Утвърдил:

доц. д-р Добри Ярков
Ректор на Тракийски университет

МЕТОДОЛОГИЯ ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ОТ НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

1. ЦЕЛ

- Дефиниране на методиката за оценка на въздействието от възникнало нарушение на сигурността на ЛД върху организацията и субектите на данните, които тя администрира.
- Осигуряване на адекватна реакция и идентифициране на коригиращите и превантивни мерки за справяне с така възникналата ситуация.

2. ОБХВАТ

Методологията обхваща целия процес по оценка на въздействието и риска от настъпило нарушение на сигурността на ЛД, администрирани от организацията, попадащи в обхвата на GDPR (Общ регламент за защита на данните).

3. ОТГОВОРНОСТИ

Настоящата методология се прилага от членовете на Отговорния екип за действие при НСЛД и DPO на организацията.

4. ТЕРМИНОЛОГИЯ И СЪКРАЩЕНИЯ

- Организацията – Тракийски университет
- GDPR/ОРЗД – 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/ Отговорно лице в организацията
- НСЛД – Нарушаване на сигурността на личните данни
- ИТ – отдел, служител, или външна структура, отговорни за поддръжката на информационните технологии в организацията
- НВ – ниво на въздействие

5. ДЕЙСТВИЯ И МЕТОДИ

5.1. Общи положения

Всяко открито НСЛД трябва да бъде незабавно оценено от гледна точка на риска, който би имало за организацията и/или Субекта на данните, обект на нарушението. За целите на настоящата процедура нивото на въздействие (НВ) на НСЛД се дефинира като

„оценка на величината на потенциалното въздействие върху засегнатия Субект на данни в следствие на НСЛД“. В този смисъл, оценката на нивото на въздействие трябва да се асоциира с оценка на самото Нарушението.

Целта на оценката е да се даде подходящ приоритет на нарушението, да се осигурят подходящи действия за неговото овладяване, да се ограничи въздействието му върху организацията и субектите на данни, да се предприемат подходящи корективни и превантивни действия. Отговорностите на организацията за уведомяване и комуникация с Надзорния орган (КЗЛД) и засегнатите Субекти на данни, трябва да бъдат задействани в зависимост от крайния резултат от оценката.

Оценката на въздействието трябва незабавно да бъде изготвена от предварително определения Отговорен екип за действие, следвайки описаната по-долу Методология. Готовата оценка трябва да бъде предадена за одобрение на DPO в рамките на 24 часа. Той може да поиска допълнителна информация и да включи други заинтересовани страни. DPO може да оспори оценката направена от екипа, като всяка въведена промяна трябва да бъде мотивирана и документирана.

5.2. Оценката на Нивото на въздействие (НВ)

Оценката на НВ може да има една от следните стойности:

- Ниско;
- Средно;
- Високо;
- Много високо.

Оценката на въздействието се базира на следните критерии:

- Контекстът на обработка на ЛД (КО): той разглежда типа на засегнатите данни, заедно с редица фактори, свързани с цялостния контекст на обработката;
- Леснота на идентификация (ЛИ): определя колко лесно може да бъде определена идентичността на Субекта от засегнатите в Нарушението данни;
- Обстоятелства на Нарушението (ОН): разглежда специфичните обстоятелства на Нарушението, които са свързани с вида на нарушението и най-вече със загуба на сигурността на данни и злонамерени действия.

Оценката на тези три критерия трябва да бъде направена по методологията, описана в Точка 5.3 от настоящата Методология.

Финалната оценка на нивото на въздействие (НВ) трябва да бъде определена със следната формула:

$$\mathbf{НВ = КО \times ЛИ + ОН}$$

Нива на въздействие на Нарушение на сигурността на личните данни		
НВ < 2	Ниско	Субектите няма да бъдат засегнати или е възможно да срещнат известни неудобства, които ще преодолеят без никакви проблеми (загуба на време за въвеждане на информацията отново, раздразнение, досада и т.н.)
2 ≤ НВ < 3	Средно	Субектите може да срещнат значителни неудобства, които ще могат да преодолеят, въпреки някои трудности (допълнителни разходи, отказ за достъп до бизнес

		обслужване, страх, липса на разбиране, стрес, дребни физически заболявания и т.н.)
3 ≤ НВ < 4	Високо	Субектите може да изпитат сериозни последици, който би трябвало да могат да преодолеят, въпреки големи затруднения (злоупотреби със средства, вписване в „черния списък“ на банки, имуществени щети, загуба на работа, призовки, влошаване на здравето и т.н.)
4 ≤ НВ	Много високо	Субектите могат да срещнат значителни или дори необратими последствия, които да не могат да преодолеят (финансово бедствие като значителен дълг или неработоспособност, дългосрочно психологически или физически заболявания, смърт и т.н.)

