

**АНАЛИЗА НА ЦЕЛТА, ОДНОСНО ЦЕЛИТЕ ЗА КОЈА/КОИ СЕ ПОСТАВУВА
ВИДЕОНАДЗОР 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 90 став (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 е обврска согласно друг закон (со образложение)	Не, само Законот за заштита на личните податоци
4.	Опис на недвижните и движните ствари, односно простор кои ќе сезаштитираат со поставувањето на видеонадзорот	- 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 заради кои 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 категории на 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 привилегија за 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 лица кои ќе имаат пристап до видеонадзорот	Лица вработени во контролорот, односно обработувачот (овластеното лице), 1 лице.
17.	Информации за предвидена обука за заштита 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 and by 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 камери кои 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 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.)	Само еден контролор
23.	Период до кога ќе се донесе акт во којшто ќе се уреди начинот на вршење на видеонадзорот	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 ВИДЕОНАДЗОР 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 ставаат 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 објектот 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	
---------	----------	---

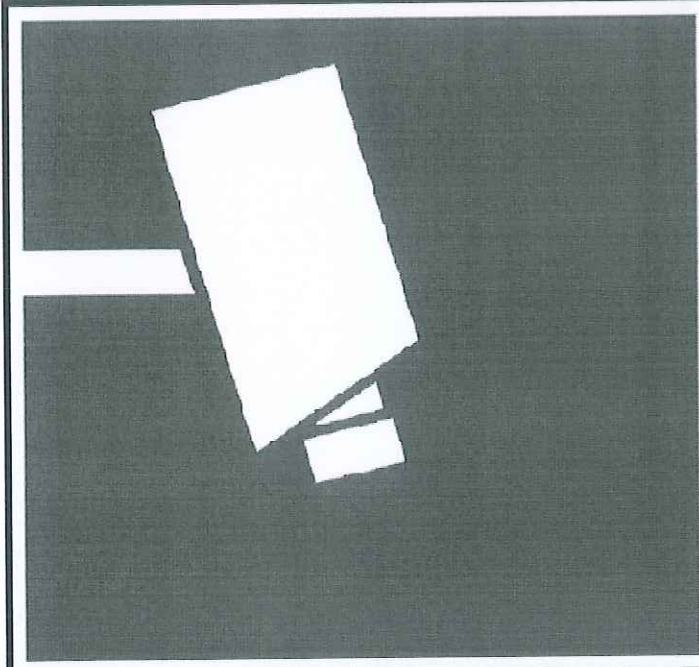
6. Одлука на функционерот, или на одговорното лице за воспоставување на систем за видеонадзор (дадено врз основа на анализата за: потребата од воспоставување на видеонадзор, степенот на влијание врз приватноста на субјектите на лични податоци кои ќе бидат опфатени со видеонадзорот – лица кои ќе се снимаат, 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

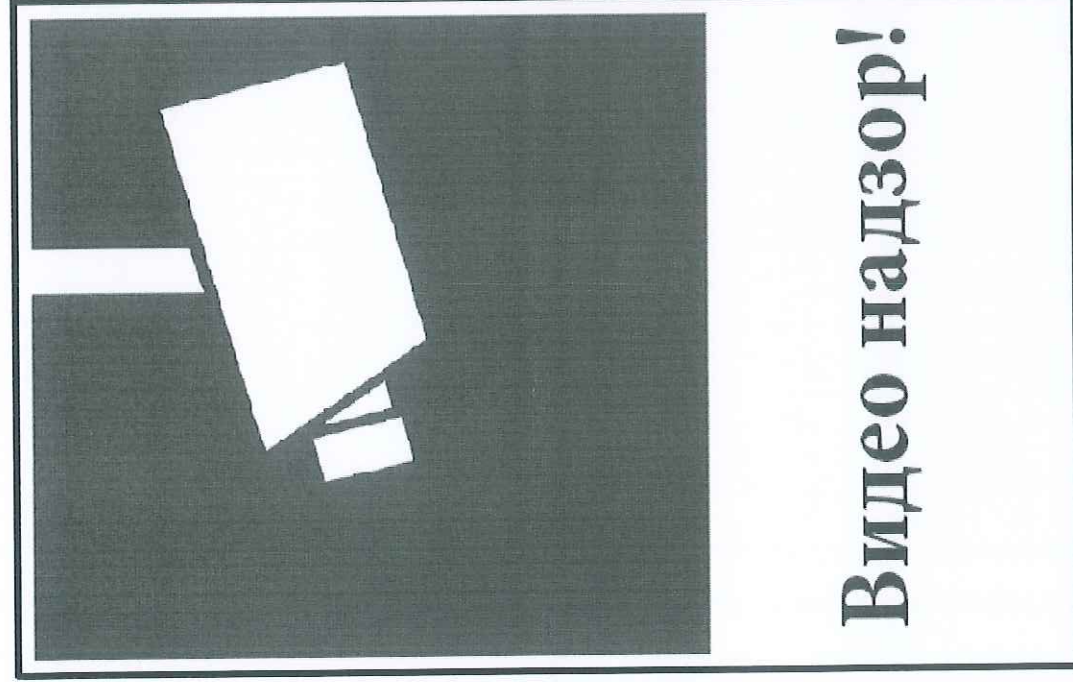
Контакт информациите за офицерот за заштита на личните податоци
(доколку е определен): тел.072/252-603,
e-mail: biljana.galovska@bas.edu.mk

