ПРОЦЕДУРА ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ
/Data Breach Management/

Утвърдил:

Доц. д-р Добри Ярков
Ректор на Тракийски университет

1. ЦЕЛ

Настоящата процедура има за цел да определи реда, отговорностите, както и системата от мерки, способи и средства за откриване и своевременно реагиране на Нарушение на сигурността на личните данни.

Да оцени риска за физическите лица и да определи минималните процеси и стъпки, които се предприемат в такива случаи.

Да се намали или да не се допуска въздействието от Нарушението на сигурността на ЛД върху Субектите.

Настоящата процедура следва да се прилага във връзка с Политиката за защита на личните данни, въведена от Организацията.

2. ОБХВАТ

Настоящият документ обхваща процесите по управление на Нарушенията на сигурността на ЛД в Университета.

Процедурата се прилага за:

- всички звена на ТрУ - факултет/филиал/колеж/департамент, в чийто процеси се включват ЛД;
- юридически лица, партньори на Университета, които оперират с ЛД, независимо дали са установени в Европейския съюз или не.

Процедурата се прилага единствено в случай на инциденти, свързани с ЛД. Не се прилага в случаи на инциденти с информация, несъдържаща ЛД.

3. ОТГОВОРНОСТИ

Настоящата процедура обхваща всички йерархични нива и служители на ТрУ.

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

- Ректорът - 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;
- Служителите от ТрУ - за прилагане на Процедурата и усъвършенстването на процеса.

4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

- Организацията - Тракийски университет - Стара Загора (Университетът, ТрУ)
- ОРЗД /GDPR/ - Общ регламент за защита на данните

- КЗЛД - Комисия за защита на личните данни/Националния компетентен надзорен орган
- ЛД - Лични данни
- DPO - Data Protection Officer/Длъжностно лице по защита на личните данни
- НСЛД - Нарушаване на сигурността на личните данни
- ИТ - отдел, служител, или външна структура, отговорни за поддръжката на информационните технологии в организацията.

5. ДЕЙСТВИЯ И МЕТОДИ

Съгласно ОРЗД „Нарушение на сигурността на личните данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до ЛД, които се предават, съхраняват или обработват по друг начин.

Университетът е приел следните типови инциденти:

- загуба/нарушения на достъп до ЛД в следствие на загуба на услуга, устройство или средства;
- неправилно функциониране или претоварвания на системата, обработваща/съхраняваща ЛД;
- човешки грешки;
- несъобразяване с политиките или указанията в организацията;
- нарушения на мерките за физическа сигурност;
- неконтролирани изменения на системата;
- неправилно функциониране на софтуера или хардуера.

Случаи, които е вероятно да бъдат класифицирани като Нарушение на сигурността на личните данни:

- Неправомерно разкриване на ЛД на клиент или служител пред трета страна, която не е оторизирана да ги получава. Например: разкриване на информация по телефона, преди да се верифицира самоличността на получателя на обаждането;
- Загуба или кражба на служебно устройство, съдържащо данни като лаптоп, таблет, мобилен телефон, сървър, резервни копия на информация;
- Така нареченото „погрешно предаване“, когато документ, съдържащ ЛД на Субект А, попадне сред документи на Субект Б (например при раздаване на служебни бележки и фишове за заплати на хартиен носител и т.н.);
- Устройство, съдържащо копие от базата данни с клиенти/служители на университета, е било загубено или откраднато;
- Загуба, в случай че единственото копие на данните е криптирано от „злонамерен софтуер“ (ransomware) или е криптирано от администратора/оператора на данни, използвайки ключ, който вече не е негово притежание;
- Неправомерен достъп до база данни;
- Постоянна или временна загуба на достъп до ЛД в следствие на прекъсване на електрозахранването, отказ на услуга и т.н.

Всяко отклонение от нормалните функции на една система в Университета може да е знак за Нарушение на сигурността на ЛД и трябва да бъде незабавно докладвано от служителят, който го е открил по определените за целта канали. Достъп до подадените сигнали имат DPO и/или ИТ /в зависимост от това дали в нарушението участва ИТ система или е установено по друг канал/.

