Образец бр. 1

АНАЛИЗА НА ЦЕЛТА, ОДНОСНО ЦЕЛИТЕ ЗА КОЈА/КОИСЕ ПОСТАВУВА ВИДЕОНАДЗОРОТ ВО БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ, СКОПЈЕ

I.

1.	Датум (период) кога е вршена анализата	21-28.06.2021 год. 28.06.2021 год
2.	Законски основ, односно цел или цели во согласност со одредбите од член 90став (1) од Законот за заштита на личните податоци заради кои се воспоставува видеонадзорот	- заштита на сопственоста, - обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории само за безбедносни цели.
3.	Дали поставувањето на видеонадзор еобврска согласно друг закон (со образложение)	Не,само Законот за заптита на личните податоци
4.	Опис на недвижните и движните ствари, односно простор кои ќе сезаштитуваат со поставувањето навидеонадзорот	- Компјутерска опрема, преносливи медиуми,, шкафови, намештај, документации, и сите останати материјали и објекти во просториите и дел дворот на Академијата;
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 зарадикои се имплементира систем за вршење на видеонадзор	- За поставениот Алармен систем - има потреба од време дури да се интервенира во момент на опасност што е ризик за безбедноста; - поради тоа е потребно дополнително обезбедување;
6.	Категории на субјекти на лични податоци кои ќе се снимаат	- Вработените во Факултетот, - студенти и - посетители и странки на факултетот.
7.	Дали со видеонадзорот ќе се обработуваат лични податоци на деца	Не

8.	Категории на лични податоци кои ќе се обработуваат преку системот за видеонадзор	Контролорот собира само слики фатени на камерите, при што не се врши тонско снимање.
9.	Начин за информирање дека се врши видеонадзор на различните категориина субјекти на лични податоци кои ќе бидат опфатени со видеонадзорот (пр.посебно информирање на вработените, истакнување на известување за видеонадзор...)	- Истакнување на Известување за видео надзор, на влезот на факултетот.
10.	Начин за остварување на правата на субјектите на лични податоци	Со испраќање на барање до Бизнис Академија Смилевски Скопје
11.	Начин на доделување на привилегииза пристап до видеонадзор	Факултетот/деканот овластува лице за пристап до личните податоци и само овластеното лице за видео надзор има право на пристап до личните податоци.
12.	Период за кој ќе биде поставен видеонадзор (неопределен период/определен период)	Неопределен период
13.	Временски период во кој биде активен видеонадзорот (24/7, по завршување на работното време и сл.)	24/7 часа
14.	Дали преку видеонадзорот ќе се обработуваат лични податоци само вореално време (мониторирање) или ќе се врши и снимање	ќе се врши и снимање
15.	Период на чување на снимките соодветен на целта/целите заради која/кои се поставува видеонадзорот	30 дена
16.	Кој ќе има пристап до видеонадзорот (лица вработени во контролорот, односно обработувачот) и број на лицакои ќе имаат пристап до видеонадзорот	Лица вработени во контролорот, односно обработувачот (овластеното лице), 1 лице.
17.	Информации за предвидена обука зазаштита на личните податоци за лицата кои ќе имаат пристап до видеонадзорот	Предвидена обука од страна на Офицерот за заштита на личните податоци.
18.	Примена на мерки за техничка и интегрирана заштита на личните податоци (Data protection by design andby default)	Не
19.	Оценка на нивото на технички и организациски мерки кои треба да се применат	Стандардно ниво на технички и организациски мерки

20.	Проценка за број на потребни камерикои ќе се постават	4 камери
21.	Тип/вид на камери (подвижни, статични, резолуција, опција за зумирање, ноќно снимање...)	Камерите за видеонадзор се инсталираат на DVR снимач со хард диск и обезбедуваат максимална резолуција на снимање од 640X480 пиксели со среден квалитет на слика; Опција за ноќно снимање.
22.	Доколку повеќе контролори заедничкивршат видеонадзор (заеднички контролори), тогаш се утврдуваат целите и начините на обработка прекусистемот за видеонадзор, како и податоци за начинот на кој што е уреден нивниот меѓусебен однос (например: со договор, закон којшто сепримену ва на тие контролори, итн.)	Само еден контролор
23.	Период до кога ќе се донесе акт во којшто ќе се уреди начинот на вршење навидеонадзорот	До 30,05,2022
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

2. Оценка/мислење од офицерот за заштита на личните податоци
   Офицерот го поддржува Поставувањето на видеонадзорот.
4. Име, презиме и потпис на лицата кои ја вршеле анализата на целта односно целите заради кои се воспоставува системот за вршење на видеонадзор

Име	Презиме	
Име	Презиме	
Име	Презиме	
Име	Презиме	
Име	Презиме	

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

Билјана	Галовска	

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...):

   Контролорот/Факултетот одлучува да се постави видеонадзорот.

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

Маја	Кузмановска	

АНАЛИЗА НА ЦЕЛТА, ОДНОСНО ЦЕЛИТЕ ЗА КОЈА/КОИ СЕ ПОСТАВУВА ВИДЕОНАДЗОРОТ ВО
Бизнис Академија Смилевски

I.

1.	Датум (период) кога е вршена анализата	Кликнете на стрелката за да го внесете датумот.
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	☒ 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 само за безбедносни цели.
3.	Дали поставувањето на видеонадзор е обврска согласно друг закон (со образложение)	не
4.	Опис на недвижните и движните ствари, односно простор кои ќе се заштитуваат со поставувањето на видеонадзорот	Службениот влез за во Академијата и ходниците во нејзината внатрешност
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	Безбедност на сите субјекти вработени и студенти како и надворешни лица
6.	Категории на субјекти на лични податоци кои ќе се снимаат	Во објектот во кој постои видео надзор не се снимаат збирки со лични податоци, тие се кластираат привремено и се пуштаат во дирекцијата во Скопје каде се стават во соодветни збирки

7.	Дали со видеонадзорот ќе се обработуваат лични податоци на деца	не
8.	Категории на лични податоци кои ќе се обработуваат преку системот за видеонадзор	Идентитет на личност по потреба (нарушување на редот и мирот во институцијата и објкетот кога е затворен како и дејствија кои се казнуваат со закон)
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...)	За вработени информирање од ОЗЛП, за надворешни лица обележување на објектот со лепенки
10.	Начин за остварување на правата на субјектите на лични податоци	Потпишување на изјава
11.	Начин на доделување на привилегии за пристап до видеонадзор	Овластување од контролорот
12.	Период за кој ќе биде поставен видеонадзор (неопределен период/определен период)	неопределен
13.	Временски период во кој биде активен видеонадзорот (24/7, по завршување на работното време и сл.)	да
14.	Дали преку видеонадзорот ќе се обработуваат лични податоци само во реално време (мониторирање) или ќе се врши и снимање	Ако нема потреба податоците по 30 денови сами се бришат, ако има службено барање или потреба во тој случај се обработуваат со одредена цел
15.	Период на чување на снимките соодветен на целта/целите заради која/кои се поставува видеонадзорот	30 денови
16.	Кој ќе има пристап до видеонадзорот (лица вработени во контролорот, односно обработувачот) и број на лица кои ќе имаат пристап до видеонадзорот	2
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	солидно
20.	Проценка за број на потребни камери кои ќе се постават	4
21.	Тип/вид на камери (подвижни, статични, резолуција, опција за зумирање, ноќно снимање...)	Кликнете тука за да го внесете текстот.
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	30.05.2022
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

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

   Видео надзорот е потребен по проценка од контролорот за безбедност и заштита на лицата и имотот

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

Име	Презиме	
Име	Презиме	
Име	Презиме	

Име	Презиме	
Име	Презиме	
Име	Презиме	

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

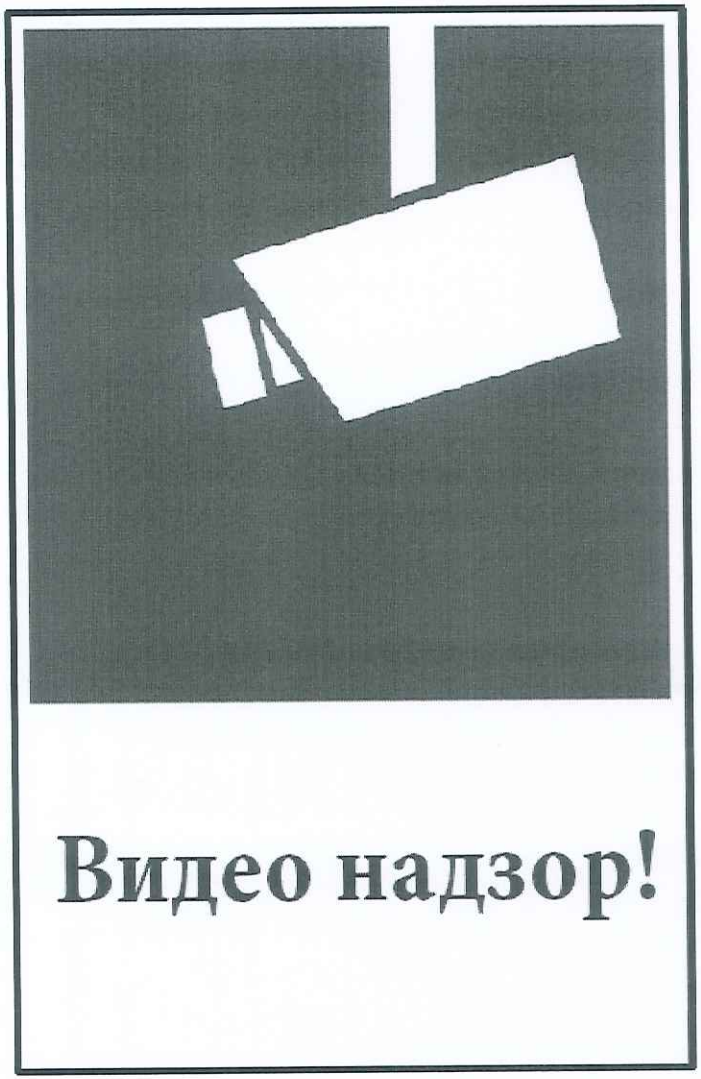
Билјана	Галовска	

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...):

Со одлука на директорот на БАС и по препорака на приватната Агенција за обезбедување "Карпатија", нивната техничка служба на наше барање направи анализа за инсталирање на видео надзорот. Склучен е договор и по нивна проценка поставен видео надзорот согласно Законот за ЗЛП и останати правила и прописи согласно Законот за приватно обезбедување и заштита

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

Маја	Кузмановска	



Видео надзор!