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



Дополнителни информации ќе најдете:

- Преку известување
- На пријавница/ рецепција/ инфо пулт
- На интернет (www)...

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

Контакт информации:

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

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

Цел, односно цели за вршење на видео надзорот:

Права на субјектите на лични податоци: Како субјект на личните податоци можете да остварите повеќе права, особено право да пристапите или да барате да се избришат вашите лични податоци.

Повеќе детали за видео надзорот и за вашите права може да најдете од информациите наведени од контролорот преку опциите наведени во левиот агол.

¹ Забелешка: Информациите мора да бидат бесплатни, во транспарентна, разбирлива и лесно достапна форма, напишана на едноставен јазик. Ова известување

ЕВИДЕНЦИЈА

За нарушување на безбедноста на личните податоци

[illegible]

Дата:

Одговорно лице:

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:

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

Дата:

Одговорно лице:

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:

**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 ќе имаат пристап до видеонадзорот.
15.	Потреба од континуирана обука на овластените лица (предлог тема на обуката, број на лица што треба да бидат обучени)	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 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

Бр. 0302-257/140
27.10. 2021 год.
СКОПЈЕ

ИЗЈАВА ЗА ПРИВАТНОСТ ПРИ ВРШЕЊЕ НА ВИДЕОНАДЗОР

Оваа Изјава за приватност го објаснува видот на лични податоци што [кликнете тука](#) за да го внесете текстот. (во натамошниот текст: Контролор), ги собира од вас при посета на службените/деловните простории и како Контролорот ги користи овие податоци.

1. Зошто собираме (обработуваме) лични податоци?

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

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

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

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

Камерите за видеонадзор се инсталираат на [кликнете тука](#) за да го внесете текстот. и се поставени и фокусирани така што се снимаат само лица кои ќе пристапат до службените/деловните простории (објекти), вклучително и имотот (на пример за паркирање).

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

2. Какви податоци собира Контролорот?

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

3. Кој е одговорен за обработка на податоците?

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

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

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

- заштита на животот или здравјето на луѓето;
- заштита на сопственоста;
- заштита на животот и здравјето на вработените поради природата на работата; или
- обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории.

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

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

5. Кој може да ги види моите лични податоци?

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

6. Како да ги контролирате вашите податоци?

Може да испратите барање на кликнете тука за да го внесете текстот. (на пример: е-пошта на кликнете тука за да ја внесете @., адреса кликнете тука за да го внесете текстот.).

7. Мојам ли да пристапам до моите податоци?

Вие имате право да пристапите до вашите податоци во секое време и бесплатно, со испраќање на барање до [кликнете тука](#) за да го внесете текстот., или преку е-пошта до: [кликнете тука](#) за да ја внесете @..

8. Мојам ли да ги менувам моите податоци?

Не е дозволено изменување на видео записот за видеонадзор.

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

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

10. Дали можам да ги избришам моите податоци?

Вие имате право да ги избришете вашите податоци во секое време со испраќање на барање на [кликнете тука](#) за да го внесете текстот. (на пример: е-пошта на [кликнете тука](#) за да ја внесете @., адреса [кликнете тука](#) за да го внесете текстот..), кога обработката е незаконска.

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

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

12. Дали имам право на приговор?

Да, имате право на приговор и да се спротивставите на обработката во кое било време со испраќање на барање на [кликнете тука](#) за да го внесете текстот. (на пример: е-пошта на [кликнете тука](#) за да ја внесете @., адреса [кликнете тука](#) за да го внесете текстот..), кога имате легитимни причини во врска со вашата конкретна ситуација. Контролорот ќе постапи по вашето барање во рок од 15 дена од денот на поднесување на барањето.

