ПРИЛОЖЕНИЕ № 1

КЪМ ИНСТРУКЦИЯ ЗА ПРАКТИЧЕСКОТО ОСЪЩЕСТВЯВАНЕ НА НАДЗОРНАТА ДЕЙНОСТ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

МЕТОДИКА ЗА ОПРЕДЕЛЯНЕ НИВОТО НА РИСКА ПРИ НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Тази методика определя реда и условията, при които Комисията за защита на личните данни (КЗЛД/комисията) определя нивото на риска за правата и свободите на физическите лица при нарушение на сигурността на личните им данни (нарушението).

Поради многообразието на нарушения в сигурността на личните данни и постоянно развиващите се техники и технологии за извършване на нарушения и тяхното преодоляване, налице са неизброими комбинации от ситуации, които могат да характеризират едно нарушение, както и възможности за реакция и преодоляване на реалните и потенциални вреди. Не е възможно да се създаде изчерпателен алгоритъм за оценяване на всички обстоятелства. Настоящата методика е механизъм за оценяване на риска с отчитане на основни параметри. По преценка е допустимо да се отчетат и допълнителни фактори, които е възможно да намалят или увеличат риска за правата и свободите на лицата.

I. Общи положения.

1. Определянето на нивото на риска по тази методика се извършва вследствие на **анализ на данните от подадено от АЛД уведомление** по чл.62 от Правилника на КЗЛД, както и последващи отговори на допълнителни въпроси.

2. При всяко нарушение на сигурността винаги се извършва оценка на риска за всички типове нарушения, като се започва от „нарушение на поверителността“. За окончателна се взема най-високата оценка.

Например: *Криптирана е информацията на фирма за услуги. Личните данни, които са засегнати от това нарушение са на две типа хора – служители на фирмата и клиенти. Тук водещото и доказано е нарушение от типа загуба на* ***наличност****. Едновременно с това данните са били достъпни за нарушителя, възможно е да са били изтеглени и/или манипулирани, т.е. налице са евентуални „****нарушение на поверителността****“ и „****нарушение на целостта****“. В този случай ще се извърши поотделно оценка за „нарушение на поверителността“, „нарушение на целостта“ и „нарушение на наличността“ и за окончателна ще се вземе най-високата оценка.*

3. Нарушение на сигурността на данните е **всяка една комбинация или самостоятелно проявление** на някой от следните три типа нарушение „**Нарушение на поверителността“, „Нарушение на целостта“** и/или **„Нарушение на наличността“.**

- **Нарушение на поверителността** е неправомерно преднамерено или случайно разкриване или достъп до лични данни. Това включва разкриване на лични данни пред (или достъп до тях на) получатели, които не са оправомощени да ги получат (или да имат достъп до тях), или всеки друг вид обработване, което е в нарушение на ОРЗД.

- **Нарушение на целостта е** преднамерено или случайно повреждане на лични данни. „Повреждане“ е налице, когато личните данни са променени, подправени или станали вече непълни.
- **Нарушение на наличността** е преднамерена или случайна загуба на данни, унищожаване на данни или неналичена услуга. „Загуба“ на лични данни е състояние, при което данните може да са все още налични, но администраторът на лични данни (АЛД) е загубил контрол или достъп до тях или вече не ги притежава. „Унищожаване“ на лични данни е налице, когато данните вече ги няма или ги няма във вид, в който може да бъдат използвани.

Никой от тези три типа нарушения не е с по-голям приоритет, тъй като всеки би могъл да има сериозни последици върху правата и свободите на субектите на данни – загуба на права, загуба услуги, злоупотреба със самоличност и т.н.

Тъй като за оценяването на риска при различните типове нарушение значение имат различни обстоятелства, оценката се извършва по различни критерии за различни типове нарушение.

При **загуба на данни или тяхното манипулиране** (при което основното негативно въздействие върху лицата е загуба на права и услуги) е важно да се отчетат:

- **доколко е възможно** данните да бъдат възстановени,
- **колко бързо** може да стане възстановяването,
- **предварителните** действия на аминистратора (създаване на архивни копия и готовност за бързо и качествено възстановяване на данните),

При **нарушението на поверителността** (при което основното негативно въздействие е злоупотреба с информацията) следва да се отчетат:

- доколко данните, обект на нарушението могат да послужат за **идентифициране** на лицата;
- до каква степен данните дават възможност за извършване на **евентуална злоупотреба**;
- дали **характерът на нарушението** е такъв, че може да се очаква някаква злоупотреба (пр. наличие на умисъл);
- **последващите** действия на администратора (предприемане на мерки за ограничаване на вредни последствия - уведомяване на лицата, промяна на информация, за която това е възможно, пр. акаунти)

4. При нарушение на сигурността на данните е възможно да бъдат засегнати по различен начин различни категории физически лица. В този случай оценяването трябва да се извърши за всяка група самостоятелно. Като окончателна оценка на риска се взема по-високата.