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:

Приватна непрофитна високообразовна установа
самостојна висока стручна школа
Бизнис академија Смилевски – БАС
Скопје
Седиште ул. Јане Сандански бр, 111/2 Скопје

e-mail: studentska.sluzba@bas.edu.mk

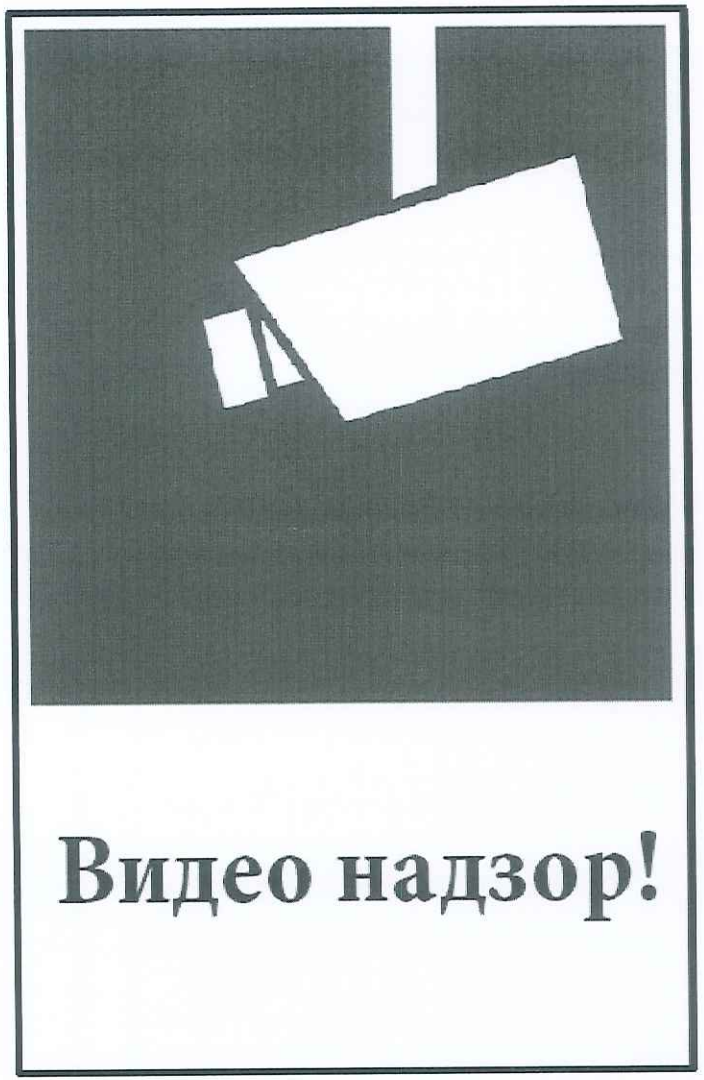
Контакт информациите за офицерот за заштита на личните податоци (доколку е определен): тел.072/252-603,
e-mail: biljana.galovska@bas.edu.mk

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): Период на чување на снимките - 30 дена; Период на следење – 24 часа дневно; Снимките не се објавуваат и пренесуваат на трети страни, освен со ваша дозвола или со дозвола од Контролорот при што ќе бидете известени за законскиот основ.

Цел, односно цели за вршење на видео надзорот: Заштита на сопственоста; Обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории; Заштита на животот или здравјето на луѓето.

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.*



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:

<u>Права на субјектите на лични податоци</u>: 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*

Образец бр.30

ЕВИДЕНЦИЈА

За нарушување на безбедноста на личните податоци

Ред.бр.	Бр./Дата на Известување до агенцијата за заштита на личните податоци	Субјект на личните податоци	Бр./Дата на Известување до Субјектот	Опис на природата на нарушувањето

Дата:

Одговорно лице:

_____

_____

Образец бр.22

ЕВИДЕНЦИЈА

На инциденти

Бр.	Инцидент	Дата кога се појавил инцидентот	Овластено лице кое го пријавило инцидентот	Лице на кого е пријавен инцидентот	Мерки кои се преземени за негово санирање	Категории на лични податоци кои се вратени и датум на враќање на истите
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Дата:

_____

Одговорно лице:

_____

Образец бр.21

ЕВИДЕНЦИЈА

За пристапот и увидот до личните податоци обработени преку системот за вршење на видеонадзор

Бр.	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 одвидеонадзорот	Вид на медиумот во кој е содржана снимката од видеонадзорот	Други податоци
1.							
2.							
3.							
4.							
5.							
6.							

Дата:

_____

Одговорно лице:

_____

Образец бр.22-а

ЕВИДЕНЦИЈА

На инциденти при Видеонадзорот

Бр.	Инцидент	Дата кога се појавил инцидентот	Овластено лице кое го пријавило инцидентот	Лице на кого е пријавен инцидентот	Мерки кои се преземени за негово санирање
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Дата:

_____

Одговорно лице:

_____

Образец бр. 2

ИЗВЕШТАЈ ОД ИЗВРШЕНА ПЕРИОДИЧНА ОЦЕНКА НА ПОСТИГНАТИТЕ РЕЗУЛТАТИ ОД СИСТЕМОТ ЗА ВРШЕЊЕ ВИДЕОНАДЗОР ВО

Бизнис Академија Смилевски

1.	Датум на воспоставување на системот за вршење на видеонадзор	2012 Дополнување/обновување:
2.	Датум (период) кога е извршена периодичната оценка	06.09.2021 - 10.09.2021
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	Да, Видеонадзорот ги исполнува целите во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кои е воспоставен.
5.	Оценка дали причините за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите, сеуште се релевантни	Да, Причините - заштита на сопственоста и обезбедување на контрола над влегувањето и излегувањето од службените простории за безбедносни цели, за поставување на видеонадзорот сеуште се релевантни.
6.	Статистички показатели за пристапот до снимките направени при вршење на видеонадзорот	Да, се пополнува Образец бр.21: Евиденција За пристапот и увидот до личните податоци обработени преку системот за вршење на видеонадзорот.
7.	Статистички показатели за начинот на искористување на снимките	Да, се пополнува Образец бр.21: Евиденција За пристапот и увидот до личните податоци обработени преку системот за вршење на видеонадзорот.
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;	Начинот за информирање дека се врши видеонадзор е соодветен.
9.	Статистички показатели за поднесени барања за остварување на правата на субјектите на лични податоци од видеонадзорот	Да, Образец: Евиденција 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)	Да, Образец бр.18: Евиденција За личните податоци кои се дадени на користење на корисник
11.	Статистички податоци од пријавени инциденти поврзани со системот за вршење на видеонадзор;	Да, Образец бр.22-а: Евиденција на инциденти при Видеонадзорот.
12.	Статистички податоци за нарушување на безбедноста на личните податоци кои се обработуваат преку системот за вршење видеонадзор	Да, Образец: Евиденција за нарушување на безбедноста на личните податоци кои се обработуваат преку системот за 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)	Периодот на чување на снимките е соодветен предлог истиот.
14.	Оценка дали има потреба од намалување или зголемување бројот на лица кои ќе имаат пристап до видеонадзорот	Нема потреба од зголемување на бројот на лица кои ке имаат пристап до видеонадзорот.
15.	Потреба од континуирана обука на овластените лица (предлог тема на обуката, број на лица што треба да бидат обучени)	Нема потреба од обука на овластените лица.
16.	Оценка дали целосно се применети мерките за техничка и интегрирана заштита на личните податоци (Data protection by design and by default)	Мерките за техничка и интегрирана заштита на личните податоци не се целосно применети, се применети само при снимањето на снимките од видеонадзорот.
17.	Оценка дали нивото на технички и организациски мерки кои се применуваат е соодветно	Нивото на технички и организациски мерки кои се применуваат за видеонадзорот е соодветна.
18.	Предлог за намалување/зголемување на број камери соодветно на нивото на исполнување на целта/целите заради кои е поставен видеонадзорот	Нема потреба од намалување/зголемување на камерите.
19.	Целта, односно целите за вршење на Видеонадзор	Заштита на сопственоста и обезбедување на контрола над влегувањето и излегувањето од службените простории за безбедносни цели.
20.	Оценка дали причините за поставување на видеонадзорот со образложение на потребата за исполнување на целта, односно целите сеуште се релевантни	Причините за поставување на видеонадзорот 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	Видеонадзорот ги исполнува целите во согласност со одредбите од член 90 став (1) од Законот за заштита на личните податоци заради кои е воспоставен.
22.	Податоци за спроведената проценка на влијанието на заштитата на личните податоци	Не е потребно спроведување на проценка на влијанието на заштитата на личните податоци, со оглед на обемот обемот на лицата и објектите кои се снимаат.
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	Да
25.	Можни технички или други решенија за замена на системот за вршење на видеонадзор	/
26.	Други податоци согласно проценката на Контролорот	/

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

Игор	Здравевски	
Љупчо	Џиланов	
Биљана	Димитровска	
Име	Презиме	
Име	Презиме	
Име	Презиме	

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

Офицерот за заштита на личните податоци се согласува со одлуките на лицата кои ја извршиле периодичната оценка на видеонадзорот.