13. Што можам да направам во случај на проблем?

а) Првиот чекор е да го известите Контролорот со испраќање е-пошта до [кликнете тука](#) за да ја внесете @. и да побарате да преземе акција.

б) Вториот чекор, ако не добиете одговор од нас или ако не сте задоволни од тоа, контактирајте со нашиот офицер за заштита на личните податоци на [кликнете тука](#) за да ја внесете @..

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

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

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

15. Безбедност на личните податоци

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

16. Колку долго ги чуваме вашите податоци?

Контролорот ќе ги чува вашите лични податоци [кликнете тука](#) за да го внесете текстот. календарски денови по вашата посета во нашите простории, по што сите снимени видеозаписи автоматски се бришат.

Бр. 0302-257/140
27.10. 2021 год.
СКОПЈЕ

ИЗЈАВА ЗА ПРИВАТНОСТ ПРИ ВРШЕЊЕ НА ВИДЕОНАДЗОР

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

1. Зошто собираме (обработуваме) лични податоци?

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

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

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

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

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

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

2. Какви податоци собира Контролорот?

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

3. Кој е одговорен за обработка на податоците?

Контролорот е субјект кое ја врши обработката на личните податоци и кое ги утврдува целите на обработка, единствено во согласност со Законот за заштита на личните податоци. Покрај тоа, [кликнете тука](#) за да го внесете текстот, е лице за контакт и одговорно за видеонадзорот.

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

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

- заштита на животот или здравјето на луѓето;
- заштита на сопственоста;
- заштита на животот и здравјето на вработените поради природата на работата; или
- обезбедување на контрола над влегувањето и излегувањето од службените или деловните простории.

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

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

5. Кој може да ги види моите лични податоци?

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

6. Како да ги контролирате вашите податоци?

Може да испратите барање на [кликнете тука](#) за да го внесете текстот. (на пример: е-пошта на [кликнете тука](#) за да ја внесете @., адреса [кликнете тука](#) за да го внесете текстот.).

7. Мојам ли да пристапам до моите податоци?

Вие имате право да пристапите до вашите податоци во секое време и бесплатно, со испраќање на барање до [кликнете тука](#) за да го внесете текстот., или преку е-пошта до: [кликнете тука](#) за да ја внесете @.

8. Можам ли да ги менувам моите податоци?

Не е дозволено изменување на видео записот за видеонадзор.

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

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

10. Дали можам да ги избришам моите податоци?

Вие имате право да ги избришете вашите податоци во секое време со испраќање на барање на [кликнете тука](#) за да го внесете текстот. (на пример: е-пошта на [кликнете тука](#) за да ја внесете @., адреса [кликнете тука](#) за да го внесете текстот.), кога обработката е незаконска.

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

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

12. Дали имам право на приговор?

Да, имате право на приговор и да се спротивставите на обработката во кое било време со испраќање на барање на [кликнете тука](#) за да го внесете текстот. (на пример: е-пошта на [кликнете тука](#) за да ја внесете @., адреса [кликнете тука](#) за да го внесете текстот.), кога имате легитимни причини во врска со вашата конкретна ситуација. Контролорот ќе постапи по вашето барање во рок од 15 дена од денот на поднесување на барањето.

13. Што можам да направам во случај на проблем?

а) Првиот чекор е да го известите Контролорот со испраќање е-пошта до [кликнете тука](#) за да ја внесете @. и да побарате да преземе акција.

б) Вториот чекор, ако не добиете одговор од нас или ако не сте задоволни од тоа, контактирајте со нашиот офицер за заштита на личните податоци на [кликнете тука](#) за да ја внесете @.

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

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

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

15. Безбедност на личните податоци

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

16. Колку долго ги чуваме вашите податоци?

Контролорот ќе ги чува вашите лични податоци [кликнете тука](#) за да го внесете текстот. календарски денови по вашата посета во нашите простории, по што сите снимени видеозаписи автоматски се бришат.

Бр. 0302-257/1-10
27.10. 2021 год.
СКОПЈЕ

ИЗЈАВА
ЗА ПРИВАТНОСТ ПРИ ВРШЕЊЕ НА ВИДЕОНАДЗОР
НА БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ

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

1. Зошто собираме (обработуваме) лични податоци?