5.3. Критерии за оценка на въздействието

За да бъде дадена измерима стойност на оценката на въздействието, подробно трябва да бъдат разгледани факторите, утежняващи или смекчаващи въздействието на трите критерия

А) Контекст на обработката на ЛД (КО)

Според типа на засегнатите данни се дава предварителен основен резултат, който може да бъде намален или увеличен като стойност, в зависимост от контекста.

Тип на данните		**Резултат**
Общи данни	Например биографични данни, контакти, трите имена, данни за образование, семеен живот, професионален опит	
	Предварителен основен резултат: когато Нарушението включва "общи данни" и администраторът не е наясно с никакви утежняващи фактори.	1
	КО резултатът може да бъде увеличен с 1, напр. когато обемът на "общите данни" и/или характеристиките на администратора са такива, че може да има възможност за изготвянето на определен профил на Субекта или да се направят предположения за социалното/финансовото състояние на Субекта.	2
	КО резултатът може да бъде увеличен с 2, напр. когато "общите данни" и/или характеристиките на администратора могат да доведат до предположения за здравословното състояние на индивида, сексуалните предпочитания, политическите или религиозните му убеждения.	3
	КО резултатът може да бъде увеличен с 3, напр. когато поради определени характеристики на Субекта (например: ако принадлежи към уязвими групи или е	4

	непълнолетен), информацията може да бъде от решаващо значение за неговата лична безопасност или физическо/психологическо състояние.	
Поведенчески данни	Например местоположение, данни за пътувания, данни за лични предпочитания, навици и т.н.	
	Предварителен основен резултат: когато нарушението включва "поведенчески данни" и администраторът не е наясно с никакви утежняващи или понижаващи фактори.	2
	КО резултатът може да бъде намален с 1, напр. когато естеството на данните не осигурява съществено разбиране за поведението на Субекта или данните могат да бъдат събрани лесно (независимо от Нарушението) чрез публично достъпни източници (например: комбинация от информация от търсения в мрежата).	1
	КО резултатът може да бъде увеличен с 1, напр. когато обемът на "поведенческите данни" и/или характеристиките на администратора са такива, че може да се създаде профил на Субекта, предоставяйки подробна информация за неговия ежедневен живот и навици.	3
	КО резултатът може да бъде увеличен с 2, напр. ако може да бъде създаден профил на Субекта, основан на чувствителните негови данни.	4
Финансови данни	Всички видове финансови данни (например: доходи, финансови транзакции, банкови извлечения, инвестиции, кредитни карти, фактури и т.н.). Включително данни за социалното благосъстояние, свързано с финансовата информация.	
	Предварителен основен резултат: когато нарушението включва "финансови данни" и администраторът не е наясно с никакви утежняващи или понижаващи фактори.	3
	КО резултатът може да бъде намален с 2, напр. когато естеството на набора от данни не осигурява съществено разбиране за финансовата информация на лицето (например: факта, че дадено лице е клиент на определена банка без повече подробности).	1
	КО резултатът може да бъде намален с 1, напр. когато конкретният набор от данни съдържа известна финансова информация, но все още не дава никакво съществено разбиране за финансовото	2

	състояние/ситуацията на лицето (например: номер на обикновена банкова сметка без допълнителни подробности).	
	КО резултатът може да бъде <u>увеличен</u> с 1, напр. когато поради характера и/или обема на конкретния набор от данни се разкрива пълна финансова информация (например: пълна информация от кредитна карта), която би могла да позволи измами или на база на тази информация може да бъде създаден подробен социален/финансов профил на Субекта.	4
Чувствителни данни	Всички видове чувствителни данни (например: здравно състояние, политически пристрастия, сексуален живот, религиозна принадлежност и т.н.)	
	Предварителен основен резултат: когато Нарушението включва "чувствителни данни" и администраторът не е наясно с никакви намаляващи фактори.	4
	КО резултатът може да бъде <u>намален</u> с 3, напр. когато естеството на набора от данни не осигурява съществено разбиране за чувствителни аспекти от живота на Субекта или данните могат да бъдат събрани лесно (независимо от Нарушението), чрез публично достъпни източници (например: комбинация от информация от търсения в мрежата).	1
	КО резултатът може да бъде <u>намален</u> с 2, напр. когато естеството на данните може да доведе единствено до общи предположения.	2
	КО резултатът може да бъде <u>намален</u> с 1, напр. когато естеството на данните може да доведе до предположения за чувствителна информация относно Субекта.	3

Описание на контекстни фактори, които трябва да бъдат взети предвид при оценката на КО.