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

ПОЛИТИКА

ЗА СИСТЕМОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

НА Бизнис Академија Смилевски

Скопје, октомври 2021

Врз основа на член 10 став (1) од Правилникот за безбедност на обработката на личните податоци Службен весник на Република Северна Македонија бр. 122/20 и Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), Наставно – Научен Совет на Бизнис Академија Смилевски на седницата одржана на ден 27.10.2021 година донесе

ПОЛИТИКА

ЗА СИСТЕМОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

НА Бизнис Академија Смилевски

1. Цел и опсег на Политиката

Безбедност на обработката на личните податоци

Систем за заштита на личните податоци

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, Бизнис кадемија Смилевски (во натамошниот текст – академијата) како контролор воспостави Систем за заштита на личните податоци преку примена на соодветни технички и организациски мерки за да обезбеди ниво на безбедност соодветно на ризикот.

Процесот за управување со системот за заштита на личните податоци 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.

Врз основа на Политиката за системот за заштита на личните податоци, Академијата има донесено подетални 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.

Техничките и организациските мерки на Академијата, особено опфаќаат:

- 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.

2. Нивоа на мерки за безбедност на обработката на личните податоци

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. Документација за технички и организациски мерки

Документацијата за технички и организациски мерки содржи:

- 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;

- 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;

- 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 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.

Академијата 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. Управување со ризик

(1) Академијата при управувањето со ризик (утврдувањето и проценатa 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) 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.

(3) 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.

5. Начела поврзани со обработката на лични податоци

Заради обезбедување на заштита на личните податоци Академијата применува Начела поврзани со обработката на лични податоци.

Личните податоци се:

- обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци („законитост, правичност и транспарентност“),

- собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели. Натамошната обработка за цели на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели, нема да се смета дека не е во согласност со првичните цели за кои се собрани личните податоци („ограничување на целите“),

- соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат („минимален обем на податоци“),

- точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени („точност“),

- чувани во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци. Личните податоци може да се чуваат подолго од нивниот рок на чување ако се обработуваат само за целите на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели, а со применување на соодветни технички и организациски мерки, заради заштита на правата и слободите на субјектот на личните податоци („ограничување на рокот на чување“),

- обработени на начин кој обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки („интегритет и доверливост“).

Академијата има утврдено овластени 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.

Академијата има определено овластено лице за заштита на личните податоци - офицер за заштита на личните податоци.

Академијата обезбедува офицерот за заштита на личните податоци на соодветен начин и навремено да е вклучен во сите прашања поврзани со заштитата на личните податоци.

Субјектите на личните податоци може да го контактираат офицерот за заштита на личните податоци за сите прашања поврзани со обработката на нивните лични податоци и за остварувањето на нивните права.

Офицерот за заштита на личните податоци ја почитува тајноста или доверливоста во однос на извршувањето на своите работи, во согласност со закон.

6.Законитост на обработката на личните податоци

Во Академијата обработката е потребна за исполнување на законска обврска на контролорот, во однос на: Законот за заштита на личните податоци; Законот за вработени на јавниот сектор чл.19; Законот за евиденција на областа на трудот чл.8 и чл.21; Законот за општа управна постапка; Законот за прекршоци; Закон за работни односи чл.116; и Закон за работни односи чл.117.

7. Одговорност на контролорот

(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 соодветни технички и организациски мерки за да обезбеди и да може да докаже дека обработката се врши во согласност со овој закон. Техничките и организациските мерки по потреба се преиспитуваат и се ажурираат.

(2) Ако е пропорционално на активностите за обработка, тогаш мерките од ставот (1) на овој член вклучуваат и примена на соодветни политики за заштита на личните податоци од страна на контролорот.

8. Обработка со овластување од страна на контролорот или обработувачот

Обработувачот и секое лице кое дејствува со овластување од страна на контролорот или обработувачот, а кое што има пристап до личните податоци, не треба да ги обработува тие податоци ако не се дадени упатства од контролорот, освен ако обработката не се бара со овој или друг закон.

9 .Евиденција на активностите за обработка

(1) Секој контролор и неговиот овластен претставник, води евиденција на операциите за обработка, а за кои е одговорен. Оваа евиденција, особено ги содржи следните информации:

(а) називот, односно името и презимето и контакт податоци на контролорот и на сите заеднички контролори, на овластениот претставник на контролорот и на офицерот за заштита на личните податоци;

(б) целите на обработката;

(в) опис на категориите на субјектите на личните податоци и на категориите на личнитеподатоци;

(г) категориите на корисници на кои се откриени или ќе бидат откриени личните податоци, вклучувајќи корисници во трети земји или меѓународни организации;

(д) преносот на лични податоци во трета земја или меѓународна организација, вклучувајќи идентификација на таа трета земја или меѓународна организација, а во случај на пренос на лични податоци, од членот 53 став (1) втор потстав од законот за заштита на личните податоци Сл.Весник 42/20, документација за соодветни заштитни мерки;

(ѓ) предвидените рокови за бришење на различните категории на лични податоци;

(е) општ опис на техничките и организациските мерки за безбедност од членот 36 став (1) од законот за заштита на личните податоци Сл.Весник 42/20.

10.Соработка со Агенцијата

Контролорот и обработувачот и нивните овластени претставници, се должни на барање на Агенцијата да соработуваат со неа, при исполнување на нејзините задачи.

11. Права на субјектите на лични податоци

Правата на субјектите на лични податоци се следните:

- Правото на пристап (член 19 од Законот за Заштита на Личните Податоци)
- Право на исправка (член 20 од ЗЗЛП)
- Право на бришење "право да се биде заборавен" (член 21 од ЗЗЛП)
- Право на ограничување на обработката (член 22 од ЗЗЛП)
- Право на преносливост (член 24 од ЗЗЛП)
- Право на приговор (член 25 од ЗЗЛП)
- Право во врска со автоматско донесување на поединечни одлуки, вклучувајќи и профилирање (член 26 од ЗЗЛП).

12.Известување на Агенцијата за нарушување на безбедноста на личните податоци

(1) Во случај на нарушување на безбедноста на личните податоци, контролорот веднаш и не подоцна од 72 часа откако дознал за истото е должен да ја извести Агенцијата за нарушувањето на безбедноста на личните податоци, освен ако не постои веројатност нарушувањето на безбедноста на личните податоци да создаде ризик за правата и слободите на физичките лица. Кога известувањето до Агенцијата не е поднесено во рок од 72 часа, заедно со известувањето треба да биде доставено и образложение за причините за доцнењето.

(2) Обработувачот е должен да го извести контролорот веднаш, откако дознал за нарушување на безбедноста на личните податоци.

13.Известување на субјектот на личните податоци за нарушување на безбедноста наличните податоци

(1) Во случај на нарушување на безбедноста на личните податоци, за кое постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, контролорот, веднаш го известува субјектот на личните податоци за нарушувањето на безбедноста на личните податоци.

Академијата Политиката да ја ревидира и усогласува согласно промените во неговото работење.

Директор: д-р Маја Кузмановска

ПРАВИЛНИК

За активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот

НА Бизнис Академија Смилевски

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20) и член 31 од Правилникот за безбедност на обработката на личните податоци Наставно – Научен Совет на Бизнис Академија Смилевски, на седницата одржана на ден 27.10.2021 година донесе

ПРАВИЛНИК

За активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот

НА Бизнис Академија Смилевски

Член 1

(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.

Член 2

(1) 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.

(2) Изјавата од ставот (1) 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.

(3) Изјавата од ставот (1) на овој член задолжително се чува во досиејата на лицата кои се вработуваат или се ангажираат кај контролорот.

Член 3

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

Член 4

(1) Офицерот за заштита на личните податоци покрај останатите задачи ги врши и следните работи:

(а) ги информира и советува контролорот или обработувачот и вработените кои вршат обработка соодветно на нивните обврски според одредбите од овој закон;

(б)врши подигнување на свеста и обучување на вработените кои што учествуваат во операциите на обработка на личните податоци, преку:

- организирање на обуки, и

- изработка на известувања, упатства, летоци со содржина од начелата и правилата за заштитата на личните податоци.

(2) Офицерот за заштита на личните податоци пополнува Регистар на обуки за планираните обуки за вработените кои вршат обработка на лични податоци (Образец бр.8).

Член 5

Овој правилник влегува во сила со денот на донесувањето од страна на Наставно – Научниот Совет на Ветеринарен Факултет Битола.