Например: *Обект на нарушение от типа „нарушение на поверителността“ са лични данни на 2 категории физически лица – трима служители (всякакви данни - основни, финансови, чувствителни данни) и 50 000 клиенти (само основни данни). В този случай оценяването трябва да се извърши поотделно, тъй като при механично комплексно оценяване ще се получи необосновано висока оценка.*

5. Следва да се има предвид, че **обикновено не е възможно да се отговори еднозначно на всички въпроси, свързани с нарушението** (напр. налице ли е умисъл). При извършването на оценката на риска се отчита това, което е предоставено от администратора като информация, както и служебно събраната такава. Би могло да се вземе предвид и

оценката и предположенията на администратора, ако са обосновани. Всякакви допълнителни допускания следва да бъдат в рамките на разумната допустимост.

II. Формула за определяне нивото на риска.

Нивото на риска се определя от:

– **оценката на тежестта на въздействието** (т.е. от потенциалните въздействия и техният увреждащ характер върху правата и свободите на гражданите**)**

– **вероятността това въздействие да настъпи**.

Ниво на риска се определя по следната формула:

НР = ТВ * ВЕР

където:

НР – ниво на риска (**стойност от 1 до 5)**

ТВ – тежест на въздействието (**стойност от 1 до 5)**

ВЕР – **вероятността** евентуалното въздействие да настъпи (**стойност от 0 до 1,** където 0 означава 0% вероятност, а 1 – 100% вероятност**)**

Нивото на риска се оценява както следва:

ниско ниво – от 0 до 1

средно ниво – от 1,25 до 2,25

високо ниво – от 2,5 до 5

За графично онагледяване на нивото на риска би могла да се ползва следната таблица:

ВЕР					
1	1	2	3	4	5
0,75	0,75	1,5	2,25	3	3,75
0,5	0,5	1	1,5	2	2,5
0,25	0,25	0,5	0,75	1	1,25
0	0	0	0	0	0
	1	2	3	4	5 **ТВ**

III. Определяне на тежестта на въздействието (ТВ).

ТВ е число от 0 до 5, като на 0 съответства на най-малка тежест на въздействието, а 5 е най-голяма тежест на въздействието.

Изчислява се по следната формула:

ТВ=ВДИ+ДО

където:

ВДИ (вид на данните и възможност за идентифициране) – за определянето му се взема предвид видът на данните (ВД), потенциална тежест за всеки вид и, в случай на „нарушение на поверителността“ - възможността за идентификация.

ДО - допълнителни обстоятелства, увеличаващи тежестта на въздействието.

1. **Определяне на ВД (вид на данните)** и оценяване на тяхното значение по отношение тежестта на въздействието.

Данните са следните 5 вида с нарастващо значение по отношение на тежестта на въздействието:

Вид на данните (ВД)	**Базова оценка**
Основни данни - биографични данни, данни за контакт, имена, ЕГН, данни за образование, семеен живот, професионален опит и др.	**1**
Профилиращи данни - данни, свързани с поведението на физическите лица (местоположение, трафични данни, данни, отнасящи се до лични предпочитания и навици и др.)	**2**
Финансови данни - данни, свързани с финансовото и имотно състояние на физическите лица **(**доходи, трансакции, банкови извлечения, кредитни карти, социално осигуряване и др.).	**3**
Чувствителни данни - специални категории данни и данни, свързани с присъди и нарушения (данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, както и за присъди и правонарушения или свързани с тях мерки за сигурност, както и данни свързани с присъди и нарушения)	**4**
Биометрични, генетични или графологични за целите на идентифицирането на физическите лица. Данни, достатъчни за **злоупотреби, заплахи, изнудване, кражба на идентичност и др.** Данни, които в съчетание с характеристиките на физическото лице са от значение за неговата **безопасност или физическото/психическо състояние**.	**5**

Възможно е обект на нарушението да са данни, комбинация от гореизброените видове, напр. финансови и основни данни. При такава ситуация се извършва оценка на всеки вид поотделно, като се отчита наличието на всички засегнати от нарушението данни, и за окончателна се взема най-високата оценка.

За всеки от гореизредените видове данни, базовата оценката може да бъде коригирана (да бъде увеличена или намалена) в зависимост от това дали данните за определен субект, тяхното количество и качество, както и възможностите да се комбинират, позволява да се правят предположения относно допълнителни аспекти, въз основа на които да се премине в друга категория на данните или да се оцени, че е необходимо базовата оценка да се увеличи или намали.

Пример за преминаване в друга категория данни, при което се променя базовата оценка:

Налице е неправомерено разкриване или достъп до „**основни данни**“, при което **базовата оценка е 1**.

