ДЕТСКА ГРАДИНА „НЕЗАБРАВКА“ ,ГР.МИЗИЯ

гр.Мизия, ул.”Петко Банков” № 7,
тел.0892 234 125,
e-mail:info-609168@edu.mon.bg

УТВЪРДЕНА: Tsvetanka Kirilova Damyanova Digitally signed by Tsvetanka Kirilova Damyanova Date: 2026.10.04 21:06:02 +03'00'
Директор:Цветанка Дамянова
Заповед №РД 01-05-141/04.10.2026 год.

ПРОЦЕДУРА ЗА ДЕЙСТВИЯ ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В ДГ „НЕЗАБРАВКА“

Процедурата е разработена с цел да подпомогне дейността на ДГ „Незабравка“ при реагиране на нарушения на сигурността на личните данни.

1. Терминологични уточнения – по смисъла на тази процедура:

1.1. „Нарушение на сигурността на личните данни“ е нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин (чл. 4, т. 12 от Регламент (ЕС) 2016/679).

1.2. „Унищожаване“ е налице, когато личните данни ги няма или ги няма във вид, в който администраторът може да ги използва.

1.3. „Повреждане“ е налице, когато личните данни са променени, подправени или станали вече непълни.

1.4. „Загубата“ е състояние, при което данните може все още да са налични, но администраторът е загубил контрол или достъп до тях или те не са вече притежавани от него.

1.5. „Неразрешено разкриване“ е разкриване на лични данни пред или предоставяне на достъп до тях на получатели, които не са оправомощени да ги получат или да имат достъп до тях.

2. Признаци за нарушение на сигурността на личните данни

2.1. При установяване на признаци за нарушение на сигурността на личните данни всеки служител на ДГ „Незабравка“ е длъжен незабавно да информира прекия си ръководител, длъжностното лице по защита на данните и директора на детската градина/училището.

2.2. Признаците на нарушенията на сигурността могат да включват: индикатори от системите за физическа защита, загуба на документи, съдържащи лични данни или на носители на лични данни, недостъпност на информационни системи, в които се обработват лични данни и други подобни, при които е вероятно да има унищожаване, повреждане, загуба или нерегламентиран достъп до лични данни.

3. Установяване на естеството на нарушението

3.1. Длъжностното лице по защита на данните преценява дали има нарушение на сигурността на личните данни и ако да, в какво се изразява неговото естество.

3.2. Нарушенията на сигурността на личните данни се категоризират в следните видове, както и в каквато и да е комбинация от тях:

а) нарушение на поверителността – когато има неразрешено или случайно разкриване или достъп до лични данни;

б) нарушение на целостта – когато има неразрешена или случайна промяна на лични данни;

в) нарушение на наличността – когато има неразрешена или случайна загуба на достъп до или унищожаване на лични данни. Загуба на наличността за определен период от време също е вид нарушение, ако може да окаже значително въздействие върху правата и свободите на физическите лица.

Естеството на нарушението се отчита при прилагане на мерките за справяне с последиците от нарушението на сигурността на личните данни.

3.3. Преценката на длъжностното лице по защита на данните се предоставя на директора на детската градина/училището във възможно най-кратък срок.

4. Анализ на риска от нарушението за правата и свободите на физическите лица

4.1. Рискът се определя като възможност за настъпване на имуществена или неимуществена вреда за субекта на данните при определени условия, оценена от гледна точка на нейната тежест и вероятност (§ 1, т. 16 от Допълнителните разпоредби на Закона за защита на личните данни).

4.2. При определяне на вероятността и тежестта на риска се отчитат следните обстоятелства:

а) естество на данните, обект на нарушението на сигурността – рискът може да бъде различен в зависимост от това дали данните, обект на нарушението, са „обикновени“ или специални категории, или данни, свързани с присъди и нарушения. Очаквано е рискът да е по-висок при специалните категории лични данни и при личните данни, свързани с присъди и нарушения.