За всички служители, в чиито служебни задължения влиза обработването на ЛД, трябва да бъдат организирани подходящи обучителни програми във връзка с практиките в Университета по обработване и опазване сигурността на данните. Като правило, всеки служител трябва да има

достъп само до информацията, строго необходима за изпълнение на възложените му дейности и задачи в Университета.

Процесът на управление на Нарушение на сигурността на ЛД включва следните етапи:

- Идентифициране на Нарушение на сигурността на ЛД;
- Оценка на Нарушението на сигурността на ЛД;
- Корективни действия в случай на Нарушение на сигурността на ЛД;
- Когато се изисква, сигнализиране на КЗЛД и комуникация със засегнатите

Субекти на ЛД;

- Записване на Нарушения на сигурността на ЛД.

5.1 Идентифициране на Нарушение на сигурността на личните данни

Всички Нарушения на сигурността на ЛД трябва да бъдат правилно и навременно идентифицирани.

В ТрУ са въведени и се прилагат подходящи технически и организационни мерки за осигуряване на подходящо ниво на сигурност, съобразно извършена оценка на риска. Тези мерки подлежат на постоянен процес на мониторинг, подробно изпитване, преценяване и оценка на ефективността им, с оглед да се гарантира сигурността на обработването на ЛД. Въведени са технически решения, в съответствие с приложимото законодателство, за да се идентифицира неподходящо поведение от страна на служители или трети страни.

Нарушение в сигурността на ЛД може да бъде открито и докладвано на организацията от вътрешни или външни заинтересовани страни като:

- Клиенти;
- Доставчици и външни възложители;
- Служители на Университета;
- Информационни системи за мониторинг на сигурността;
- ИТ отдел.

Всеки, който открие Нарушение на сигурността на ЛД, е необходимо своевременно да уведоми организацията, като нарушението трябва да бъде сигнализирано чрез един от следните канали:

- Предназначен за целта e-mail: vanya.trifonova@trakia-uni.bg;
- Телефон за контакт с отговорното лице - DPO: 042 699 206;
- Фирмена информационна система: Интегрирана университетска информационна система.

Всички тези канали и форми на оповестяване са изрично посочени в официалния сайт на Университета, както и в специално предназначени документи, достъпни за заинтересованите лица.

Минимално необходимите реквизити, които трябва да съдържа един сигнал, подаден до DPO са:

- Име и фамилия на подателя;
- Наименование на отдел и длъжност на служителя/фирмата (за сигнали подадени от трети страни);
- Телефон и e-mail за връзка с подателя;
- Дата на събитието;
- Вид на засегнатите ЛД, ако е възможно да се определи;
- Описание на нарушението;
- Причини за възникване на нарушението (ако е приложимо, например: човешка грешка, проблем при изпълнението на процес, системен проблем, неизвестно и др.).

След като е идентифицирано Нарушение на сигурността на ЛД, ТрУ следва незабавно да го оцени и да реагира. DPO и/или ИТ следва да преценят дали е налице нарушение и ако да, дали са

засегнати ЛД. За осъществяване на преценката те могат да поискат допълнителна информация или съдействие от други служители и/или отдели в Университета. В случай на установено НСЛД, отговорност на DPO е настоящата Процедура да бъде приложена.

Университетът използва следната скала за класификация:

- За инцидент - с ниска и висока приоритетност:
  - С ниска приоритетност - време за реакция до 5 часа.
  - С висока приоритетност - време за реакция до 1 час.
- За значим инцидент - незабавна реакция.

Значим инциденти са:

- когато единичен инцидент оказва влияние върху голяма група информационни масиви или цели системи, съдържащи ЛД;
- когато е налице пълна загуба до системи или информационни носители с ЛД.

Резултати от оценката и решението се записват в Регистър на инцидентите.

