ТРАКИЙСКИ УНИВЕРСИТЕТ
СТАРА ЗАГОРА

ПРОЦЕДУРА ЗА ОЦЕНКА НА РИСКА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Утвърдил:

доц. д-р Добри Ярков
Ректор на Тракийски университет

1. ЦЕЛИ

Настоящата процедура има за цел да определи реда и отговорностите в процеса по оценка на въздействието на дадена обработка върху личните данни.

Да оцени произлизащите от обработката рискове за организацията, и правата и свободите на субектите на данни.

Да осигури адекватна защита на конфиденциалността, целостта и наличността на личните данни, администрирани от организацията.

2. ОБХВАТ

Процедурата обхваща процесите по оценка на риска за ЛД, администрирани от организацията, попадащи в обхвата на Общия регламент за защита на данните /ОРЗД/GDPR/.

3. ОТГОВОРНОСТИ

Настоящата процедура се прилага от членовете на работната група по защита на ЛД и Длъжностното лице по защита на личните данни /DPO/.

Пряка отговорност за прилагане и спазване на настоящата процедура носят лицата от организацията, както следва:

- Управител за непрекъснат контрол на процесите и осигуряване на необходимите ресурси;
- DPO за оказване на контрол и методическа помощ в структурните звена и пряко управление на процесите в неговите правомощия и функционални задължения;

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/

5. ДЕЙСТВИЯ И МЕТОДИ

5.1. ОБЩИ ПОЛОЖЕНИЯ

С приемането на GDPR през април 2016 г, ЛД се превръщат в актив, чието притежание поражда определени задължения за организацията и следователно трябва да бъде защитен по подходящ начин. Оценката на потенциалните рискове по отношение на ЛД се прави с цел постоянно подобрение на сигурността, целостта, конфиденциалността, наличността и приложимото право.

Съответствието с регламента защитава както интересите на Университета, така и на субектите, чиито ЛД се администрират от него.

5.2. ОПРЕДЕЛЕНИЕ

DPIA представлява процес, чиято цел е да опише обработването на ЛД, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на субектите на данни, произтичащи от това обработването, като ги оцени и определи мерки за справяне с тези рискове. DPIA е важен инструмент за отчетност, тъй като помага на организацията да е в съответствие с изискванията на GDPR и да демонстрира, че са предприети подходящи мерки за непрекъснатото гарантиране на това съответствие.

Типовете ЛД, обработвани и администрирани от Университета могат да бъдат:

- Общи лични данни - означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;
- Чувствителни лични данни - разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

Сигурността на ЛД се характеризира като запазване на:

- Конфиденциалност: ЛД са достъпни само за тези, които са упълномощени да имат достъп до тях;
- Цялостност: гарантиране на точността и пълнотата на ЛД и на методите за тяхната обработка;
- Наличност: винаги, когато е необходимо упълномощените потребители имат наличен достъп до ЛД;

- Правно съответствие: ЛД се обработват в съответствие с изискванията на GDPR.

Съгласно GDPR, ако не бъде извършена DPIA, когато обработването подлежи на такава, ако бъде извършена неправилно или ако не бъде проведена консултация с компетентния надзорен орган (КЗЛД), когато това се изисква, това може да доведе до налагане на административна глоба на организацията.

5.3. ОБХВАТ НА DPIA

ТрУ въвежда подходящи мерки, за да гарантира и докаже спазването на GDPR, като взема предвид рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Извършването на DPIA от Университета, следва да се разбира в контекста на общото й задължение да управлява по подходящ начин рисковете, породени от обработването на ЛД.

В съответствие с основания на анализ на риска подход, извършването на DPIA не е задължително за всяка операция по обработване на ЛД. Тя се изисква само когато съществува вероятност обработването да породи висок риск за правата и свободите на субектите на данни.

„Риск“ означава неблагоприятен сценарий, описващ дадено събитие и неговите последици, оценени от гледна точка на тяхната тежест и вероятност. „Управлението на риска“ може да се определи като координирани дейности за ръководене и контролиране на процесите във връзка с риска, който те пораждат. С цел управление на рисковете за правата и свободите на физическите лица тези рискове трябва редовно да се идентифицират, анализират, преценяват, оценяват, третират (напр. като се премахват, ограничават, смекчават и т.н.) и преразглеждат.

Разглеждането на „правата и свободите“ на субектите на данни е свързано най-вече с правата за защитата на личните данни и неприкосновеността на личния живот, но може да включва и други основни права, като например свободата на словото, свободата на мисълта, свободата на движение, забраната за дискриминация, правото на свобода и свободата на съвестта и религията.