- Утежняващи фактори:

○ <u>Обемът на данните, разкрити при Нарушението (за един и същ Субект):</u> този фактор може да увеличи основния КО резултат в зависимост от количеството на разкритата информация. Обемът трябва да се има предвид, както по отношение на времевия диапазон, който разкритата информация обхваща (например: един и същ тип данни за различни периоди от време), така и по отношение на пълнотата на разкритата информация (допълващи се данни от един и същ тип). Например, в случай на нарушение на данните за трафика в интернет доставчик, резултатът от КО (за един Субект) би бил по-висок, ако данните обхващат период от една година, отколкото ако са ограничени до една седмица.

Друг пример е случай на разкриване на банкова информация, където оценката на КО би била по-висока при разкриване на пълното досие на даден Субект, отколкото ако е разкрит само един документ от досието.

- Специфични характеристики на администратора на данни: този фактор се отнася до полето на действие и дейностите на администратора на данни, което би могло да увеличи основния КО резултат, като сам по себе си разкрива допълнителна информация за набора от данни. Например, оценката на КО при разкриване на списък на клиентите би била по-висока, ако е от онлайн аптека, отколкото ако е от магазин за канцеларски материали;
- Специални характеристики на отделните Субекти: Основният КО резултат за даден набор от данни би могъл да се увеличи и в случай, че индивидите, чиито данни са разкрити, принадлежат към социална група със специфични нужди или характеристики (например ако са непълнолетни, ако принадлежат към друга чувствителна група, или са лица от група със специални характеристики). Например, оценката на КО за разкриване на списък с телефонни номера ще се увеличи, ако телефоните принадлежат на известни членове на националния парламент.

- Фактори, намаляващи тежестта на Нарушението:
  - Невалидност/неточност на данните: основният резултат на КО на даден набор от данни може да бъде намален, ако на администратора е известно, че разкритите данни са невалидни или неточни (например: поради възрастта на информацията или съдържанието) и следователно тяхното значение е чувствително намалено. Администраторът трябва да е сигурен в това обстоятелство, за да го включи в оценката. Например, при разкриване на пощенски списък с адреси, на които писмата не могат да бъдат доставени, се счита за неточен (т.е. най-вероятно хората са се преместили на друг адрес);
  - Обществена достъпност на данните: основният резултат на КО за даден набор от данни може да бъде намален и в случай, че разкритите данни вече са били публично достъпни преди Нарушението или могат лесно да бъдат събрани, и/или открити чрез обществено достъпни източници;
  - Естество на данните: друг понижаващ фактора, в някои случаи може да бъде самото естество на набора от данни, който въпреки първоначалната си висока оценка на КО е с по-малко значение по отношение на информацията, която може да разкрие за Субекта. Например, такъв е случаят на разкриване на медицинско свидетелство, което само удостоверява, че лицето е в добро здравословно състояние, без да разкрива друга информация. В този случай, въпреки че основният резултат ще бъде 4, тъй като данните за здравословното състояние са чувствителни, крайният резултат на КО за конкретния набор от данни ще бъде 1, тъй като не може сам по себе си да засегне личния живот на Субекта. Този фактор, обаче трябва да бъде разгледан с голямо внимание и ясна обосновка на причината, поради която крайният резултат от КО е бил намален спрямо основния.

Б) Оценяване на Леснотата на Идентификация (ЛИ):

Идентификацията на Субекта може да бъде пряка или непряка и се извършва чрез определени идентификатори, като се взима предвид и цялостният контекст на обработката на ЛД.

