Република Северна Македонија

Министерство за јавна администрација

Врз основа на член 28 од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија" бр. 42/20, 294/21 и 101/25) и Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија", бр. 122/2020), Министерот за јавна администрација, ја донесе следната

АНАЛИЗА НА РИЗИК НА АКТИВНОСТИТЕ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ ВО МИНИСТЕРСТВОТО ЗА ЈАВНА АДМИНИСТРАЦИЈА

1. Опфат и цел

Со оваа Анализа се опфатени безбедносните ризици во однос на активностите во врска со обработката на личните податоци и утврдени се насоките за спроведување на клучните безбедносни мерки и контроли во сите процеси и активности на информацискиот систем на Министерството за јавна администрација (во натамошниот текст: министерството). Наведените се однесуваат и на обработувачот со цел спречување на настанување на безбедносни инциденти, како и намалување на ранливоста на информацискиот систем

„Работнатата карта" на оперативни системи, апликации и процеси на коишто се врши обработка на личните податоци, е претставена со табеларен приказ на:

- евентуални грешки при работењето;
- потенцијални напади на информацискиот систем; и
- настани што се случуваат како последица на виша сила (vis major).

Оперативни системи	
Софтвери	
Платформи	
Евентуални грешки при работењето	Оштетување на работна единица, губење на работна единица итн.
Потенцијални напади на информацискиот систем	
Настани што се случуваат како последица на виша сила (vis major)	Елементарни непогоди

2. Фази на анализата

2.1.1. Идентификација

Авторизиран пристап
Администратор на информацискиот систем
Контрола на пристап
Работна единица (комппјутер, лаптоп)
Медиум
Корисничко име и лозинка
Сигурносна копија (backup)

Оперативен систем	
Софтвери	
Платформи	www.mja.gov.mk

2.1.2. Проценка

Оперативен систем	Застарување на системот
Внатрешна мрежа	Физички или технички оштетувања
Алатки	Необновување на лиценци
Процеси	Малвери сомнителни програми
Сервери	Ракување од нестручни лица

Проценка на веројатноста заканата се материјализира, односно остварuva како: ниска, средна и висока.

Ниска	**Средна**	**Висока**
Грешка при ракувањето	Заразен софтвер или хардвер	Злоупотреба на службените овластувањата

Преоптовареност на работната станица(компјутер, лаптоп)	Key logger	Кражба на лаптоп, усб стик
Гео-локација на серверите	Оштетување на работните единици (компјутер, лаптоп)	Упад во системот од овластени соработници
Пад на електричната енергија		Вода, пожар,
		Надворешен упад, конкурент итн.

Анализа на влијанието на заканата која го има врз безбедноста на личиите податоци – ниско, средно и високо:

Ниско	**средно**	**високо**
Техничка грешка	Вирус	Упад во системот

Оценка на ризикот, односно нивото на ризик, како добиена вредност (множење од вредноста на проценетата веројатност и сериозноста на влијаиетот врз безбедоснста на личните податоци

Во случајот на горенаведените единствена превенција е чување на резервна копија (backup).

2.1.3. Спроведување и проверка на безбедносните мерки и контроли за секој идентификуван ризик

При изготвувањето н аоваа Анализа е земено во предвид дека министерството во рамките на својот делокруг на работење, а со цел извршување на својата основна дејност во доменот на прибирање, обработка, одржување, управување, користење, дистрибуција, издавање и единствен пристап кон податоците, врши собирање, чување и обработка на лични податоци, во единствен информациски систем и информациска структура.

Системот за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци во министерството се состои од следните формално-правни механизми имплементирани со донесување и изготвивање на соодветни акти:

1. Донесување на План за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци;
2. Донесување на Процедура за технички и организациски мерки за обезбедување на безбедност и заштита на обработката на личните податоци;

3. Донесување на Процедура за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица;
4. Донесување на Процедура за пријавување, реакција и санирање на инциденти;
5. Донесување на Процедура за правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
6. Донесување на Процедура за правото на исправка на личните податоци од страна на субјектите на личните податоци.
7. Донесување на Процедура за начинот на уништување на документите, бришење и чистење на медиумите;
8. Донесување на Процедура за начинот на вршење на видеонадзор во министерството;
9. Изготвување на Анализа на целите за кои се поставува видеонадзорот во министерството;
10. Донесување на Методологија влијанието на заштитата на личните податоци;
11. Изготвување на Анализа на ризик на активностите за обработка на личните податоци;
12. Донесување на Политика со опис на техничките и организациските мерки на информацискиот систем и информатичката инфраструктура;
13. Изготвување на Преглед на порти на заштитниот ѕид (firewall);
14. Донесување на внатрешни акти и посебни овластувања за обработка на личните податоци со коишто се утврдени правата, обврските и одговорностите на сите кои имаат пристап до информацискиот систем на Министерството за јавна администрација на којшто се врши обработката на личните податоци; и
15. Донесување и изготвување и на други акти поврзани со заштитата и безбедноста на личните податоци.

2.1.4. Превенција и одржување

Во министерството е воспоставен континуиран процес на донесувањето на внатрешни акти и посебни овластувања за обработка на личните податоци со коишто се утврдени правата, обврските и одговорностите на сите кои имаат пристап до информацискиот систем на министерството на којшто се врши обработката на личните податоци

Евиденциите на активностите за обработка на личните податоци со рокови за чување утврдени согласно прописите за архивско работење и се табеларно прикажани во посебен

Преглед што е во прилог и е составен дел од Политиката за воспоставување на систем за заштита на личните податоци во министерството.

Во случајот на горенаведените единствена превенција е чување на резервна копија (backup)

3. Ревизија на анализата

Ревизијата на оваа Анализа е потребно да се врши по потреба, а задолжително во случај кога се менуваат актите за организација и систематизација на работните места во министерството.

4. Завршна одредба

Оваа Анализа влегува во сила и ќе се применува со денот на нејзиното донесување.

Министер за јавна администрација
Горан Минчев