Бизнис Академија Смилевски
Директор:
д-р Маја Кузмановска

ПРАВИЛНИК

за динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола

на БАС

Скопје, октомври 2021

Датум на поднесување на Извештајот: __/__/____ година

Ревизијата/контролата/проверката е спроведена од:

_____ (име и презиме и потпис)

Одговорни лица за имплементација на корективните мерки:

_____ (име и презиме и потпис)

_____ (име и презиме и потпис)

1 Контролорот да одлучи кој термин ќе го употребува за оваа постапка

Прилог бр.3

Контролна листа на подготвителни активности на ОЗЛП

за спроведување на ревизија/контрола/проверка

1. Да се прибере потребната документација: внатрешни прописи на контролорот, договори, извештаи од претходни проверки и други релевантни документи	
2. Да се прочитаат и анализираат прописите и документите	
3. Да се подготви План која збирка на лични податоци односно која организациска единица ќе биде предмет на ревизија/ контрола/проверка	
4. Да се подготви Список со кого треба да се одржат состаноци и што треба да се договори на состаноците	
5. Да се усогласи временскиот период и термините во кои ќе се спроведе ревизијата/контролата/проверката	
6. Да се утврди подетално што ќе биде предмет на ревизијата/контролата/проверката	
7. Да се определи кои документи ќе бидат предмет на детална проверка	
8. Да се провери дали наодите од претходни извештаи/решенија се надминати	
9. Да се оцени дали треба да се направи поединечно или групно интервју во организациската единица во која ќе се спроведе ревизијата/контролата/проверката	
10. Да се оцени потребата од состанок со обработувачите или трети лица	
11. Да се подготви Листа за проверка што ќе се користи при ревизијата/контролата/проверката	
12. Да се подготви допис до организациската единица каде што ќе се спроведе ревизијата/контролата/проверката и до нејзиниот раководител/менаџер	
13. Да се предвиди времето кога треба да заврши ревизијата/контролата/проверката	
14. Да се оцени потребата од поддршка од други организациски единици при спроведување на ревизијата/контролата/проверката	
15. Да се подготви Извештај за извршената ревизија/контрола/проверка	

Прилог бр.4

Извештај

за извршена внатрешна контрола

Внатрешна контрола број: _____

Датум на почеток на внатрешната контрола:_____

Период во кој ќе се спроведе внатрешната контрола:_____

Цели на внатрешната контрола:

Внатрешна контрола на Информацискиот систем и информатичката инфраструктура на факултетот 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.

Опис на операциите на обработка на лични податоци што се предмет на внатрешната контрола:

- на технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци;

- на евиденција на секој авторизиран/неавторизиран пристап до информацискиот систем;

- на доверливоста и сигурноста на лозинките и на останатите форми на идентификација;

- на начинот за пристап на вработените и ангажираните лица во факултетот до интернет, кои се однесуваат на симнување и снимање на документи преземени од електронска пошта и други извори;

- на уништување на документи кои содржат лични податоци по истекување на рокот за чување, како и за начинот на уништување, бришење и чистење на медиумите;

- на начинот на управување со медиуми кои се носители на лични податоци;

- на примената на принципот "чисто биро";

- на писмените овластувања издадени од страна на факултетот/контролорот за вршење на обработка на личните податоци и за пренесување на медиуми надвор од работните простории на факултетот;

- на начинот на воспоставување на физичка сигурност на работните простории и опремата каде што се обработуваат и чуваат личните податоци;

- на начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;

- на евиденцијата за физички пристап до просторијата во која се сместени серверите; и

- на постапката за потпишување на изјави за тајност и заштита на обработката на личните податоци од страна на вработените и ангажираните лица во факултетот.

Релевантни законски, подзаконски и интерни прописи:

1. Закон за заштита на личните податоци;

2. Правилник за безбедност на обработката на личните податоци;

3. Правилник за содржината на анализата на целта, односно целите за која се поставува видеонадзорот и извештајот од извршена периодична оценка на постигнатите резутати од системот за вршење на видеонадзор.
4. Правилник за начинот на известување за нарушување на безбедноста на личните податоци.
5. План за создавање систем на технички и организациски мерки за обезбедување тајност и заштитана обработката на личните податоци;

6. Правилник за идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);

7. Правилник за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот; во кои се вклучени и следните правила:

- 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;
- начинот на обезбедување на опремата на факултетот на која се врши обработка на личните податоци;
- начинот на обезбедување на преносливите медиуми;
- начинот на обезбедување на серверите и веб-страницата на факултетот;
- начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци;
- начинот на обработка на личните податоци кои се криптирани;
- физичка безбедност;

- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);

8. Правилник за обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;

9. План за управување со континуитет на информацискиот систем;

10. Правилник за пријавување, реакција и санирање на инциденти;

11. План за обезбедување на континуитет;

12. Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;

13. Правилник за начинот на уништување и бришење на документите;

14. Правилник за активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во факултетот;

15. Правилник за дизајнирање, развивање и одржување на софтверските програми за обработка наличните податоци, а особено од аспект на техничка и интегрирана заштита на личните податоци (Data protection by design and by default); и

16. Правилник за динамика и начин на вршење на периодични контроли, како и процесите за вршење навнатрешна контрола.

Организациска единица во која се спроведува внатрешната контрола:

Ветеринарен Факултет Битола

Комисија/ Лица кои учествуваат во внатрешната контрола:

Извештај од извршената внатрешната контрола:

Каталогот на предложени корективни мерки и препораки:

Бр.	Наод	Опис на корективна мерка/ препорака	Краен рок за постапување	Преземени активности	Статус
6.					
7.					
8.					
9.					
10.					

Оценка/мислење од офицерот за заштита на личните податоци:

Датум на поднесување на Извештајот: __/__/____ година

внатрешната контрола е спроведена од:

_____ (име и презиме и потпис)

_____ (име и презиме и потпис)

_____ (име и презиме и потпис)

Одговорни лица за имплементација на корективните мерки:

_____ (име и презиме и потпис)

_____ (име и презиме и потпис)

Офицер за заштита на личните податоци:

_____ (име и презиме и потпис)

Образец бр.12

Табела

за следење на наодите од извршени ревизии/контроли/проверки/инспекции1

Ред бр.	Институција/компанија што ја спровела ревизијата/ контролата/проверката/ инспекцијата	Вид на ревизија/ контрола/ проверка/ инспекција	Период кога е извршена	Наоди	Корективни мерки	Препораки	Одговорен за исполнување на корективните мерки и препораките	Краен рок за исполнување на корективните мерки и постапување по препораките	Преземени активности	Статус на наодот: затворен/ во тек
1.										
2.										
3.										
4.										
5.										
6.										

1 Во оваа Табела ќе бидат внесени наодите од ревизиите/контролите/проверките спроведени кај контролорот од страна на ОЗЛП или друга организациска единица, но и наодите од инспекциите од ДЗЛП и контролите од надворешни компании

ПРАВИЛНИК

ЗА ИДЕНТИФИКАЦИЈА, ОЦЕНКА И КЛАСИФИКАЦИЈА НА РИЗИКОТ НА ПРОЦЕСИТЕ СО КОИ СЕ ВРШИ ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

(АНАЛИЗА НА РИЗИК)

НА БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ

СКОПЈЕ, ОКТОМВРИ 2021

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), Наставно – Научен Совет на Бизнис Академија Смилевски на седницата одржана на ден 27.10.2021 донесе

ПРАВИЛНИК

ЗА ИДЕНТИФИКАЦИЈА, ОЦЕНКА И КЛАСИФИКАЦИЈА НА РИЗИКОТ НА ПРОЦЕСИТЕ СО КОИ СЕ ВРШИ ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

(АНАЛИЗА НА РИЗИК)

на Бизнис Академија Смилевски

Член 1

Со овој правилник се пропишува начинот на управување со ризик односно утврдувањето и проценатa на 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 во Бизнис Академија Смилевски кој се јавува во својство на контролор.

Член 2

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;

Член 3

Управувањето со ризикот од член 1 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.

Член 4

Списокот на процеси со кои се врши обработка на личните податоци од член 1 точка а) преку целосно или делумно автоматизирана обработка на личните податоци или друга обработка на лични податоци, ги опфаќа:

- Хардверот (сервери, лаптопи, хард дискови и други медиуми);

- Софтверот (оперативни системи и софтверски програми развиени за потребите на контролорот);

- Комуникациски канали (оптички кабли, интернет, безжична мрежна технологија – Wi-Fi);

- Документи во хартиена форма (печатени документи, фотокопии).

Член 5

(1) Проценатa на ризиците од член 2 точка б) на член 3, ги опфаќа:

(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).

(2) Образец бр.25: Прашалник за проценка на ризик за операциите на обработка на лични податоци, (Прилог бр.1) е составен дел на овој Правилник.

Член 6

Контролорот задолжително врши спроведување и проверка на планираните мерки од член 3 точка в), а со цел да се обезбеди дека тие се применуваат и тековно се тестираат.

Член 7

Контролорот задолжително спроведува периодични безбедносни проверки од член 3 точка г), за што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.

