ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - ГАБРОВО

УТВЪРЖДАВАМ: /П/
проф. дтн инж. Р. Иларионов
Ректор на ТУ-Габрово

ВЪТРЕШНИ ПРАВИЛА

за оценка на въздействието

върху защитата на личните данни

в Технически университет-Габрово

2019 г.

Габрово

СЪДЪРЖАНИЕ:

Глава първа ОБЩИ ПОЛОЖЕНИЯ 3
Глава втора ОЦЕНКА НА РИСКА ПРИ ОБРАБОТКА НА ЛИЧНИТЕ ДАННИ.....3
Глава трета ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ 4
Глава четвърта ПРЕДВАРИТЕЛНА КОНСУЛТАЦИЯ 5
Глава пета ЗАДЪЛЖЕНИЯ И РОЛИ 6
Преходни и заключителни разпоредби.....6
Приложение 1 7

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите Вътрешни правила уреждат реда и критериите за оценка на риска при обработване на лични данни и за оценката на въздействието върху защитата на личните данни в Технически университет-Габрово (ТУ-Габрово).

(2) Настоящите Вътрешни правила са разработени на основание на:

1. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), наричан по-нататък Регламент (ЕС) 2016/679;
2. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент 2016/679 (Насоките);
3. Закон за защита на личните данни;
4. Вътрешни правила за защита на лични данни в Технически университет-Габрово - чл. 37, ал. 2.

(3) Настоящите Вътрешни правила се отнасят и при обработката на личните данни в Технически колеж-Ловеч (ТК-Ловеч), като основно звено в структурата на ТУ-Габрово и в Университетски център за научни изследвания и технологии (УЦНИТ).

Чл. 2. ТУ-Габрово е администратор на лични данни и като такъв има задължение за извършване на Оценката на въздействието върху защитата на данни (ОВЗД).

Глава втора
ОЦЕНКА НА РИСКА ПРИ ОБРАБОТКА НА ЛИЧНИТЕ ДАННИ

Чл. 3. (1) При започването на всяка нова дейност или проект Ръководителят на съответната дейност/проект заедно с длъжностното лице по защита на данните извършват оценка на риска, като вземат предвид вида на личните данни и начините за обработването им.

(2) Преглед за необходимостта от извършване на оценка на въздействието се прави и при всяка промяна в риска, с който са свързани вече съществуващи операции по обработване.

(3) Ректорът на ТУ-Габрово определя със заповед извършването на оценка на риска.

(4) Оценката на риска се ръководи от длъжностното лице по защита на данните.

(5) За идентифициране на рисковете свързани със защитата на личните данни длъжностното лице по защита на данните изготвя риск-регистър, които попълва съвместно с Ръководителя на съответната дейност/проект.

Чл. 4. (1) При извършването на оценка на риска се използва Матрица за определяне нивото на риска ***Приложение № 1***, където нивото на риска се определя от комбинация на вероятността за настъпване на съответното нарушение на сигурността на данните и въздействието.

(2) При оценка на риска се определят 3 нива на риска – нисък, среден и висок.

Чл. 5. (1) При определянето на степента на риска се вземат:

1. критериите за вероятен „висок риск“ на чл. 34, параграф 3 от Регламент (ЕС) 2016/679 и дадените примери в Насоките за начина на използване на критериите, за да се оцени дали конкретна операция по обработване изисква ОВЗД;
2. наред с преките рискове за правата и свободите на физическите лица, произтичащи от обработката на лични данни се отчитат и рисковете за цялостния управленски процес (репутационни, правни и т.н.), както и целите и задълженията на самата организация (регулаторни и договорни).

(2) Водещ критерий при преценката нивата на рисковете за правата и свободите на субектите на данни е степента (нивото) на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица. В съответствие с това се анализира вероятността за възникване на нарушение на сигурността на данните.

(3) Определят се 3 нива на въздействие – ниско, средно и високо.

Чл. 6. (1) В зависимост от определеното ниво на въздействие се:

1. извършва приоритизация на идентифицираните рискове в зависимост от резултатите от оценката им;

2. определя адекватно ниво на защита, включващо техническите и организационни мерки, които трябва да предприеме за тяхното ограничаване.

(2) Редът на приоритет на идентифицираните рискове е, както следва:

1. Високите рискове трябва да бъдат напълно избегнати или ограничени чрез прилагане на мерки за сигурност, които намаляват както въздействието, така и тяхната вероятност. В плана за управление на рисковете се предвиждат мерки за предотвратяване, защита и възстановяване.

2. Средните рискове трябва да бъдат избегнати или ограничени чрез прилагане на мерки за сигурност, които намаляват както въздействието, така и тяхната вероятност. Приоритетно се предвиждат мерки за предотвратяване и възстановяване.

3. Ниските рискове могат да бъдат третирани на по-късен етап още повече, че прилагането на мерките спрямо рисковете с по-висок приоритет може да доведе до тяхното елиминиране или значително ограничаване.

Чл. 7. В зависимост от приоритизацията на рисковете и идентифицираното ниво на въздействие се определя съответно ниво на защита – ниско, средно или високо, както и организационните и технически мерки, адекватни на така определеното ниво.

Чл. 8. (1) Риск-регистърът по чл. 3, ал. 5 е основание за вземане на решение, за необходимостта от извършване на ОВЗД.

(2) Ректорът на ТУ-Габрово, по предложение от длъжностното лице по защита на данните, взема решение за извършване на ОВЗД.

Глава трета
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Чл. 9. (1) Оценката на въздействието върху защитата на данни (ОВЗД) е процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност, да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработване на лични данни, като ги оцени и определи мерки за справяне с тези рискове.

(2) При извършване на ОВЗД се иска становище на длъжностното лице по защита на данните.