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

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

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

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

Камерите за видеонадзор се инсталираат на DVR снимач со хард диск и се поставени и фокусирани така што се снимаат само лица кои ќе пристапат до службените/деловните простории (објекти)

Системот со видеонадзор ја опфаќа областа на: влезот на факултетот, 4 камери во ходниците на факултетот

2. Какви податоци собира Контролорот?

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

3. Кој е одговорен за обработка на податоците?

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

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

Контролорот користи опрема за видеонадзор за: заштита на животот или здравјето на луѓето;

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

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

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

5. Кој може да ги види моите лични податоци?

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

6. Како да ги контролирате вашите податоци?

Може да испратите барање на Бизнис Академија Смилевски - Битола

Можам ли да а). пристапам до моите податоци?

Вие имате право да пристапите до вашите податоци во секое време и бесплатно, со испраќање на барање до БАС.

7. Мојам ли да ги менувам моите податоци?

Не е дозволено изменување на видео записот за видеонадзор.

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

Вие имате право да ја ограничите обработката на вашите лични податоци во секое време со испраќање на барање на Бизнис Академија Смилевски ,кога ја оспорувате точноста на вашите лични податоци, или кога на Контролорот повеќе не му се потребни податоците за извршување на неговите задачи. Вие исто така можете да ја блокирате обработка и кога работењето е незаконско и вие се спротивставувате на бришење на податоците. Сепак, блокирањето не е можно во секој случај на службена истрага.

9. Дали мојам да ги избришам моите податоци?

Вие имате право да ги избришете вашите податоци во секое време со испраќање на барање на Бизнис Академија Смилевски кога обработката е незаконска.

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

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

11. Дали имам право на приговор?

Да, имате право на приговор и да се спротивставите на обработката во кое било време со испраќање на барање Бизнис Академија Смилевски кога имате легитимни причини во врска со вашата конкретна ситуација. Контролорот ќе постапи по вашето барање во рок од 15 дена од денот на поднесување на барањето.

12. Што мојам да направам во случај на проблем?

а) Првиот чекор е да го известите Контролорот со испраќање е-пошта studentkaslužba@bas.edu.mk и да побарате да преземе акција.

б) Вториот чекор, ако не добиете одговор од нас или ако не сте задоволни од тоа, контактирајте со нашиот офицер за заштита на личните податоци на biljana.galovska@bas.edu.mk

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

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

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

14. Безбедност на личните податоци

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

15. Колку долго ги чуваме вашите податоци?

Контролорот ќе ги чува вашите лични податоци 30 календарски денови по вашата посета во нашите простории, по што сите снимени видеозаписи автоматски се бришат.

Бизнис Академија Смилевски

директор:
д-р Маја Кузмановска



[Handwritten signature in blue ink]

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
БИЗНИС АКАДЕМИЈА СМИЛЕВСКИ - БАС

Бр. 0302-257/1-11
28.10. 2021 год.
СКОПЈЕ

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 ефективната 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 процената 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 процената 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 личните податоци;

(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;

(ф) 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 на личните 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



Maia

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): Персонален компјутер (два) и надворешен хард диск; 2. Софтвер (оперативни системи и софтверски програми развиени за потребите на контролорот): Оперативен систем Windows 10; Софтверски програми: Office, софтвер за плата и софтвер за финансиско и материјално работење -Metex; 3. Комуникациски канали (оптички кабли, интернет, безжична мрежна технологија – Wi-Fi): оптички кабли, интернет – A1, Електронска евиденција за студентите (iknow.uklo.edu.mk), безжична мрежна технологија – Wi-Fi ; и 4. Документи во хартиена форма: Досиеја на вработени; Матична книга на запишани студенти; Главна книга на дипломирани студенти; Досиеја на студенти.
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.	1. / 2. / 3. / 4. /
3.	Идентификување на изворите на ризик кои што може да бидат 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).	1. / 2. / 3. / 4. /
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:	1. / 2. / 3. / 4. /

	- 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 (скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална).	

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): Персонален компјутер (два) и надворешен хард диск; 2. Софтвер (оперативни системи и софтверски програми развиени за потребите на контролорот): Оперативен систем Windows 10; Софтверски програми: Office, софтвер за плата и софтвер за финансиско и материјално работење -Metex; 3. Комуникациски канали (оптички кабли, интернет, безжична мрежна технологија – Wi-Fi): оптички кабли, интернет – A1, Електронска евиденција за студентите (iknow.uklo.edu.mk), безжична мрежна технологија – Wi-Fi ; и 4. Документи во хартиена форма: Досиеја на вработени; Матична книга на запишани студенти; Главна книга на дипломирани студенти; Досиеја на студенти.
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.	1. / 2. / 3. / 4. /
3.	Идентификување на изворите на ризик кои што може да бидат 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).	1. / 2. / 3. / 4. /
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:	1. / 2. / 3. / 4. /

	- 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 (скала што може да се користи за проценка: занемарлива, умерена, значајна и максимална).	