Член 8

Овој правилник влегува во сила на денот на денот на донесувањето на Одлука од страна на Наставно – Научниот Совет на Бизнис Академија Смилевски

Бизнис Академија Смилевски

Директор

Д-р Маја Кузмановска

ПРАВИЛНИК

ЗА ИДЕНТИФИКАЦИЈА, ОЦЕНКА И КЛАСИФИКАЦИЈА НА РИЗИКОТ НА ПРОЦЕСИТЕ СО КОИ СЕ ВРШИ ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

(АНАЛИЗА НА РИЗИК)

НА БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ

СКОПЈЕ, ОКТОМВРИ 2021

Врз основа на член 66 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), Наставно – Научен Совет на Бизнис Академија Смилевски на седницата одржана на ден 27.10.2021 донесе

ПРАВИЛНИК

ЗА ИДЕНТИФИКАЦИЈА, ОЦЕНКА И КЛАСИФИКАЦИЈА НА РИЗИКОТ НА ПРОЦЕСИТЕ СО КОИ СЕ ВРШИ ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

(АНАЛИЗА НА РИЗИК)

на Бизнис Академија Смилевски

Член 1

Со овој правилник се пропишува начинот на управување со ризик односно утврдувањето и проценатa на 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 во Бизнис Академија Смилевски кој се јавува во својство на контролор.

Член 2

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;

Член 3

Управувањето со ризикот од член 1 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.

Член 4

Списокот на процеси со кои се врши обработка на личните податоци од член 1 точка а) преку целосно или делумно автоматизирана обработка на личните податоци или друга обработка на лични податоци, ги опфаќа:

- Хардверот (сервери, лаптопи, хард дискови и други медиуми);

- Софтверот (оперативни системи и софтверски програми развиени за потребите на контролорот);

- Комуникациски канали (оптички кабли, интернет, безжична мрежна технологија – Wi-Fi);

- Документи во хартиена форма (печатени документи, фотокопии).

Член 5

(1) Проценатa на ризиците од член 2 точка б) на член 3, ги опфаќа:

(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).

(2) Образец бр.25: Прашалник за проценка на ризик за операциите на обработка на лични податоци, (Прилог бр.1) е составен дел на овој Правилник.

Член 6

Контролорот задолжително врши спроведување и проверка на планираните мерки од член 3 точка в), а со цел да се обезбеди дека тие се применуваат и тековно се тестираат.

Член 7

Контролорот задолжително спроведува периодични безбедносни проверки од член 3 точка г), за што се подготвува акционен план, чија имплементација се следи од страна на раководството на контролорот.

Член 8

Овој правилник влегува во сила на денот на денот на донесувањето на Одлука од страна на Наставно – Научниот Совет на Бизнис Академија Смилевски

Бизнис Академија Смилевски

Директор

Д-р Маја Кузмановска

ПРАШАЛНИК

За Проценка на ризик за операциите на обработка на лични податоци:

1.	Список (преглед) на сите процеси со кои се врши обработка на лични податоци;	1.Хардвер (сервери, лаптопи, хард дискови и други медиуми); 2. Софтвер (оперативни системи и софтверски програми развиени за потребите на контролорот); 3. Комуникациски канали (оптички кабли, интернет, безжична мрежна технологија – Wi-Fi); 4. Документи во хартиена форма (печатени документи, фотокопии).
2.	Утврдување на потенцијалните влијанија и ефекти на обработката на личните податоци врз правата и слободите на субјектите, за следните потенцијални закани, односно настани: - неовластен пристап до личните податоци; - непосакувани промени на личните податоци; и - привремена или целосна недостапност до личните податоци.	
3.	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).	
4.	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.).	
5.	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).	
6.	Оценување на сериозноста и веројатноста на ризиците, во однос на претходните елементи предвидени во овој став (скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална).	

Правилник

за изменување и дополнување на

Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), и член 10 став (3) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Наставно – Научен Совет на БАС, на седницата одржана на ден 27.10.2021 година донесе

Правилник

за изменување и дополнување на

Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица

Член 1

Во Правилникот За определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица, на Бизнис Академија Смилевски во членот 3, став (1), се дополнува:

- 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, при што кога проверката се врши врз основа на корисничко име и лозинка, 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;
- обезбедува 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); во случај на одреден број на неуспешни обиди за најавување на информацискиот систем, кои се во спротивност со политиките за автентикација на факултетот, обезбедува автоматизирано отфрлање од информацискиот систем после три последователни неуспешни обиди; инсталира заштитен ѕид (firewall); поставува и редовно ажурира антивирусен софтвер; и други дополнителни мерки од Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на факултетот;
- Води евиденција на операциите за обработка на личните податоци;

- Текстот од алинеја 4 се брише, а на нејзино место се става: врши Контрола на пристап до информацискиот систем при што: обезбедува Овластените лица задолжително да имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи; ги доделува, менува или одзема привилегиите на авторизираниот пристап (корисничко име и лозинка) до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на факултетот (при вработување или престанок на работниот однос);
- Текстот од алинеја 9 се брише, а на нејзино место се става: воспоставува и води евиденција за секој пристап до информацискиот систем logs, која содржи: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем, како 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; и ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем и обезбедува заштита на системот за евиденција за пристап до информацискиот систем; Операциите кои овозможуваат евидентирање на податоците треба да бидат контролирани од страна на офицерот за заштита на личните податоци, кој најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.

Член 2

Овој правилник влегува во сила со денот на донесувањето од страна на Наставно – Научниот Совет на Бизнис Академија Смилевски

Бизнис Академија Смилевски

Директор:

Др. Маја Кузмановска

ПРАВИЛНИК
ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА

ПРАВИЛНИКОТ ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ НА БАС

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), и чл.10, став (3) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Наставно – Научен Совет на БАС, на седницата одржана на ден _____2021 година донесе

ПРАВИЛНИК
ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА

ПРАВИЛНИК
ЗА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ НА ВЕТЕРИНАРЕН ФАКУЛТЕТ БИТОЛА

Член 1

Во правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на БАС, во член 7, став (4), точка (г), се брише „информациска ревизорска трага” и по „безбедност на просториите” се додава „и криптирање.”.

Член 2

Во член 8, став (2), по „се класифицираат во” се брише „две нивоа” и на нивно место се става „едно ниво”, и во алинеја 1 се брише точка и запирка и „и” и се става точка, а во алинеја 2 се брише „високо.”.

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, факултетот применува соодветно ниво на технички и организациски мерки кое ќе биде пропорционално и на активностите за обработка на личните податоци.

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

- стандардно; и
- високо.

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

Член 9

Во член 9, став (2), по „стандардното," се бриши останатиот текст.

(1) Факултетот 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) Факултетот 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.

Член 10

(1)Во член 10, став (3), точка в), се бриши алинеја 3 - „начинот на обезбедување евиденција за секој пристап до информацискиот систем;" .

(2) Во член 10, став (3), точка в), се додава алинеја:

- „начинот на заштита на внатрешната мрежа на контролорот;" .

(3)Во член 10, став (3), точка е), после `континуитет` се додава „на информацискиот систем;" .

(4) Во член 10, став (3) по точка ј) се додаваат следните точки:

к) Правилник за содржината и формата на актот за начинот на вршење на видеонадзор На Ветеринарен Факултет Битола;

л) План за управување при користење на услуги за обработка на личните податоци од страна на обработувачи На Ветеринарен Факултет Битола;

љ) Процедура за чување и бришење на личните податоци од Видеонадзорот во Ветеринарен Факултет Битола;

м) Процедура за овластувањата и улогата на офицерот за заштита на личните податоци во Ветеринарен Факултет Битола;

н) Процедура за правата на субјектите на лични податоци во Ветеринарен Факултет Битола;

њ) Процедура за уредување на организациските единици вклучени во одговарањето на барањата од субјектите во Ветеринарен Факултет Битола;

о) Процедура за одлучување при изборот на обработувачот во Ветеринарен Факултет Битола;

п) Процедура за пристап на корисници до личните податоци во Ветеринарен Факултет Битола;

р) Процедура за управување со архивскиот материјал на лични податоци во Ветеринарен Факултет Битола;

с) Правила за начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци во Ветеринарен Факултет Битола;

т) Правила за пристап на овластените лица до интернет кои се однесуваат на симнување и снимање на документи преземени од електронската пошта и други извори во Ветеринарен Факултет Битола.

Член 12

(1) Во член 12, став (1), алинеја 5, по „сигурносна копија" се става точка и се брише останатиот текст - „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.".

(2) Во член 12, став (2), се брише алинеја 6 - „ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;" .

Член 15

Член 15 целосно се брише.

Обезбедување на преносливите медиуми
Член 16

(1)Во член 16, став 2, алинеја 2, по „резервна копија" се брише точка-запирка и се додава „на мобилните работни станици, со цел да заштитат од губење на зачуваните податоци;".

Член 17

По член 16 се додава член 17 - Заштита на внатрешната мрежа:

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

- 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);
- обезбедување ниту еден административен панел за управување со содржина и нагодување на системот да не биде директно достапен преку интернет (далечинското одржување задолжително се врши преку Microsoft Teams – Remote desktop Client); и
- ограничување на мрежниот сообраќај со филтрирање на влезниот/појдовниот сообраќај на опрема со заштитен ѕид, 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).

Обезбедување на веб-страницата
на факултетот
Член 19

(1)Во член 19, став 1, алинеја 1, по „(TLS заменувајќи го SSL) на" се брише „сите веб страници на факултетот (ако има повеќе од една)" и се додава „на страницата на

факултетот".

(2) Во член 19, став 1, алинеја 2, по „ веб- страницата" се брише запирката и се става точка, а останатиот текст се брише.