Ако „**основните данни**“ са такива, че е възможно въз основа на тяхното количество и качество да се извърши профилиране (автоматично обработване по определени параметри), се отива в категорията „п**рофилиращи данни“** и **базовата оценка става 2**.

Ако „**основните данни**“ са такива, че е възможно въз основа на тяхното количество и качество да се направят предположения относно социалния/финансовия статус на физическото лице се отива в категорията „**финансови данни“** и **базовата оценка става 3**.

Ако „**основните данни**“ са такива, че е възможно въз основа на тяхното количество и качество да се направят предположения относно здравния статус, сексуалните предпочитания, политическите или религиозните възгледи на физическото лице, се отива в категория **„чувствителни данни“** и **базовата оценка става 4**.

Ако „**основните данни**“ са такива, че информацията може да бъде използвана за злоупотреби, заплахи, изнудване, кражба на идентичност и др. **– базовата оценката става 5**.

Пример за увеличаване и намаляване на базовата оценка:

Налице е неправомерено разкриване или достъп до „**финансови данни**“, при което **базовата оценка е 3**.

Ако „**финансовите данни**“ са такива, че не са достатъчни да бъдат направени *каквито и да е заключения* относно финансовото състояние на физическото лице (пр. физическото лице е клиент на определена банка), тогава базовата оценка се намалява до минималната, т.е. **става 1**.

Ако „**финансовите данни**“ са такива, че могат да дадат някои *общи представи относно профила* на физическото лице, базовата оценка **става 2**.

Ако „**финансовите данни**“ са такива, че са достатъчни за да се направят *сериозни заключения* за финансовото състояние на физическото лице, базовата оценка се увеличава и **става 4**.

Ако „**финансовите данни**“ са такива, че въз основа на вида и/или обема на данните може да бъдат разкрити такива данни, свързани с финансовото състояние на физическото лице, които *биха могли да доведе до измами и финансови злоупотреби***, базовата оценка става 5.**

2. Определяне на ВДИ ((вид на данните и възможност за идентифициране на лицата)

2.1. При нарушения от тип „**нарушение на наличността**“ и „**нарушение на целостта**“ се отчита само вида на данните, без да се отчита възможността за идентифициране, т.е. ВДИ=ВД

2.2. При нарушение от тип „**нарушение на поверителността**“ за определяне на ВДИ е необходимо отчитане вида на данните и на възможността за идентифициране на лицата в зависимост от изтеклите данни, което се извършва при следната таблица:

- Данните **идентифицират** лицата без да са необходими никакви допълнителни усилия и/или – колона А *(базовата оценка ВД+1)*
- Лицата могат да бъдат **идентифицирани лесно, при допълнителна информация, която е лесно достъпна** (напр. публична информация) – колона Б (*тези стойности съвпадат с базовата оценка на вида на данните*)
- Лицата могат да бъдат **идентифицирани трудно, при наличие на допълнителна информация и специални механизми за обработване** – колона В *(базовата оценка ВД-1, с изкл. на основните данни, където не става 0, а остава 1)*
- Данните **не могат да послужат за идентифициране** на съответните субекти (напр. криптирани или анонимизирани) – колона Г

Възможност за идентифициране / **Вид на данните**	**А**	**Б**	**В**	**Г**
Основни данни - биографични данни, данни за контакт, имена, ЕГН, данни за образование, семеен живот, професионален опит и др.	**2**	**1**	**1**	**0**
Профилиращи данни - данни, свързани с поведението на физическите лица (местоположение, трафични данни, данни, отнасящи се до лични предпочитания и навици и др.)	**3**	**2**	**1**	**0**
Финансови данни - данни, свързани с финансовото и имотно състояние на физическите лица **(**доходи, трансакции, банкови извлечения, кредитни карти, социално осигуряване и др.).	**4**	**3**	**2**	**0**
Чувствителни данни - специални категории данни и данни, свързани с присъди и нарушения (данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, както и за присъди и правонарушения или свързани с тях мерки за сигурност, както и данни свързани с присъди и нарушения)	**5**	**4**	**3**	**0**
Биометрични, генетични или графологични за целите на идентифицирането на физическите лица. Данни, достатъчни за **злоупотреби, заплахи, изнудване, кражба на идентичност и др.** Данни, които в съчетание с характеристиките на физическото лице са от значение за неговата **безопасност или физическото/психическо състояние**.	**5**	**5**	**4**	**0**

3. Определяне на ДО – допълнителни обстоятелства, увеличаващи тежестта на въздействието, *като например (без да е изчерпателно):*

- специални категории субекти (малолетни деца, инвалиди, възрастни хора, граждани на трети държави) (+1);
- голям брой засегнати лица (+1);
- повторяемост на нарушение от един и същи тип.(+1).

