ТРАКИЙСКИ УНИВЕРСИТЕТ
СТАРА ЗАГОРА

МЕТОДОЛОГИЯ ЗА ОЦЕНКА НА РИСКА ПРИ ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Утвърдил:

доц. д-р Добри Ярков
Ректор на Тракийски университет

1. ЦЕЛИ

- Дефиниране на методиката за оценка на риска за притежаваните от Университета лични данни, по отношение гарантиране сигурността им.
- Осигуряване на адекватна защита на конфиденциалността, целостта и наличността на личните данни, администрирани от организацията.

2. ОБХВАТ

Методологията обхваща целия процес по оценка на риска на ЛД, администрирани от Университета, попадащи в обхвата на Общия регламент за защита на данни /ОРЗД/GDPR/

3. ОТГОВОРНОСТИ

Настоящата методология се прилага от ръководителите на отделите и звената в ТрУ, членовете на работна група по защита на ЛД и DPO.

4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

- Организацията – Тракийски университет – Стара Загора
- DPO – Data Protection Officer /Длъжностно лице по защита на личните данни/
- DPIA – Data Privacy Impact Assessment /Оценка на Въздействието върху Защитата на Данните/
- ЛД – Лични данни
- GDPR – General Data Protection Regulation /Общ регламент за защита на данните/
- Работна група по защита на ЛД

5. ДЕЙСТВИЯ И МЕТОДИ

5.1. ИЗВЪРШВАНЕ НА ПЪВОНАЧАЛНА ОЦЕНКА

Съгласно GDPR не се изисква DPIA за всяка операция по обработване на ЛД, която може да породи рискове за правата и свободите на физическите лица. Извършването на DPIA е задължително, само когато съществува вероятност обработването да породи висок риск за правата и свободите на физическите лица. Това е от особено значение, когато се въвежда нова технология за обработване на данни. В случай, че не е ясно дали се изисква DPIA, препоръчително е такава да бъде направена.

Обстоятелства, които биха породили необходимост да се извърши DPIA са:

- 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 физическите лица или по подобен начин сериозно засягат субектите на данни. Това може да включва анализиране и прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили;
- Обработване в голям мащаб на чувствителни ЛД;
- Систематично, мащабно наблюдение на публично достъпни зони.

Така посочените обстоятелства не са изчерпателни, възможно е да съществуват и други операции, които не са включени в този списък, които да пораждат сходен висок риск. При планиране на такива операции, те следва да подлежат на DPIA.

Първоначалната оценка на риска се извършва от ръководителя на отдела, инициращ внедряването на новия процес или промяната на вече съществуващ такъв, като при необходимост търси съдействие от DPO и/или други служители/отдели в Университета.

За да се прецени, дали дадена операция или набор от операции по обработването изисква DPIA, следва да се вземат под внимание следните критерии:

- Оценка или точкуване;
- Автоматизирано вземане на решения с правни последици или подобни сериозни последици за субекта на ЛД;
- Систематично наблюдение;
- Чувствителни данни или данни от изключително лично естество;
- Мащабно обработване на данни;
- Търсене на съвпадения или съчетаване на набори от данни;
- Данни относно уязвими субекти на данни;
- Иновативно използване или прилагане на нови технологични или организационни решения;
- Операциите сами по себе си възпрепятстват субектите на ЛД да упражняват дадено право или да използват някоя услуга или договор.

За идентифицирането на тези критерии, следва да се даде отговор на следните въпроси от собственика на информацията (ръководителя на отдела, инициирал процеса):

Процесът ще включва ли оценка, профилиране или прогнозиране на аспекти, имащи отношение към резултатите в работата на субектите на ЛД, тяхното здраве, икономическо състояние, лични предпочитания или интереси, благонадеждността или поведението им, местоположението или движенията им?	ДА/НЕ При отговор “ДА“, моля посочете подробности.

Процесът ще включва ли автоматизирано вземане на решения, които имат правни последици за физическите лица или ги засягат сериозно по подобен начин?	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът ще включва ли обработване, чрез систематично наблюдение, което се използва за мониторинг или контрол на субектите на данни, които се събират чрез мрежи, или чрез систематично, мащабно наблюдение на публично достъпни зони?	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът ще включва ли обработването на чувствителни данни или данни от изключително лично естество, като: • Расов или етнически произход; • Здравословно състояние; • Полов живот или сексуална ориентация; • Политически възгледи; • Религиозни или философски убеждения; • Членство в синдикални организации; • Биометрични и генетични данни използвани единствено с цел идентифицирането на субектите на ЛД; • Финансови данни, като данни за банкови сметки, кредитни • карти и др.; • Данни за съдимост.	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът ще включва ли мащабно обработване на данни? За идентифициране на обработването, като мащабно, могат да се използват следните критерии: • Брой на засегнатите субекти, като конкретна цифра или като • дял от съответното население; • Обемът на данните и/или обхватът на различните видове • данни, които се обработват; • Продължителността или непрекъснатостта на дейността по • обработване на данните; • Географски обхват на дейността по обработване.	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът включва ли търсене на съвпадение или съчетаване на набори от данни, например с произход от две или повече операции по обработването на данни, извършени за различни цели и/или от различни администратори, по начин, който надхвърля разумните очаквания на субекта на ЛД?	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът включва ли обработването на данни относно уязвими субекти?	ДА/НЕ