Сигурносни копии и повторно враќање на зачуваните лични податоци (обезбедување континуитет)
Член 22

Во член 22, став 2, по „овој член" се брише „треба да", а наместо „усвојува" се става „има усвоено".

Во член 22, став 6, по „личните податоци" во заградата се додава „на пример: со криптирање на сигурносните копии,".

Начин на архивирање и чување на податоците
Член 23

Во член 23, став 1, по „безбеден начин" се брише запирката и останатиот текст и се става точка.

Управување со преносливи медиуми
Член 24

(1) Во член 24, став 1, по „личните податоци." се брише останатиот текст и се додава „Преносliв медиум - УСБ се користи само при носењето на личните податоци од налози за плата во трезорот на РСМ, кои се криптирани, заради исплата на плата на вработените во факултетот."

Криптирање на личните податоци
Член 25

Во член 25, се брише став 1.

Во член 25, став 2, по „криптирање" се додава „само при правење на бекап-копии" и по „Енкрипција)" се брише точката и се додава запирка и „при што обезбедува заштита на тајните лозинки за криптирање, до кои имаат пристап само овластените лица."

Физичка безбедност
Член 26

Во член 26, став 1, алинеја 2, по „пожар" се додава „(користење на противпожарен апарат)", по „прашина" се брише останатиот текст и се става точка.

Во член 26, став 1, алинеја 3, се додава „при што само овластените лица имаат пристап до истите;".

Во член 26, став 1, алинеја 4, по „воспоставување на" се брише „правила и методи за".

Во член 26, став 1, се брише алинеја 5 и на нејзино место се става „одржување на просториите за серверите (користење на парно греење во зимскиот период, одржување на хигиената, итн.).".

Во член 26, став 1, алинеја 6, се брише точката и се додава „само овластените лица имаат пристап до клучевите за просториите)."

Контрола на информацискиот систем
и информатичката инфраструктура

Член 27

Во член 27, став 1, по „во членот 10 од" наместо „овој правилник" се става „правилникот за безбедност на обработката на личните податоци бр.на Сл.Весник на СРМ 122/20".

2. Организациски мерки

Пристап до документите

Член 32

Во член 32, став 2 се брише целосно.

Чување на документи

Член 34

Во член 34, став 1, по „ соодветни механизми" се брише текстот „(се чуваат заклучени во плакар)" и се додава по „отворање" се брише точката и се става запирка и се додава „како што се чување на документите во хартиена форма во просторија, заклучени со клучеви во метален сеф или заклучени во плакар, до кои имаат пристап само овластените лица за обработка на документите."

Во член 34, се бришат став 2 и став 3.

Начин на чување на документите

Член 36

Во член 36, став 1, по „заклучени со" се брише „синџир, катанец и клуч." и се додава „клучеви, до кои имаат пристап само овластените лица за обработка на документите."

I. ВИСОКО НИВО

1. Технички мерки

Дополнителни мерки

Член 37

Факултетот 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 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 (криптирање) за да се спречи неовластено обработување на личните податоци снимени на нив.

Тестирање на информацискиот систем

Член 41

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

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

Пренесување на медиуми

Член 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.

1. Организациски мерки

Пренесување на документи

Член 46

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

Влегување во сила

Член 49

Овој правилник влегува во сила со денот на донесувањето од страна на Наставно – Научниот Совет на Ветеринарен Факултет Битола.

Бизнис Академија Смилевски

Директор :
Д-р Маја Кузмановска

ПРАВИЛНИК

ЗА НАЧИНОТ НА ПРАВЕЊЕ НА СИГУРНОСНА КОПИЈА, АРХИВИРАЊЕ И ЧУВАЊЕ, КАКО И ПОВТОРНО ВРАЌАЊЕ НА ЗАЧУВАНИТЕ ЛИЧНИ ПОДАТОЦИ

(обезбедување континуитет)

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), и член 22 став (2) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Наставно – Научен Совет на Бизнис Академија Смилевски, Скопје, на седницата одржана на ден _____2021 година донесе

ПРАВИЛНИК

ЗА НАЧИНОТ НА ПРАВЕЊЕ НА СИГУРНОСНА КОПИЈА, АРХИВИРАЊЕ И ЧУВАЊЕ, КАКО И ПОВТОРНО ВРАЌАЊЕ НА ЗАЧУВАНИТЕ ЛИЧНИ ПОДАТОЦИ

(обезбедување континуитет)

Член 1

Со овој Правилник се пропишува начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци кои се предмет на обработка во Бизнис Академија Смилевски (во натамошниот текст: БАС).

Член 2

(1)БАС врз основа на анализата на ризикот прави сигурносна копија и архивирање на податоците во системот, на начин кој ќе гарантира повторно воспоставување на достапноста до личните податоци во случај на настанат физички или технички инцидент.

(2)БАС прави сигурносни копии на личните податоци на редовни временски интервали, при што се прави целосна сигурносна копија (full back-up) еднаш месечно, секој последен работен ден во месецот.

(3)Податоците од извршениот “backup” – резервна копија се криптираат и префрлаат на екстерен хард диск, кој се чува во шкаф заклучен со клуч, надвор од просторијата во која се наоѓаат серверите со лични податоци (во друга просторија), заради оневозможување на каква било модификација и заштита од неовластен пристап, до кои има пристап само администраторот на информацискиот систем.

(4)Администраторот на информацискиот систем еднаш месечно задолжително ја проверува функционалноста на сигурносните копии од став (1) на овој член за што го известува Офицерот за заштита на личните податоци.

Член 3

Администраторот на информацискиот систем е одговорен за примената на Правилникот за правење на сигурносна копија, арихивирање и чување, како и за повторно враќање на зачуваните лични податоци.

Член 4

(1)При настанат инцидент се пристапува кон постапки за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени, при што се копира направената копија на лични податоци од надворешниот хард диск и се префрла на персоналниот компјутер на кој се чувале/чуваат личните податоци.

(2)Одговорните лица вршат евидентирање на вратените лични податоци, при што се евидентира датумот на враќање на податоците и категоријата на податоци што се враќа (Евиденција на инциденти – Образец бр.22).

Член 5

Факултетот 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 (чување на безбедно место на сигурносната копија за кое се применети мерки и контроли кои го минимизираат ризикот од поплава, пожар, кражба и слично).

Член 6

Со денот на влегувањето во сила на овој правилник престанува да важи Правилникот начинот на правење на сигурносна копија, архивирање и чување, како и повторно враќање на зачуваните лични податоци, на Бизнис Академија Смилевски

Член 7

Овој правилник влегува во сила со денот на донесувањето од страна на Наставно – Научниот Бизнис Академија Смилевски

Бизнис Академија Смилевски
Директор:
Д-р Маја Кузмановска

Образец бр.12

Табела

за следење на наодите од извршени ревизии/контроли/проверки/инспекции1

Ред бр.	Институција/компанија што ја спровела ревизијата/ контролата/проверката/ инспекцијата	Вид на ревизија/ контрола/ проверка/ инспекција	Период кога е извршена	Наоди	Корективни мерки	Препораки	Одговорен за исполнување на корективните мерки и препораките	Краен рок за исполнување на корективните мерки и постапување по препораките	Преземени активности	Статус на наодот: затворен/ во тек
1.										
2.										
3.										
4.										
5.										
6.										

1 Во оваа Табела ќе бидат внесени наодите од ревизиите/контролите/проверките спроведени кај контролорот од страна на ОЗЛП или друга организациска единица, но и наодите од инспекциите од ДЗЛП и контролите од надворешни компании

Образец бр.12

Табела

за следење на наодите од извршени ревизии/контроли/проверки/инспекции1

Ред бр.	Институција/компанија што ја спровела ревизијата/ контролата/проверката/ инспекцијата	Вид на ревизија/ контрола/ проверка/ инспекција	Период кога е извршена	Наоди	Корективни мерки	Препораки	Одговорен за исполнување на корективните мерки и препораките	Краен рок за исполнување на корективните мерки и постапување по препораките	Преземени активности	Статус на наодот: затворен/ во тек
1.										
2.										
3.										
4.										
5.										
6.										

1 Во оваа Табела ќе бидат внесени наодите од ревизиите/контролите/проверките спроведени кај контролорот од страна на ОЗЛП или друга организациска единица, но и наодите од инспекциите од ДЗЛП и контролите од надворешни компании

ПРАВИЛНИК
ЗА НАЧИНОТ НА УНИШТУВАЊЕ И БРИШЕЊЕ НА ДОКУМЕНТИТЕ

Скопје, октомври 2021

Врз основа на член 17 став (7) од Законот за вработените во јавниот сектор ("Службен весник на Република Македонија" бр.27/2014 и 199/2914) и член 66 од Законот за високото образование и Врз основа на член 41-а алинеа 4 од Законот за заштита на личните податоци (Службен весник на Р.М бр.7/05, 103/08, 124/10, 135/11, 43/14, 153/15 и 99/16), Деканската управа на Бизнис Академија Смилевски на ден 27.10.2021 година донесе

П Р А В И Л Н И К

За начинот на уништувањето на документите и нивно бришење

Член 1

Со овој Правилник се пропишува начинот на уништување на документите, како и начинот на бришење во Бизнис Академија Смилевски во понатамошниот текст академијата.

Член 2

Документите од став 1 на овој член се уништуваат со уред за ситнење при што истите повторно неможат да бидат употребливи, за што комисијата составува записник којшто го доставува до деканот на факултетот.