Списък на често срещаните идентификатори и различните случаи на възможното им използване за оценяване на ЛИ:

Пълно име (име, презиме, фамилия): Това се счита за най-често срещания директен идентификатор, но оценката за ЛИ може да варира в зависимост от случая, тъй като пълното име не винаги само по себе си уникално идентифицира Субекта. Например, когато идентификацията се извършва само с пълното име на лицето:

• ЛИ = 0,25 (пренебрежимо), когато сред населението на дадена страна много хора споделят едно и също име;

• ЛИ = 0,5 (ограничено), когато сред населението на дадена страна малко хора имат същото име;

• ЛИ = 0,75 (значително), когато сред населението на малък град има малко хора или изобщо няма хора, споделящи същото име;

• ЛИ = 1 (максимално), когато се използва и друг идентификатор, като например датата на раждане и имейл адресът.

Номер на лична карта/паспорт/номер на социална осигуровка: Всички те се считат за уникални идентификатори и могат да бъдат използвани за идентифициране на Субекта, доколкото е възможно да се отнесат към референтна база данни (например свързване на лична карта с определено лице). Например, когато идентификацията се извършва само с един от следните начини:

- ЛИ = 0,25 (пренебрежимо), когато не е предоставена друга информация за лицето или не е възможно да се намери допълнителна информация, освен ако не бъде получен достъп до референтната база данни даваща връзка между номера и конкретния Субект;
- ЛИ = 0,75 (значително), когато идентификаторът разкрива допълнителна идентификационна информация за отделния Субект (например ЕГН, показващо датата на раждане) и е свързан с други данни (например пощенски адрес или имейл);
- ЛИ = 1 (максимално), когато е на лице информация от референтната база данни (например на лична карта и три имена и/или снимка).

Телефонен номер/домашен адрес: И двете са индиректни идентификатори, които могат да се използват и за комуникация или достъп до Субекта. Когато идентификацията се основава само на един от тези два идентификатора:

- ЛИ = 0,25 (пренебрежимо) сред населението на страната, когато телефонният номер/адресът не е регистриран в публично достъпен регистър;
- ЛИ = 0,5 (ограничено) сред населението на малък град и телефонният номер/адресът не е регистриран в публично достъпен регистър (идентификацията е възможна чрез комуникация със Субекта);
- ЛИ = 1 (максимално) сред населението на страната и телефонният номер/адресът е включен в публично достъпния регистър.

Имейл адрес: Той също е индиректен идентификатор, който може да се използва за комуникация със Субекта и в някои случаи може да включва информация за неговото/нейното име (собствено и/или фамилно). Когато идентификацията се основава на имейл:

- ЛИ = 0,25 (незначително), когато имейл адресът не разкрива друга идентификационна информация (например име) и не се използва като основен адрес на Субекта в интернет сайтове, форуми или социални мрежи;
- ЛИ = 0,75 (значително), когато имейл адресът не разкрива друга идентификационна информация (например: име), но се използва като основен адрес на

Субекта в интернет сайтове, форуми или социални мрежи (които имат възможност да бъдат намерени при търсене в мрежата);

- ЛИ = 1 (максимално), когато имейл адресът разкрива името на лицето и се използва като негов основен адрес в интернет сайтове, форуми или социални мрежи (с възможност да бъдат намерени при търсене в мрежата).

Снимка: В зависимост от случая, тя може да бъде пряк или косвен идентификатор. Например, когато идентификацията се основава само на снимка:

- ЛИ = 0.25 (пренебрежимо), когато снимката е неясна или размазана (например: кадри от далечно разстояние);
- ЛИ = 0,5 (ограничено), когато снимката е неясна или размазана, но включва допълнителна информация (например фон, показващ конкретно местоположение), която може да доведе до идентифициране на Субекта;
- ЛИ = 0,75 (значително), когато снимката е ясна, но с нея не е свързана друга идентификационна информация;
- ЛИ = 1 (максимално), когато снимката е ясна и е свързана с допълнителна информация (например информация за участие в определена група, домашен адрес и т.н.).

Кодиране/Псевдоними/Инициали: Кодирането се отнася до задаването на уникален идентификационен номер на всяко лице, напр. в контекста на конкретна база данни. Използването на псевдоними е форма на псевдонимизиране, в смисъл че конкретен идентификатор (обикновено пълното име на индивида) се замества с псевдоним. Инициалите са тип псевдоним, който се извлича от пълното име на индивида. Както при другите уникални идентификатори, кодовете и псевдонимите могат да се използват, за да се идентифицира физическото лице, доколкото е възможно да се свържат с референтната база данни (напр. базата данни свързваща кода/псевдонима с пълното име на определен Субект). Въз основа на кодиране или използване на псевдоними:

- ЛИ = 0,25 (незначително), когато кодът/псевдонимът не разкрива и не може да бъде свързан с други ЛД за физическото лице, освен ако не бъде получен достъп до референтната база данни;
- ЛИ = 0,75 (значително), когато псевдонимът разкрива някои данни за Субекта (например първо име) и е свързан с други ЛД (например имейл адресът на Субекта);
- ЛИ = 1 (максимално), когато псевдонимът разкрива пълното име на Субекта или пълните данните от референтната база данни са на разположение.