Чл. 10. (1) Когато съществува вероятност определен вид обработване, да породи висок риск за правата и свободите на физическите лица преди да бъде извършено обработването се извършва ОВЗД.

(2) ОВЗД се изисква в следните случаи:

1. когато се извършва систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

2. при мащабно обработване на „чувствителни“ лични данни или на лични данни за присъди и нарушения;

3. при систематично мащабно наблюдение на публично достъпна зона.

(3) ОВЗД се изисква и за видовете операции по обработване, посочени в списък, приет и оповестен от Комисията за защита на личните данни (КЗЛД).

(4) По предложение на длъжностното лице за защита на данните и решение на Ректора на ТУ-Габрово ОВЗД може да бъде направена и при отсъствие на условията по ал. 2 и ал. 3.

Чл. 11. ОВЗД трябва да съдържа най-малко следното:

1. опис на предвидените операции по обработване и целите на обработването;
2. оценка на необходимостта и пропорционалността на операциите по обработване;
3. оценка на рисковете за правата и свободите на субектите на данни;
4. мерките, предвидени за справяне с рисковете, включително гаранциите;
5. мерките за сигурност и механизмите за осигуряване на защитата на личните данни;
6. демонстриране спазването на Регламент (ЕС) 2016/679.

Чл. 12. (1) Избраната методология за извършване на ОВЗД, трябва да е в съответствие с критериите посочени в Приложение 2 от Насоките относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск" за целите на Регламент 2016/679.

(2) ОВЗД може да е свързана само с една единствена операция по обработване на данни или в една ОВЗД може да бъде разгледан набор от сходни операции по обработването, които представляват сходни високи рискове.

(3) Длъжностното лице по защита на данните взема решение кои процеси да се оценяват самостоятелно и кои да се групират.

Чл. 13. (1) За извършване на ОВЗД длъжностното лице по защита на данните изготвя Въпросник за ОВЗД, който попълва съвместно с Ръководителя на съответната дейност/проект.

(2) След попълване на Въпросника за ОВЗД и неговият анализ се изготвя списък на ключовете рискове за сигурността по отношение на инцидентно или злонамерено унищожаване, загуба, промяна, неоторизиран достъп или разкриване на лични данни.

(3) След установяване на ключовите рискове и тяхното приоритизиране длъжностното лице по защита на данните формулира мерки и съставя план за тяхното смекчаване, в който се описват:

1. предпазни мерки, които следва да се предприемат;
2. отговорник по прилагане на мерките;
3. срокове за изпълнение.

(4) След прилагане на взетите мерки длъжностното лице по защита на данните документира резултата от изпълнението.

(5) Ректорът на ТУ-Габрово одобрява ОВЗД за всяка подлежаща на оценка на въздействието дейност/проект по обработка на лични данни.

Чл. 14. (1) ОВЗД може да бъде публикувана в сайта на ТУ-Габрово, като резюме или заключението от нея.

(2) Ректорът на ТУ-Габрово взема решение за това дали да бъде публикувана или не ОВЗД.

Глава четвърта
ПРЕДВАРИТЕЛНА КОНСУЛТАЦИЯ

Чл. 15. (1) Задължителна предварителна консултация с Комисията за защита на личните данни (КЗЛД) е необходима, когато:

1. оценката на въздействието върху защитата на данните покаже, че предвиденото обработване ще породи висок риск за субектите на данни; и
2. ТУ-Габрово не може да идентифицира адекватни мерки за ограничаване и контрол на риска.

(2) Предварителна консултация може да не бъде проведена, ако ТУ-Габрово счете, че идентифицирания риск може да бъде смекчен с разумни средства по отношение на наличните технологии и разходите за изпълнение.

Чл. 16. При консултация по чл. 15 ТУ-Габрово предоставя на КЗЛД:

1. информация за съответните отговорности, като администратор, за съвместните администратори и за обработващите лични данни, които се занимават с обработването, в случай че е приложимо;
2. целите на планираното обработване и средствата за него;
3. предвидените мерки и гаранции за защита на правата и свободите на субектите на данни;
4. координатите за връзка на длъжностното лице по защита на данните;
5. копие от Оценката на въздействието върху защитата на данните;
6. всякаква друга информация, поискана от КЗЛД.

Глава пета
ЗАДЪЛЖЕНИЯ И РОЛИ

Чл. 17. Ръководителите на основните и структурни звено заедно с длъжностното лице по защита на данните споделят отговорността за вземането на подходящи мерки за ограничаване на всички рискове, идентифицирани в процеса на оценка на въздействието, като и за вземането на последващо решение за започване, респ. продължаване на обработката.

Чл. 18. Лицата, ръководещи отделните процеси по обработка на данните в ТУ-Габрово, са отговорни за своевременното известяване на длъжностното лице по защита на данните и за съвместното вземане на решения във връзка с възникнали рискове за сигурността на личните данни.

Чл. 19. В случай, че обработването на лични данни се извършва изцяло или частично от обработващ лични данни, то обработващия лични данни подпомага ТУ-Габрово при извършването на ОВЗД.

Преходни и заключителни разпоредби

§ 1. За всички неуредени въпроси в настоящите Вътрешни правила се прилагат разпоредбите на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) и Закона за защита на личните данни.

§ 2. Настоящите Вътрешни правила са приети с решение на Академичния съвет на ТУ - Габрово (Протокол № 7 от 11.04.2019 г.).

Приложение 1

Матрица за определяне нивото на риска

		Въздействие от риска		
		Ниско	Средно	Високо
Вероятност от риск	Висока	Среден Риск	Висок Риск	Висок Риск
	Средна	Нисък Риск	Среден Риск	Висок Риск
	Малка	Нисък Риск	Нисък Риск	Среден Риск