Тук се включват физически лица, които може да не са в състояние лесно да се съгласят или да възразят срещу обработването на техните ЛД (напр.: деца, възрастни или болни хора).	При отговор "ДА", моля посочете подробности.
Процесът предвижда ли използването или прилагането на нови технологични или организационни решения, включващи, като например съчетаване на използването на пръстови отпечатъци и разпознаване на лицата с цел подобряване на контрола за физически достъп?	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът ще включва ли операции, които сами по себе си възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор? Пример за това са справките извършвани от банки в референтна база данни за кредити, с цел предложение или отказ на услуга.	ДА/НЕ При отговор "ДА", моля посочете подробности.
Процесът ще включва ли трансфер на ЛД в държави извън ЕС, които не са определени от Европейската комисия, като имащи адекватно ниво на защита на ЛД.	ДА/НЕ При отговор "ДА", моля посочете подробности.

Първоначалната оценка се представя на DPO. Той я анализира, като на база дадените отговори, решава дали е необходимо извършването на пълна DPIA.

Дори при наличието на само един положителен отговор, може да възникне висока опасност за правата и свободите на субектите. В такива случаи, според конкретния контекст на обработката, DPO следва да прецени дали е необходимо да се извърши пълна DPIA. В случай, че на два или повече от въпросите в предварителната оценка е отговорено с „ДА", DPO изисква задължително извършване на пълна DPIA. При вземането на това решение DPO може да поиска допълнително съдействие от други служители и/или отдели в Университета.

Конкретна операция по обработването може да отговаря на горепосочените критерии и въпреки това да не се изисква извършването на DPIA, поради това, че не съществува вероятност да породи висок риск за правата на субектите. В този случай DPO на организацията следва да обоснове и документира, причините, поради които не се извършва DPIA. Така изготвения анализ следва да се утвърди от Ректора на ТрУ.

5.2. ИЗВЪРШВАНЕ НА ПЪЛНА DPIA

DPIA се извършва преди започване на процеса по обработване на ЛД. Извършването на DPIA следва да започне на възможно най-ранен етап от проектирането на операцията по обработване, дори ако някои от операциите по обработване все още не са известни. DPIA следва редовно да бъде актуализирана.

Изготвянето на пълна DPIA се извършва от работната група по защита на ЛД, DPO и ръководителя на отдела, инициращ внедряването на новия процес или промяна на вече съществуващия такъв.

5.3. МЕТОДИКА ЗА ИЗЧИСЛЯВАНЕ НА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО НА РИСКА

Оценка въздействието на риска се пресмята за всеки вид ЛД и съответно за всяка заплаха за съответния актив.

Изчислението на въздействието на риска включва следните компоненти

КОМПОНЕНТИ НА ВЪЗДЕЙСТВИЕТО НА РИСКА	Стойност на оценката
Оценка на правно съответствие – ПС	**1 -5 (1 най-висока)**
Потребителски контроли/конфиденциалност	**1 -5 (1 най-висока)**
Системни контроли/цялостна	**1 -5 (1 най-висока)**
ITконтроли/наличност	**1 -5 (1 най-висока)**

Изчисление на отделните компоненти на риска

- Оценка на правното състояние – извършва се от Длъжностно лице по защита на ЛД. Като по негова преценка може да бъде съгласувано с правен консултант. Оценката се извършва на база качествен анализ на възможността за гарантиране правата на субектите според GDPR в комбинация с практиките по споделяне на ЛД извън територията на ЕИП. Оценката варира в интервала от 1 до 5 като 1 е данни с най-високо потенциално негативно въздействие върху Организацията, а с оценка 5 са данни без въздействие върху нея.
- Потребителски контроли/конфиденциалност – оценката на всеки един компонент се извършва на базата на минимално въведения брой добри практики в областта на защитата на информацията, потребителския достъп, осигуряването на конфиденциалност, цялостност, наличност с различни технологични инструменти. Контролите се оценяват по метод „въведен (1)/невъведен (5)“. Общата оценка на крайния резултат е от 1 до 5 (1 най-висока).
- Системни контроли/цялостност - оценката на всеки един компонент се извършва на базата на минимално въведения брой добри практики в областта на защитата на информацията, потребителския достъп, осигуряването на конфиденциалност, цялостност, наличност с различни технологични инструменти. Контролите се оценяват по метод „въведен (1)/невъведен (5)“. Общата оценка на крайния резултат е от 1 до 5 (1 най-висока).
- IT контроли - оценката на всеки един компонент се извършва на базата на минимално въведения брой добри практики в областта на защитата на информацията, потребителския достъп, осигуряването на конфиденциалност, цялостност, наличност с различни технологични инструменти. Контролите се оценяват по метод „въведен (1)/невъведен (5)“. Общата оценка на крайния резултат е от 1 до 5 (1 най-висока).