Една DPIA може да е свързана с една единствена операция по обработване на ЛД, но може да оценява и множество такива операции, които са сходни по своето естество, контекст, цел и рискове. DPIA също така може да бъде изготвена за оценяване на въздействието върху защитата на данните на даден технологичен продукт, например хардуер или софтуер. Извършването на DPIA цели систематичното проучване на нови ситуации. В този смисъл тя трябва да бъде извършвана при всяко внедряване на нови технологии и процеси по обработване на ЛД или промяна във вече съществуващи такива, когато това би могло да доведе до висок риск за правата и свободите на субектите на ЛД.

5.4. КОГА СЕ ИЗВЪРШВА DPIA

Университетът непрекъснато оценява рисковете, които се пораждат от неговите дейности, за да идентифицира кога съществува вероятност определен вид обработване да породи висок риск за правата и свободите на субектите на данни.

С влизането в сила на GDPR, за ТрУ възниква задължението на първо място да бъде

извършена DPIA за всички настоящи процеси по обработване на ЛД.

При внедряване на нов процес по обработване на ЛД или промяна на вече съществуващ такъв, следва да бъде извършена първоначална оценка на риска, резултатът от която води до решение, необходимо ли е извършването на пълна DPIA за конкретния процес или не. Първоначалната оценка се извършва от ръководителя на отдела/звеното, инициирал промяната или внедряването на новия процес по обработване. За осъществяване на първоначалната оценка той може да поиска допълнителна информация или съдействие от други служители и/или отдели в организацията. Изготвянето на първоначалната оценка на риска се извършва съгласно приетата в организацията Методология за оценка на риска при обработване на лични данни.

Така изготвената първоначална оценка се представя пред DPO, който я анализира и взема решение подлежи ли процеса на пълна DPIA или не. За вземането на това решение DPO също може да поиска допълнителна информация или съдействие от други служители и/или отдели в организацията.

DPIA следва да бъде извършена преди започване на процеса по обработването и/или въвеждането в експлоатация на нова технология (хардуер / софтуер), участваща в процеса по обработване на ЛД. Това съответства на принципите за защита на данните на етап проектиране и по подразбиране

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. Актуализирането на DPIA през целия жизнен цикъл на проекта гарантира, че се отчита цялостното въздействие от обработката, както върху организацията така и върху субектите на данни. Освен това е възможна необходимостта да се повторят отделни стъпки от оценката с напредването на процеса по разработване, защото подборът на определени технически или организационни мерки може да окаже въздействие върху тежестта и вероятността на рисковете, породени от обработването.

Налагането на актуализиране на DPIA след реалното започване на обработването, не е основателна причина да се отложи или да не се извърши DPIA. DPIA е текущ процес, особено когато операцията по обработване е динамична и подлежи на промени. Извършването на DPIA е постоянен процес, а не еднократно действие.

5.5. КОЙ ИЗВЪРШВА DPIA

Университетът, в ролята си на администратор на ЛД носи отговорност да гарантира, че се извършва DPIA. Ако Университета е възложил обработването на ЛД, изцяло или частично на подизпълнител, то той в ролята си на обработващ ЛД, следва да подпомага администратора при извършването на DPIA и да предостави цялата необходима за това информация.

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. Работната група по защита на ЛД е предварително определена и за нейни членове са избрани служители от Университета, притежаващи необходимите компетенции в сферата на защита на ЛД. Изготвянето на DPIA се извършва съгласно приетата в организацията Методология за оценка на риска при обработване на лични данни.

Когато е необходимо/целесъобразно може да се потърси становище на независими експерти от различни области (адвокати, ИТ експерти, експерти по сигурността, социолози, експерти по етични стандарти и др.).

5.6. СТАНОВИЩЕ НА СУБЕКТИТЕ НА ДАННИ

Когато е целесъобразно, ТрУ следва да се обръща към субектите на данни или техни представители за становище относно планираното обработване на ЛД. Тези становища могат да бъдат потърсени по различни начини в зависимост от контекста (напр. чрез общо проучване, въпросници, анкети сред клиенти, запитване към представителите на персонала и т.н.). В случай, че Университетът е събрал становища от субектите на данни, но въпреки това окончателното му решение се различава от тях, то причините за това решение следва да бъдат подходящо обосновани и документирани.

ТрУ, също така следва да документира своята обосновка да не потърси становищата на субектите на данни, ако реши, че това не е целесъобразно, например ако би изложило на риск поверителна информация или би било непропорционално или непрактично.

Преценката дали е целесъобразно да бъде потърсено становището на субектите на данни се извършва от Ректора на ТрУ след обсъждане с DPO.

