениот линк.

(10) Известувањето до субјектот на личните податоци од ставот (1) на овој член, не е задолжително, доколку е исполнет еден од следните услови:

- Комисијата применила соодветни технички и организациски мерки за заштита и тие мерки биле применети во однос на личните податоци засегнати од нарушувањето на безбедноста на личните податоци, особено мерки кои што ги прават личните податоци неразбирливи за секое лице кое нема овластување за пристап до нив, како што е криптирањето;
- Комисијата применила дополнителни мерки кои гарантираат дека веќе не постои веројатност за појавување на висок ризик за правата и слободите на субјектите на личните податоци од ставот (1) на овој член;
- ако известувањето бара несразмерен напор. Во таков случај, се врши јавно известување или се применува друга слична мерка со која субјектите на личните податоци ќе бидат подеднакво информирани на ефикасен начин.

(11) Комисијата детално го документира нарушувањето на безбедноста на личните податоци и воспоставува 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.

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

Член 33

(1) Комисијата 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) Комисијата 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, Комисијата 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.

(3) Комисијата задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци.

(4) Комисијата 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).

Криптирање на личните податоци

Член 34

Кога Комисијата 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.

Физичка безбедност

Член 35

(1) Комисијата 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 Комисијата 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 Комисијата 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 Комисијата.

(3) Во случајот од ставот (2) на овој член, меѓусебните права и обврски на Комисијата 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 36

(1) Во документацијата за технички и организациски мерки, 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 Комисијата со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

(2) Информацискиот систем и информатичката инфраструктура на Комисијата 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.

II.2.2. ВИСОКО НИВО НА ТЕХНИЧКИ И ОПЕРАТИВНИ МЕРКИ ЗА ДИГИТАЛНА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Дополнителни мерки

Член 37

(1) Комисијата 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.

(2) Комисијата 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.

(3) Комисијата 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).

(4) За пренесените медиуми надвор од работните простории на Комисијата, треба да бидат преземени неопходни мерки за да се спречи неовластено обработување на личните податоци снимени на нив.Тестирање на информацискиот систем

(5) Комисијата 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.

(6) Тестирањето од став (5) на овој член се врши преку обработка на документи кои содржат имагинарни лични податоци.

(7) Комисијата 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.

(8) Медиумите можат да се пренесуваат надвор од работните простории на Комисијата 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.

III. ЗАВРШНИ ОДРЕДБИ

Влегување во сила

Член 38

Овој правилник влегува во сила со денот на неговото донесување.

Број 01-208/1
06-04-2022 година
Скопје

Претседател на
Комисија за спречување и заштита од дискриминација,

Прилог 1

Овластување за обработка на лични податоци

Врз основа на член 33 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр.40/20), Комисијата за спречување и заштита од дискриминација на седницата одржана на _____ година, донесе

ОВЛАСТУВАЊЕ
за обработка на лични податоци
во Комисијата за спречување и заштита од дискриминација

(1) Се овластува _____, _____, во Одделение _____, Сектор_____, да врши обработка на личните податоци содржани во _____.

(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 упатствата добиени од Комсијата за спречување и заштита од дискриминација;
- ги почитува техничките и организациските мерки за обезбедување безбедностна личните податоци кои ќе ги дознае при работата во Комисијата за спречување и заштита од дискриминација; и
- ги чува како доверливи личните податоци, како и мерките за нивна заштита.

(3) Обемот на овластувањето за пристап до личните податоци е: _____ (*да се опшите обемот на овластување (на пример, да внесува лични податоци, да брише, да корегира, 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 начини*)

(5) Рокот на важење на ова овластување е за време додека е на работното место _____ (*работното место на кое е распоредено лицето*) во Комисијата за спречување и заштита од дискриминација.

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

Претседател на Комисијата,

_____

Прилог 2

Изјава за тајност и заштита на обработката на личните податоци

Врз основа на член 31 став (4) од Правилникот за безбедност на обработката на личните податоци („Службен Весник на Република Северна Македонија" бр. 122/20), а во врска со член 31 став (4) од Правилникот за безбедност на обработката на личните податоци во Комисијата за спречување и заштита од дискриминација бр._____ од _____ година, ја давам следната

И З Ј А В А
за тајност и заштита на обработката на
личните податоци

Јас долупотпишаниот/ата, _____, распореден/на на работното место _____ во _____, во согласност со Правилникот за безбедност на обработката на личните податоци и Правилникот за безбедност на обработката на личните податоци во Комисијата за спречување и заштита од дискриминација, се обврзувам дека:

- ќе ги почитувам начелатаа поврзани со обработката на личните податоци;
- ќе ги применувам техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот и ќе ги чувам како доверливи личните податоци, како и мерките за нивна заштита;
- ќе вршам обработка на личните податоци согласно упатствата добиени од Комисијата за спречување и заштита од дискриминација.

Потпис,

_____