ДО се изчислява с натрупване, т.е. вземат се предвид всички налични обстоятлства, като за всяко налично допълнително обстоятелство се прибавя 1 (т.е. +1).

Окончателната стойност на ТВ е в границите от 0 до 5. В случай, че в резултат от натрупването при отчитане на допълнителни обстоятелства, увеличаващи тежестта на въздействието, се премине границата от 5, то се приема, че ТВ=5.

IV. Определяне на вероятността евентуално негативно въздействие да настъпи (ВЕР).

1. Определяне на ВЕР (стойност от 0 до 1, където 0 означава 0% вероятност, а 1 – 100%**).**

до 1	много голяма вероятност
до 0,75	голяма вероятност
до 0,5	средна вероятност
до 0,25	малка вероятност
0	няма вероятност

ВЕР се определя по различен начин в зависимост от **вида нарушение** на сигурността на личните данни (**„нарушение на поверителността“, „нарушение на целостта“ и „нарушение на наличността“).** При всяко нарушение се извършва оценка на риска за всички типове нарушения, като се започва от „нарушение на поверителността“. За окончателна се взема най-високата оценка на риска.

Ако не е възможно да се определи стойност на ВЕР, по подразбиране се приема ВЕР=0,5.

2. Определяне на ВЕР в случай на „нарушение на поверителността“.

В този случай се отчитат следните два фактора:

- характер на нарушението,
- предварителните и последващи **действията на администратора** за преодоляване на евентуални последици от нарушението.
  - Независимо от действията на администратора, последиците са необратими и извън неговия контрол И/ИЛИ вече е доказано наличие на злоупотреба - колона А.
  - Необходими са сериозни усилия (от страна на администратора и ФЛ) за предотвратяване на последствията - колона Б.

- Налице са действия на администратора, които намаляват евентуалните последствия от нарушението (напр. уведомяване на ФЛ) – колона В
- Налице са действия на администратора, които напълно неутрализират евентуалните последствия – колона Г

Оценяването на вероятността евентуалното нежелано въздействие да настъпи се извършва по следната таблица:

Действия на АЛД / **Характер на нарушението**	**А**	**Б**	**В**	**Г**
Наличие на умисъл	1	0,75	0,5	0
Непредпазливост (пр. погрешно изпратен мейл)	0,75	0,5	0,25	0
Осъществен случаен достъп (пр. при загубени или откраднати устройства/ документи)	0,5	0,25	0,25	0

2. Определяне на ВЕР в случай на „нарушение на целостта“ и „нарушение на наличността“.

При „**нарушение на целостта**“ или „**нарушение на наличността**“ вероятността от настъпване на негативни последствия за правата и свободите на субектите на данни се оценява **в зависимост от възможността за възстановяване на данните**:

– Невъзможно е възстановяване на данните. (**ВЕР = 1**)

– Възстановяването на данните е много трудно – необходимо е последващо или допълнително събиране на информация. Необходими са усилия както от страна на администратора, така и от страна на субекта на данни. (**ВЕР = 0,75**)

– Възстановяването на данните е средно трудно – възстановяване на истинската информация от налични документи или електронни копия (чрез повторно въвеждане и проверка). Необходими са сериозни усилия от страна на администратора. (**ВЕР = 0,5**)

– Възстановяването на данните е лесно. Пълната и вярна информация може да бъде възстановена от електронни архиви и предходни състояния на информационните масиви. (**ВЕР = 0,25**)

– Не е необходимо да се възстановяват на данни (напр. при временна неналичност на достъп до услуга, при което няма поражения върху данните, а отказът е резултат от временен технически проблем – електроподаване, доставка на интернет, претоварване на системата). (**ВЕР = 0**)

При нарушение на наличността или целостта, при което **като последствие има неналична услуга**, по преценка може да се коригира ВЕР (да се увеличи или намали с 0,5 или 0,25) според времето за възстановяване на услугата като се отчитат два фактора - моментът на *установяване на неналичие на услугата* и моментът на *възстановяване на услугата*. В зависимост от естеството на услугата, времевите измерения продлежат на преценка. Например, ако системата за проверка на документи не работи при преминаване на граница, тогава 1 ден би бил твърде голям срок за възстановяване на услугата, докато в други случаи възстановяването би могло да отнеме няколко дни без да доведе до някакви сериозни последствия за физическите лица.

Настоящата методика е изготвена на основание чл. 62, т. 2, б. „в“ от Правилника за дейността на КЗЛД и на нейната администрация и приета с решение на КЗЛД на заседание, проведено на 29 май 2020 г. (Протокол № 23), изменена и допълнена с решение на КЗЛД на заседание, проведено на 24 юни 2021 г. (Протокол № 27).