ПРАШАЛНИК

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

Бр.	Постапка на Процена на ризици	Хардвер (сервери, лаптопи, хард дискови и други медиуми)	Софтвер (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)
1.	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.				
2.	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 информациониот систем, овластеното лице, надворешниот напаѓач, конкурент), како и				

	Другите внатрешни и надворешни извори (на пример: вода, опасни материјали, пожар, вирус).				
3.	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.).				
4.	Утврдување на постојни или планирани мерки што овозможуваат решавање на секој ризик (на пример: контрола на				

	пристап, сигурносни копии, информацијска ревизорска трага, безбедност на просториите, криптирање или анонимизација).				
5.	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).				

**Известување на субјектот на личните податоци
за нарушување на безбедноста на личните податоци**

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

Место., кликнете на стрелката за да го внесете датумот.

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

Кликнете тука за да го внесете името и презимето.

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

1.	Назив и седиште на контролорот	Кликнете тука за да внесете назив на контролорот. Кликнете тука за да внесете седиште.
2.	Опис на природата на нарушувањето на безбедноста на личните податоци, вклучувајќи, категориите и приближниот број на засегнати субјекти на личните податоци, како и категориите и приближниот број на засегнати евидентирани лични податоци	Кликнете тука за да го внесете текстот.
3.	Име, презиме и контакт податоци на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации	Кликнете тука за да внесете име и презиме. Кликнете тука за да внесете контакт податоци.
4.	Опис на можните последици од нарушувањето на безбедноста на личните податоци	Кликнете тука за да го внесете текстот.
5.	Опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти	Кликнете тука за да го внесете текстот.
6.	Датум и време на инцидентот (доколку се знае, во спротивно може да се направи проценка)	Кликнете на стрелката за да го внесете датумот и времето.
7.	Датум и време на детектирање на инцидентот	Кликнете на стрелката за да го внесете датумот и времето.
8.	Услови под кои што е настанато нарушувањето на безбедноста на личните податоци	Кликнете тука за да го внесете текстот.
9.	Име, презиме и потпис на лицата кои констатирале нарушување на безбедноста на личните податоци	Име Презиме Име Презиме Име Презиме Име Презиме Име Презиме Име Презиме Име Презиме

10.	Дали во инцидентот е вклучен и обработувачот, при што ако е вклучен, се наведуваат и неговите податоци (назив и седиште, односно име и презиме и адреса на живеење, податоци за офицерот за заштита на личните податоци и други контакт податоци)	Кликнете тука за да го внесете текстот.
11.	Дали е информиран офицерот за заштита на личните податоци на контролорот за нарушувањето на безбедноста на личните податоци	Кликнете тука за да го внесете текстот.
12.	Оценка/мислење од офицерот за заштита на личните податоци преку преземени или предложени мерки за справување со нарушувањето на безбедноста на личните податоци	Кликнете тука за да го внесете текстот.
13.	Сумарен преглед на нарушувањето на безбедноста на личните податоци (вклучително физичка локација и медиум на кој се складирали податоците)	Кликнете тука за да го внесете текстот.
14.	Статистички податоци за нарушување на безбедноста на личните податоци, односно констатирање дали инцидентот првпат се појавува	Кликнете тука за да го внесете текстот.
15.	Известување до субјектот на личните податоци – ДА/НЕ	Кликнете на стрелката за да одберете една од опциите.
16.	Содржина на известувањето до засегнатите субјекти на лични податоци	Кликнете тука за да го внесете текстот.
17.	Комуникациска технологија преку која е испратено известувањето	Кликнете тука за да го внесете текстот.
18.	Број на субјекти на лични податоци што се известени	Кликнете тука за да го внесете текстот.
19.	Други податоци на контролорот, доколку ги има за настанатиот случај	Кликнете тука за да го внесете текстот.

Место., кликнете на стрелката за да го внесете датумот.

Име, презиме и потпис на функционерот, односно одговорното лице во Контролорот
Кликнете тука за да го внесете името и презимето.