В) Обстоятелствата на Нарушението (ОН)

Всички следващи категории събития се считат за Нарушаване на сигурността на личните данни:

- "Нарушение на поверителността" - когато има неразрешено или случайно разкриване или достъп до ЛД.
- "Нарушение на достъпа" - когато има случайна или неоторизирана загуба на достъп до, или ликвидиране на ЛД.
- "Нарушение на целостта" - когато има неразрешено или случайно изменение на ЛД.

Примери за загуба на достъпа са случаите, в които данните са били изтрити случайно или от неоторизирано лице, или при криптиране за осигуряване на сигурност на данни, ключът за декриптиране е изгубен. В случай че администраторът не може да възстанови достъпа си до данните, например от резервно копие, това се счита за трайна загуба на

достъп.

Загубата на достъпност може да възникне и при значителни смущения в нормалната услуга на дадена организация, например при прекъсване на електрозахранването или при атака водеща до отказ на услуга, което прави личните данни недостъпни перманентно или временно.

Загуба на поверителност

0 - Примери за данни, изложени на рискове за поверителността, без доказателства за незаконна обработка:

- При транзит се загубва хартиен документ или лаптоп;
- Изхвърлено е оборудване, без предварително да са унищожени личните данни от него.

+ 0.25 - Примери за данни, предоставени на редица известни получатели:

- По грешка е изпратен имейл с ЛД на известен брой получатели;
- Някои клиенти имат достъп до профили на други клиенти в онлайн услуга.

+ 0.5 - Примери за данни, предоставени на неизвестен брой получатели:

- Данните са публикувани в интернет форум;
- Данните са качени на сайт P2P (Peer twen Peer);
- Служител е продал CD ROM, съдържащ данни на клиента.

Загуба на целостта

0 - Примери за променени данни, но без определена неправилна или незаконна употреба:

- Записите в база данни, съдържаща ЛД, са актуализирани неправилно, но оригиналът е възстановен, преди да е настъпило каквото и да било използване на променените данни.

+ 0.25 - Примери за данни, променени и евентуално използвани по неправилен или незаконен начин, но с възможност за възстановяване:

- Документът, необходим за предоставянето на онлайн социална услуга, е променен и човекът трябва да поиска услугата по офлайн начин.
- Бил е променен запис, който е важен за точността на файла на физическо лице в онлайн медицинска услуга.

+ 0.5 - Примери за данни, променени и евентуално, използвани по неправилен или незаконен начин без възможност за възстановяване:

- Всички предишните примери, но без оригиналът да може да бъде възстановен.

Загуба на достъп

0 - Примери за възстановяване на данни без затруднения:

- Копие от файла е загубен, но има други копия;
- Базата данни е повредена, но може лесно да бъде възстановена от други бази данни.

+ 0.25 - Примери за временна загуба на достъп:

- Базата данни е повредена, но може да бъде възстановена от други бази данни, въпреки че е необходима известна обработка;
- Файлът се губи, но информацията може да бъде предоставена отново от Субекта.

+ 0.5 - Примери за пълна загуба на достъпа до данните (данните не могат да бъдат възстановени от администратора или Субектите):

- Файлът е изгубен/базата данни е повредена, няма резервно копие на тази информация и тя не може да бъде предоставена от Субекта.

Злонамерени действия

+ 0.5 – Нарушението на сигурността на личните данни се дължи на умишлено действие, напр. с цел да причини вреди на администратора на данни (например: да покаже липса на сигурност) и/или да навреди на Субектите.

- Служител на фирма умишлено споделя ЛД на клиенти на публичен сайт на социални медии;
- Служител на фирма продава ЛД на клиенти на друга компания.

6. СПРАВОЧНИ ДОКУМЕНТИ

- ОРЗД

Настоящата Методология за оценка на въздействието от нарушаване на сигурността на личните данни е в сила от 25.05.2018 г. и е актуализирана за последен път на 01.10.2021 год.