Во записникот задолжително се наведуваат сите податоци за целосната идентификација на документите што се уништуваат како и категориите на личните податоци содржани во истите.

Одредбите од овој член се применуваат и при уништувањето на копиите или умножените документи.

Член 3

Бришењето или чистењето на податоците се врши на начин што се оневозможува понатамошно обновување на снимените податоци.

Комисијата составена за бришење и уништување на податоците составува посебен записник, кои што ги содржи сите податоци за целосна идентификација на материјалите кои се уништени или бришени.

Член 4

Овој правилник влегува во сила со денот на донесувањето на Одлука од страна на топ менаџментот на Академијата

П р а в и л н и к

За определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), и член 10 став (3) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Наставно – Научен Совет на Бизнис Академија Смилевски , на седницата одржана на ден 27.10.2021 година донесе

Правилник

За определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица

Член 1

Со овој правилник се пропишуваат обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема што Бизнис Академија Смилевски, во својство на контролор го применува за обезбедување тајност и заштита на обработката на личните податоци.

Член 2

Администраторот на информацискиот систем во смисла на овој правилник е државниот службеник кој има посебно овластување од страна на Директорот на факултетот. Да се додаде: за планирање и за применување на технички и организациски мерки, како и за контрола на обезбедувањето тајност и заштита на обработката на личните податоци;

1. Овластеното лице во смисла на овој правилник е државниот службеник, надворешни соработници и други лица во академијата кои користат документи кои содржат лични податоци и имаат пристап до информатичко комуникациската опрема на Факултетот. Да се додаде: 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;

Член 3

(1) Администраторот на информацискиот систем во факултетот ги има следните обврски и одговорности:

- Врши анализа и проценка на ризиците на информацискиот систем на Факултетот;
- Врши креирање, имплементација и развој на целокупниот процес на информативна сигурност;

- Врши ревизија на инциденти поврзани со нарушувањата на безбедноста на информацискиот систем во согласност со Правилникот за пријавување, реакција и санирање на инциденти во Факултетот;
- 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, при што кога проверката се врши врз основа на корисничко име и лозинка, 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;
- Врши контрола на пристап до информацискиот систем при што: обезбедува Овластените лица задолжително да имаат авторизиран пристап само до личните податоци и информатичко комуникациската опрема кои се неопходни за извршување на нивните работни задачи; ги доделува, менува или одзема привилегиите на авторизираниот пристап (корисничко име и лозинка) до личните податоци и информатичко комуникациската опрема само во согласност со критериумите кои се утврдени од страна на факултетот (при вработување или престанок на работниот однос);
- Го определува нивото на пристап до документите/информациите содржани во информацискиот систем по претодно овластување добиено од страна на Деканот на факултетот;
- Изработува програма за ревизии во однос на сигурноста на информацискиот систем;
- Обезбедува 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); во случај на одреден број на неуспешни обиди за најавување на информацискиот систем, кои се во спротивност со политиките за автентикација на факултетот, обезбедува автоматизирано отфрлање од информацискиот систем после три последователни неуспешни обиди; инсталира заштитен ѕид (firewall); поставува и редовно ажурира антивирусен софтвер; и други дополнителни мерки од Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци на факултетот;
- Води евиденција на операциите за обработка на личните податоци;
- Се грижи за спроведување на правилата за начинот на правење на сигурносна копија, аривирање и чување, како и повторно враќање на зачуваните лични податоци согласно Правилникот за начинот на правење сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци на Факултетот.

- Му помага на офицерот за заштита на личните податоци при вршење на неговите работни задачи согласно прописите за заштита на личните податоци, документацијата за теничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на Факултетот.
- Воспоставува и води евиденција за секој пристап до информацискиот систем logs, која содржи: име и презиме на овластеното лице, работната станица од каде се пристапува до информацискиот систем, датум и време на пристапување, запис за авторизација за секое пристапување, запис за секој неавторизиран пристап и запис за автоматизирано отфрлање од информацискиот систем, како 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; и ги известува овластените лица за воспоставениот систем за евиденција за пристап до информацискиот систем и обезбедува заштита на системот за евиденција за пристап до информацискиот систем; Операциите кои овозможуваат евидентирање на податоците треба да бидат контролирани од страна на офицерот за заштита на личните податоци, кој најмалку еднаш месечно и изготвува извештај за извршената проверка и за констатираните неправилности.
- Во координација со офицерот за заштита на личните податоци се грижи за организација на обуки на вработените во однос на одржување на безбедноста на информацискиот систем.

(2) За начинот на извршување на работата на администраторот на информацискиот систем се врши периодична контрола од страна на комисија формирана од Директорот на академијата

(3) За извршената периодична контрола комисијата од ставот 2 од овој член изработува извештај во кој ги внесува констатираните неправилности и предложените мерки за нивно отстранување.

Член 4

Секое овластено лице, кое има пристап до личните податоци и до информатичко комуникациската опрема на Акдемијата ги има следните обврски и одговорности:

- Должно е да се придржува до сите правила и процедури воспоставени со донесените интерни акти на факултетот;
- Должно е да ги применува сите мерки за физичка безбедност на просториите каде се наоѓа информацискиот систем на факултетот;
- Не смее да ја прекршува превземената обрвска за доверливост, со која се обврзува дека секој податок со кој ќе дојде во текот на работењето во факултетот, а кој спаѓа во категоријата на личен податок согласно прописите за заштита на личните податоци, ќе го чува како доверлив и нема да го пренесува, оддава, ниту на друг начин ќе го стави на располагање на било кое друго лице и во било која форма, надвор од системот на пропишани и воспоставени тенички и

организациски мерки според кои во факултетот се врши обработка на личните податоци;

- Секој инцидент кој ќе го забележи овластеното лице мора до го евидентира во писмена форма од моментот кога е забележан до негова санација;
- Даденото корисничко име и лозинка овластеното лице е должно да го чува и да не го споделува со други лица;
- Овластеното лице со потпишување на договорот за работа е должно да потпише и изјава за тајност и заштита на обработката на личните податоци;
- Овластеното лице при работа со документи кои содржат лични податоци треба да внимава на истите да не ги направи непотребно видливи на трети лица;
- Овластеното лице по престанокот на работното време и за време на паузи и отсуства документите кои содржат лични посатоци треба да ги чува на место на кое што нема да бидат непотребно видливи;

Член 5

Овластените лица задолжително се информираат за техничките и организациските мерки кои се однесуваат на извршување на нивните обрвски и одговорности.

Член 6

Овој правилник влегува со сила со денот на донесување од Наставно – Научниот Совет на Бизис Академија Смилевски

Бизнис Академија Смилевски
Директор:
д-р Маја Кузмановска

Врз основа на член 41-а алинеа 4 од Законот за заштита на личните податоци (Службен весник на Р.М бр.7/05, 103/08, 124/10, 135/11, 43/14, 153/15 и 99/16), Бизнис Академија Смилевски на ден 27.10.2021 година донесе

Правилник
За пријавување, реакција и санирање на инциденти на
Бизнис Академија Смилевски

Член 1

Со овој Правилник се пропишува начинот на пријавување, реакција и санирање на инциденти кои влијаат или можат да влијаат на тајноста и заштитата на личните податоци кои се обработуваат во Бизнис Академија Смилевски (во понатамошен текст:БАС) во својство на контролор.

Член 2

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.

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 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

Член 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 кои мерки треба да се превземат за негово санирање и спречување на негово повторување во иднина.

Доколку се работи за инцидент кој се повторува, администраторот на информацискиот систем е должен да превземе мерки кои ќе гарантираат трајно отстранување на ризикот од неговото повторување.

Член 4

Доколку како последица на инцидентот дојде до губење или бришење на дел или на сите лични податоци содржани во информацискиот систем, истите ќе бидат повторно внесени-вратени во информацискиот систем, со користење на сигурносните копии кој што се чуваат во факултетот и во cloud.

Постапката од став 1 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.

Член 5

При повторно внесување-враќање на личните податоци во системот, 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 или овластените лица врз основа на претходно издадено писмено овластување од страна на Деканот на факултетот.

Член 6

Овој правилник влегува во сила со денот на донесување од Наставничкиот совет на Бизнис Академија Смилевски.

Бизнис Академија Смилевски _____

БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ		

ПРАВИЛНИК
ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ НА БАС

Скопје, октомври 2021

Врз основа на член 36 став (1) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), и чл.10, став (3) од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), Наставно – Научен Совет Бизнис Академија Смилевски , на седницата одржана на ден _____2021 година донесе

ПРАВИЛНИК
ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ
НА Бизнис Академија Смилевски

I. ОПШТИ ОДРЕДБИ

Предмет на уредување
Член 1

Со овој правилник се пропишуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци на БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ (во понатамошниот текст – БАС) во улога на контролор.

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 факултетот;
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 опфаќакоординирана примена на ресурси на факултетот 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 факултетот, 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 факултетот;

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 факултетот, 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 заштитатана 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 факултетот 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 факултетот, 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 факултетот 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 факултетот.

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, факултетот има воспоставено 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:

-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) Факултетот 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 факултетот кој треба да им одговара на природата, обемот и сложеноста на активностите коишто факултетот ги врши при обработката на личните податоци и ризиците на коишто е изложен.