Като следваща стъпка, се организира заседание на предварително определен Екип за действие при Нарушение на сигурността на ЛД. Университетът е определил неговия състав в зависимост от компетенциите на персонала, местоположението му и обичайната му заетост. Основните функции на този екип са:

- получава сигналите за Нарушение от DPO;
- извършва оценка на въздействието от НСЛД;
- определя корективни и превантивни действия;

За членове на Отговорния екип са подбрани служители от Университета, притежаващи необходимите компетенции в сферата на защитата на ЛД. Със заповед на Ректора на ТрУ, за членове на Отговорния Екип са определени ИТ специалист, счетоводител, специалист човешки ресурси.

Съставът на Отговорния екип е обвързан с обема на дейностите по обработване на ЛД, с които ТрУ борави, както и с очакваната вероятност Нарушение на сигурността на ЛД да бъде открито. Следва да се вземат под и внимание и дейностите по обработка на ЛД, собственост на организацията, осъществявани от трети страни. Определянето на размера на екипа е подходящо документирано и е на разположение на Университета и Надзорния орган (КЗЛД) при поискване.

ТрУ сключва споразумения с третите страни (доставчици, подизпълнители и др.), имащи достъп или обработващи от негово име ЛД, за прилагане на действията, изисквани в настоящата Процедура за реакция при НСЛД.

5.2 Оценка на въздействието на Нарушението на сигурността на личните данни

Всяко открито НСЛД трябва да бъде незабавно оценено от гледна точка на въздействието, с цел да се осигурят подходящи действия и време за реакция. Оценката се извършва от Отговорният екип и се одобрява от DPO, който я представя пред Ректора на ТрУ.

За целите на настоящата процедура оценка на НСЛД се дефинира като „оценка на нивото на риска за потенциалното въздействие върху засегнатия Субект на данни в следствие на НСЛД“. Определянето на нивото на въздействие трябва да бъде направено съгласно приетата в Университета Методология за оценка на въздействието на НСЛД.

5.3 Корективни действия при открито Нарушение на сигурността на личните данни

За всяко открито НСЛД Отговорният екип определя корективните и превантивни действия, които трябва да бъдат предприети за смекчаване на евентуалните последствия от Нарушението,

както и за предотвратяване на повторното му възникване. Ако Нарушението засяга процесите, осъществявани от подизпълнители или доставчици на Университета, то те също трябва да бъдат включени.

DPO одобрява предложените от Отговорния екип корективни мерки, изготвя план за действие, в който определя възможно най-краткия срок за прилагането им и проследява изпълнението им. DPO извършва проверка на крайния резултат, като при необходимост може да изиска допълнителни действия. В плана се включват превантивни мерки за недопускане на същото или подобни нарушения за в бъдеще.

Описанието на корективните и превантивни действия следва да бъде подходящо документирано.

Корективните и превантивни действия се избират в зависимост от вида на Нарушението и оценката на неговото въздействие. Въпреки това тези действия могат да включват:

- Допълнително обучение и повишаване на вниманието на служителите относно защитата на личните данни;
- Ревизия и коригиране на съответните процеси и процедури;
- Специфични процедури за управление на информационната сигурност;
- Дисциплинарни мерки (например за повтарящи се пропуски на служителя);
- Модифициране и промяна на свързаните със сигурността компютърни системи и приложения;
- Подобрения в технологичния контрол, като например псевдонимизация, ограничен контрол на достъпа до системи, използване на криптиране и защита с парола;
- Подобрения в оперативните контроли, като например намаляване на зависимостта от ръчни процеси, въвеждане на "проверки на 4 очи", използване на контролни списъци в потока от процесите и т.н.;
- Одит и редизайн на процедурата за събиране на данни;
- Одит и редизайн на процедурата за обработване на данни;
- Одит и преоценяване на "Обработващия данните" (ако е приложимо).

DPO може да оспори корективните действия, предложени от Отговорния екип и да изиска по-специфични или по-строги мерки.