Стойността на риска (СтР) се оценява по следния математически модел, като сбор на четирите характеристики (СбХА).

СбХА = К(стойност от 1 до 5) + Ц(стойност от 1 до 5) + Н(стойност от 1 до 5) + ПС(стойност от 1 до 5)/4

Полученият сбор СбХА като стойности от 1(най-високо) до 5 се разделя на 4, като полученият резултат се привежда до цяло число – най-малко 1, най-голямо 5.

Рискът за ЛД се категоризира съобразно оценката, както следва:

КАТЕГОРИЯ	ОЦЕНКА
Много висок риск	1
Висок риск	2
Среден риск	3
Нисък риск	4
Много нисък риск	5

Всяка изчислена степен на въздействие на риска, по-малка или равна на 3, се изследва и анализира незабавно.

След пресмятане степента на въздействие на риска за ЛД, Университетът идентифицира и обръща специално внимание на тези ЛД, за които е идентифициран много висок или висок риск.

Оценката на риска позволява да бъдат съсредоточени противодействащите защити върху заплахите, асоциирани с ЛД с най-висока степен на въздействие на риска (най-малко изчислената степен). Когато коригиращото действие бъде определено и приложено, се извършва ново изчисляване на степента на въздействие на риска.

Статусът на ЛД преди коригиращото действие е наречен „Начално въздействие на риска“, а статусът след коригиращите действия е наречен „Остатъчно въздействие на риска“.

Дефиниции на различните степени на риск:

Ниво	Оценъчна стойност	Определение
Много високо	**1**	Обработката на този тип лични данни е съпроводена с **неприемлив** риск, поради спецификата на дейностите, мястото на съхранение, липсата на контролни механизми, невъзможност да се гренадира целостта им или невъзможността да се осигурят правата на субектите собственици на данните.
Високо	**2**	Обработката на този тип лични данни е съпроводена с **много висок** риск, поради спецификата на дейностите, мястото на съхранение, липсата на контролни механизми, невъзможност да се гренадира целостта им или невъзможността да се осигурят правата на субектите собственици на данните.
Средно	**3**	Обработката на този тип данни е съпроводена с **приемливо ниво на** риска, поради наличието на възможности за контрол, гарантирани са права на субектите, данните са изцяло или частично

		структурирани.
Ниско	**4**	Обработката на този тип данни е съпроводена с ниско ниво на риска, поради наличието на възможности за контрол, гарантирани са права на субектите, въведени са механизми за мониторинг и репортинг, данните са изцяло структурирани, има въведени механизми за анонимизация, криптиране или псевдонимизация.
Много ниско	**5**	Обработката не е съпроводена с рискове за организацията. Обикновено това са напълно анонимизирани, криптирани данни, данни за статистика, архивни данни без реална употреба в ежедневните операции.

Идентифицираните заплахи за ЛД, заедно с приложимите контроли, се включват в План за третиране на риска, който организацията прилага непрекъснато при процесите по управление на информационната сигурност.

Планът за намаляване на риска е документ за координация, определящ действията за намаляване на неприемливите нива на риска и въвеждане на средства за контрол, необходими за защита на информацията.

Когато е обективно невъзможно да се намалят рисковете до приемливо ниво, то Университетът взема решение дали да се добавят повече средства за контрол или тези рискове да се избягват.

Приемането на риск в противоречие на регулацията GDPR не се допуска и не се разглежда като възможна опция.

Управлението на риска за ЛД следва да се разглежда като част от цялостната информационна сигурност в ТрУ, най-вече заради текущо налаганите механизмите за контрол, които са предназначени да спират, откриват, ограничават, предотвратяват и възстановяват след нарушения/инциденти с ЛД, което гарантира свеждането на рисковете за тях до минимум.

6. СПРАВОЧНИ ДОКУМЕНТИ

- GDPR EU679/2016
- ISO/IEC 27001:2013
- ISO 31000:2009
- Насоки на работна Група 29

7. ПРИЛОЖЕНИЯ

- Регистър на обработвани ЛД

Настоящата Методология за оценка на риска при обработката на лични данни е в сила от 25.05.2018 г. и е актуализирана за последен път на 04.02.2020 г.