(5) Факултетот 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) Факултетот 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, ги опфаќа:

- хардверот (на пример: сервери, лаптопи, хард дискови и други медиуми);

- софтверот (на пример: оперативни системи и софтверски програми развиени за потребите на факултетот);

- 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, ги опфаќа:

(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).

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

(5) Факултетот 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) Факултетот 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 факултетот.

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, факултетот применува 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.

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

Член 9

(1) Факултетот 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) Факултетот 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) Факултетот 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, факултетот донесува подетални 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 се однесуваат на:

а) План за создавање систем на технички и организациски мерки за обезбедување тајност и заштитана обработката на личните податоци;

б) Правилник за идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);

в) Правилник за техничките и организациските мерки за обезбедување тајност и заштитана обработката на личните податоци соодветно на ризикот; во кои се вклучени и следните правила:

- 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;
- начинот на обезбедување на опремата на факултетот на која се врши обработка на личните податоци;
- начинот на обезбедување на преносливите медиуми;
- начинот на обезбедување на серверите и веб-страницата на факултетот;
- начинот на обработка на личните податоци кои се криптирани;
- физичка безбедност;
- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);

г) Правилник за обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема;

д) План за управување со континуитет на информацискиот систем;
ѓ) Правилник за пријавување, реакција и санирање на инциденти;
е) План за обезбедување на континуитет;
ж) Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
з) Правилник за начинот на уништување и бришење на документите;
ѕ) Правилник за активности за обука и подигнување на свеста на раководството и вработените запривatноста и безбедносните ризици во факултетот;
ј) Правилник за динамика и начин на вршење на периодични контроли, како и процесите за вршење навнатрешна контрола;

(4) Документацијата од ставовите (2) и (3) на овој член, факултетот 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) Факултетот 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 факултетот може да го обезбеди преку:

- информација која единствено овластеното лице ја знае (единствено корисничко име и лозинка за секое овластено лице, при што лозинката е составена од комбинација на најмалку осум алфанумерички карактери букви (мали и големи), симболи, броеви и интерпукциски знаци.

(3) Факултетот 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.

(4) При проверката врз основа на корисничко име и лозинка факултетот 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) Факултетот обезбедува 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, факултетот 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 факултетот, факултетот обезбедува автоматизирано отфрлање од информацискиот систем. Бројот на неуспешни обиди факултетот го определува соодветно на ризикот и природата на работата и работните процеси во однос на обработката на личните податоци, е три последователни неуспешни обиди;

- инсталиран заштитен ѕид (firewall);
- редовно ажуриран антивирусен софтвер; и
-зачувување на податоците на корисниците на серверите на факултетот 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.

(2) Покрај мерките од ставот (1) на овој член, врз основа на спроведената анализа на ризик, доколку се утврди за потребно, факултетот 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 факултетот, со цел откривање дали се загрозени и други елементи;
- безбедносен надзор на софтверот и хардверот што се користи во системот на факултетот;
- ажурирање на софтверските програми кога се идентификуваат и ги коригираат критичните недостатоци;
- 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 факултетот.

Сегрегација на должности и одговорности

Член 13

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

(3) Факултетот 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 факултетот, 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 факултетот.

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, факултетот воспоставува и води евиденција за секој пристап до информацискиот систем logs.

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

(8) Факултетот обезбедува заштита на системот за евиденција за пристап до информацискиот систем, со примена на единствено корисничко име и лозинка на одговорното лице за водење на евиденцијата, од било каков неовластен пристап, особено на лицата чија активност се евидентира на системот за евиденција.

(9) Факултетот 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) Факултетот 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) Факултетот 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 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; и
- мерки за криптирање за заштита на мобилни работни станици и медиуми за мобилно складирање (надворешен хард-диск).

Обезбедување на серверите

Член 18

(1) Факултетот согласно анализата на ризик на врвот на својата листа од аспект на примената на технички и организациски мерки ги има своите сервери на кои се централизира обработката на голема количина на лични податоци. При тоа факултетот ги применува 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 (промена на лозинките по секое заминување на администраторот);
- 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); и
- правење на сигурносни копии и нивна редовна проверка.

Обезбедување на веб-страницата на факултетот

Член 19

(1) Факултетот за својата веб-страница ги применува следните технички мерки:

-имплементација на криптографски протокол (TLS заменувајќи го SSL) на сите веб страници на факултетот (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;

- 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.

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

Член 20

(1) Факултетот 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, кои се опишани во Правилникот за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица на факултетот;

(2) Факултетот 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) Факултетот 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) Факултетот врз основа на анализата на ризик има утврдено 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, факултетот го определува начинот на управување со инциденти кои ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци, кој е опишан во Правилник за пријавување, реакција и санирање на инциденти.

(3) Управувањето со инциденти од ставот (2) на овој член, опфаќа пријавување, реакција и санирање на инцидентите, при што факултетот води Евиденција 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) Факултетот 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) Факултетот обезбедува дека овластените лица 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 (редовно тестирање на функционалноста на уредите).

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

Член 22

(1) Факултетот 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 факултетот усвојува План за обезбедување континуитет (business continuity plan) кој ги предвидува сите можни инциденти (на пример: хардверски инцидент). Факултетот има изработено и Правилник за начинот на правење на сигурносна копија, архивирање и чување, како и повторно враќање на зачуваните лични податоци.

(3) Факултетот 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, прави целосна сигурносна копија (full back-up) еднаш месечно, на начин кој ќе гарантира повторно воспоставување на достапноста до личните податоци во случај на настанат физички или технички инцидент.

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

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

(6)Факултетот 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 (чување на безбедно место на сигурносната копија за кое се применети мерки и контроли кои го минимизираат ризикот од поплава, пожар, кражба и слично).

Начин на архивирање и чување на податоците

Член 23

(1) Факултетот, 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, факултетот 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) Факултетот 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) Факултетот е должен документот од ставот (3) на овој член да го ревидира и усогласува

годишно согласно промените во работењето на факултетот и законскитеуслови за чување на личните податоци.

Управување со преносливи медиуми

Член 24

(1)Факултетот не користи преносливи медиуми (мобилна опрема) на која се врши обработка на личните податоци. Преносливите медиуми ги користи само во случај кога треба да се дадат лични податоци на корисник со законско овластување, при што корисникот ги применува соодветните мерки за заштита на личните податоци според законот за заштита на личните податоци.

Криптирање на личните податоци

Член 25

(1) Кога факултетот 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) Факултетот врши криптирање со зиповање на досиејата (во зип форма, 256 Bit AES – Енкрипција).

Физичка безбедност

Член 26

(1) Факултетот 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 факултетот 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;
- обезбедување безбедност на клучевите и шифрите за аларми кои овозможуваат пристап до просториите;
- воспоставување на правила и методи за контрола на пристапот на посетителите и тоа минимум со придружба од едно лице во факултетот со посетителите надвор од областите за прием на странки;
- посебна физичка заштита на ИТ-опремата преку специфични методи (систем за спречување на пожар, поплави).
-обезбедување дека само овластените лица можат да пристапат до просториите со ограничен пристап.

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 факултетот со прописите за заштита на личните податоци и со донесената документација за технички и организациски мерки.

(2) Информацискиот систем и информатичката инфраструктура на факултетот 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) Факултетот има воспоставено процес за управување при користење на услуги за обработка на личните податоци од страна на обработувачи, 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) Факултетот применува процедура за одлучување за избор на обработувач со која предвидува:

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 факултетот што можат да произлезат при обработката на личните податоци од страна на обработувачите.

Ангажирање на обработувачи

Член 29

(1) Во случај кога факултетот ќе одлучи да пренесе работи од неговиот делокруг на работа поврзани со обработка на лични податоци на обработувачот, обезбедува 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, факултетот 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 факултетот и обработувачот се уредуваат со договор при што факултетот пред да го склучи договорот бара 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 факултетот.

(4) Безбедносната политика од ставот (3) на овој член содржи податоци со кои ќе се гарантира 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 факултетот 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 факултетот; 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) Факултетот обезбедува 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 со корисничко име и лозинка 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 факултетот, 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 факултетот, пред нивното отпочнување со работа се запознаваат со прописите за заштита на личните податоци, како и со донесената документација за технички и организациски мерки.

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

(3) Факултетот 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 во факултетот, 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 факултетот, 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 факултетот.

(7) Факултетот 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 е ограничен само за овластени лица на факултетот.

(2) За пристапувањето до документите задолжително се воспоставени механизми за идентификација на овластените лица со идентификување на логирањата.

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

Правило „чисто биро“

Член 33

Факултетот 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 се врши на начин така што се применуваат соодветни механизми (се чуваат заклучени во плакар) за попречување на секое неовластено отворање.

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, факултетот ќе 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 факултетот 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 се сместени во простории, заклучени со синџир, катанец или клуч. Просториите се заклучени и за време на периодот кога документите не се обработуваат од овластените лица.

IV. ВИСОКО НИВО

1. Технички мерки

Дополнителни мерки

Член 37

Факултетот 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 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 (криптирање) за да се спречи неовластено обработување на личните податоци снимени на нив.

Тестирање на информацискиот систем

Член 41

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

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

Пренесување на медиуми

Член 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.

1. Организациски мерки

Пренесување на документи

Член 46

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

V. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

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 на Ветеринарен Факултет – Битола (бр. 01-174/1), 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 со денот на донесувањето од страна на Наставно – Научниот Совет на Ветеринарен Факултет Битола.

Бизнис Академија Смилевски

Директор:
Д-р Маја Кузмановска