5.7. КРИТЕРИИ

Оценката на риска за ЛД е ключов процес при управлението им. Без такава оценка организацията не може да идентифицира:

- ЛД, подлежащи на защита (третиране);
- системите, към които тази защита трябва да бъде приложена;
- необходимите ресурси;
- оперативните ограничения, които организацията смята за подходящи за намаляването на риска до приемливо ниво.

Минимално необходимите реквизити, които трябва да съдържа една DPIA са:

- Системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от организацията законен интерес;
- Оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
- Оценка на рисковете за правата и свободите на субектите на данни;
- Мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на ЛД.

5.8. ОТЧЕТНОСТ НА ПРОЦЕСА ПО DPIA

Резултатите от оценката на риска за ЛД служат при определяне:

- заплахите вътрешни и външни вектори;
- вероятността тези заплахи да се случат;
- въздействието върху Организацията.

След извършване на оценката на риска, Университетът избира подходящата стратегия и тактически приоритети при третиране на риска. Подходящите мерки за

третиране на риска зависят от конкретния контекст и рисковете във връзка с операциите по обработване. Такива биха могли да са, но не единствено: псевдонимизиране и криптиране на ЛД, свеждане на данните до минимум, прилагане на механизми за мониторинг и др.

Работната група по защита на ЛД заедно с DPO изготвя подробен доклад относно извършената DPIA. Минимално необходимите реквизити, които доклада трябва да съдържа са следните:

- Описание на обработката на ЛД в разглеждания процес;
- Описание на обхвата на извършваната оценка;
- Списък на приложимото законодателство;
- Идентификацията и оценката на заплахите, уязвимите места и вероятността за тяхната реализация;
- Списък на контролите за третиране на риска;
- Обосновка за потвърждаване на направената оценка;
- План за действие и мерките, които трябва да бъдат предприети за третиране на идентифицираните рискове.

DPO следи за правилното документиране на процеса по DPIA, изготвянето и прилагането на плана за третиране на рисковете, документиране и обосновка на взетите решения относно извършването на DPIA.

Докладът от DPIA и дефинираните в него план за действие, стратегия и мерки за третиране на идентифицираните рискове се представят пред Ректора на Университета за одобрение.

DPO извършва периодичен преглед на DPIA и на обработването, което се оценява чрез нея, най-малкото когато настъпи промяна на риска, породен от операцията по обработване.

5.9. ПУБЛИКУВАНЕ НА DPIA

Въпреки, че не съществува правно изискване за публикуване на DPIA, когато е целесъобразно организацията може да публикува резюме или заключение от извършената оценка. Целта на този процес е да се подпомогне изграждането на доверие в извършваните от ТрУ операции по обработване на ЛД и да се демонстрира отчетност и прозрачност. Решението за публикуване на резюме или заключения от извършената DPIA се взима от Ректора на Университета.

5.10. КОНСУЛТАЦИЯ С НАДЗОРНИЯ ОРГАН

DPIA се изисква, когато съществува вероятност обработването да породи висок риск за правата и свободите на субекта на данни. В такъв случай ТрУ носи отговорност да оцени рисковете и да определи мерки за намаляване на тези рискове до приемливо равнище, за да демонстрира спазването на GDPR. Ако въпреки предприетите от Университета мерки, нивото на остатъчния риск продължава да бъде високо трябва да се извърши консултация с надзорния орган (КЗЛД).

Примерите за неприемливо висок остатъчен риск включват случаи, в които за субектите на данни могат да настъпят значителни или дори необратими последици,

които те не могат да преодолеят (например незаконен достъп до данни, който води до заплаха за живота на субектите на данни, съкращение, финансов риск и др.).

Консултация с надзорния орган (КЗЛД) се извършва всеки път, когато ТрУ не може да установи достатъчни мерки за намаляване на рисковете до приемливо равнище (т.е. остатъчните рискове продължават да бъдат високи).

Надзорният орган (КЗЛД) в срок до осем седмици след получаване на искането за консултация дава писмено становище. Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване. Надзорният орган информира организацията за такова удължаване в срок от един месец от получаване на искането за консултация, включително за причините за забавянето. Тези срокове може да спрат да текат, докато надзорният орган получи всяка евентуално поискана от него информация за целите на консултацията.

При консултиране, ТрУ предоставя на надзорния орган (КЗЛД) следната информация:

- целите на планираното обработване и средствата за него;
- предвидените мерки и гаранции за защита на правата и свободите на субектите на данни;
- координатите за връзка на длъжностното лице по защита на данните (DPO);
- пълния доклад от извършената оценка на въздействието върху защитата на данните;
- всякаква друга информация, поискана от надзорния орган.

6. СПРАВОЧНА ДОКУМЕНТАЦИЯ

- ОРЗД

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