5.4 Сигнализиране на надзорния орган за Нарушение на сигурността на личните данни

Ако DPO счете, че НСЛД може да доведе до риск за правата и свободите на Субектите на данни, е длъжен да уведоми надзорния орган - Комисията за защита на личните данни, без ненужно забавяне в рамките на 72 часа, след като Университетът е установил или е бил уведомен за нарушението.

В уведомлението следва да се съдържа най-малко следното:

- описание на естеството на нарушението, включително, когато това е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителният брой на засегнатите записи на лични данни;
- посочване на името и координатите за връзка на DPO или на друго лице за контакт, от което може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от Университета мерки за справяне с нарушението, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

5.5 Комуникация със Субекта на данните относно Нарушение на сигурността на личните данни

За НСЛД, определени с ниво на въздействието „високо“ или „много високо“ съгласно Методологията за оценка на въздействието при НСЛД, DPO решава дали нарушението води до висок риск за правата и свободите на Субекта на данните.

НСЛД, които водят до висок риск за правата и свободите на Субекта на данни, се съобщават на Субекта без неоправдано забавяне.

Уведомяване на Субекта на данни, за настъпило НСЛД не се изисква в следните случаи:

- Университетът е предприел подходящи технически и организационни мерки за защита и те са били приложени по отношение на ЛД, засегнати от НСЛД, и по-специално мерки, които правят ЛД неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;
- Университетът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни.

При вземането на това решение, DPO трябва да вземе под внимание и усилията, необходими за осъществяване на връзка със Субекта на данни. Ако комуникацията изисква непропорционални усилия, DPO може да реши да не се свързва със Субекта на данни персонално, а да използва друг комуникационен канал, включително и публично достъпен /например съобщение на сайта/.

Всяко съобщаване за НСЛД, адресирано до засегнатите Субекти на данни, съдържа на ясен и разбираем език следната информация:

- Естеството на НСЛД,
- Името и данните за контакт с DPO, където може да се получи повече информация,
- Вероятните последици от нарушаването на личните данни
- Предприетите или предложените мерки за справяне с нарушението на личните данни, включително, когато е целесъобразно, мерки за смекчаване на възможните нежелани ефекти.

В процеса на информиране DPO може да реши да включи и други заинтересовани страни.

5.6 Регистър на Нарушенията на сигурността на личните данни

Всички НСЛД, независимо от определеното ниво на риска, се записват в специално определен регистър, който предоставя възможност на Надзорния орган (КЗЛД) да провери спазени ли са необходимите процедури.

DPO с подкрепата на ИТ отговаря за проектирането, внедряването, поддръжката и осигуряването на адекватни контроли на достъп до регистъра.

Описването на НСЛД в регистъра е отговорност на DPO.

Регистърът се ръководи от DPO, като при направено искане се представя на Надзорния орган.

Минималният набор от информация, свързана с НСЛД, която трябва да бъде записана в регистъра е:

- Дата на записване на НСЛД;
- Текущ статус на НСЛД (докладван, в процес на решаване, приключен). Статусът трябва да бъде периодично обновяван от DPO до приключване на процеса по управление на НСЛД;
- Определената приоритетност (ниска, висока, значителна);
- Определената оценка на въздействието на НСЛД (ниско, средно, високо и много високо);
- Предприетите корективни и превантивни действия;
- Дата на приключване на НСЛД;

- Изводи.

На база на Регистъра се изготвя анализ на годишна база на записаните в него инциденти, с цел подобряване на сигурността и предприемане на превантивни мерки.

6. СПРАВОЧНИ ДОКУМЕНТИ

- ОРЗД

7. ПРИЛОЖЕНИЯ

Приложение 1: Уведомление от администратора на лични данни до надзорния орган за нарушение на сигурността на личните данни

Приложение 2: Примерна форма за известяване на засегнатите Субекти на данни в случай на Нарушение на сигурността на личните данни

Приложение 3: Уведомление от обработващия до администратора на лични данни за нарушение на сигурността на личните данни

Настоящата Процедура за нарушение на сигурността на личните данни е в сила от 25.05.2018 г. и е актуализирана за последен път на 23.03.2021 г.