б) обхват на нарушението – каква част от обработваните лични данни засяга; засегнатите лични данни представляват ли значителен обем на регионално, национално или наднационално равнище; с течение на времето обхватът на нарушението може ли да нараства като мащаб.

в) контекст на обработването – определяне на обстоятелствата, при които са обработвани личните данни, например в трудовия контекст, обработване за статистически изследвания, има ли трансгранично движение на личните данни, предавани ли са извън Европейския съюз, което може да затрудни физическите лица могат да упражняват правата си в областта на защитата на данните.

г) цел на обработването – отчитане на първоначалните цели, за които данните а събирани, но и всякакви други съвместими с тях последващи цели, за които данните са използвани. Анализът на риска трябва да отчита евентуалното засягане на правата и свободите на субектите при обработване на всички цели на обработването.

д) естество на нарушението – категоризация дали нарушението засяга поверителността, целостта или наличността на личните данни или представлява комбинация от тях.

е). лесната на идентифициране на физическите лица – рискът се увеличава, ако въз основа на личните данни, засегнати от нарушението, физическите лица се идентифицират или лесно могат да бъдат идентифицирани, респ. се изключва, ако лицата не могат да бъдат идентифицирани.

ж). сериозност на последиците за засегнатите лица – отчита се като комбинация от вероятността за настъпване на вредоносни последици (ниска, средна, висока) и тяхната тежест, определена според засегнатите права и свободи.

з) специални характеристики на засегнатите физическите лица – изследва се дали кръгът на засегнатите лица е съставен от уязвими групи, например деца, служители и други с оглед особеностите на конкретния случай.

и) приблизителен брой на засегнатите физически лица – определяне като общ брой, а при възможност диференциране според естеството на нарушението.

й) приблизителен брой на засегнатите записи от лични данни – индикативно за обхвата на нарушението.

4.3. Риск от нарушението на сигурността на личните данни е налице, когато администраторът не е в състояние да спазва принципите, свързани с обработването на личните данни – законосъобразност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, отчетност.

4.4. Висок риск от нарушение на сигурността на личните данни има, когато могат да бъдат причинени физически, материални или нематериални вреди за засегнатите физически лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица. Високият риск може да произтича от уязвимостта на лицата, чиито данни се обработват, например деца, или от обема на личните данни и засягането на голям брой субекти на данни.

4.5. За обективност на анализа се използват Препоръките за методология на оценката на тежестта на нарушенията на личните данни (Recommendations for a methodology of the assessment of severity of personal data breaches) на Агенцията на Европейския съюз за киберсигурност (European Union Agency for Cybersecurity, ENISA), част от които се съдържат в Приложение 1 към настоящата процедура.

4.6. Администраторът, респ. длъжностното лице по защита на данните документира анализа, който прави относно тежестта на нарушението и на рисковете, които то поражда, в съответствие с принципа на отчетност.

5. Предприемане на мерки за ограничаване на неблагоприятните последици

5.1. В зависимост от вида на нарушението на сигурността на личните данни, се предприемат мерки за ограничаване на неблагоприятните му последици в следните насоки:

а) при нарушение на поверителността: незабавно преустановяване на неразрешения достъп до лични данни; заличаване на личните данни във всички неразрешени публикации, включително отправяне на искания за премахване от кеширани версии на интернет страници, където са били публикувани; криптиране на лични данни при тяхното изпращане; уведомяване на прокуратурата и полицията, ако деянието съставлява престъпление; временно преустановяване на достъпа до електронна услуга, която е обект на нарушението; други мерки с превантивен или последващ характер;

б) при нарушение на цялостността: възстановяване на данните в състоянието преди неразрешената или случайната промяна; установяване дали неточни данни са предадени на получатели; уведомяване на получателите за коригиране на данните; други мерки с превантивен или последващ характер;

в) при нарушение на наличността: определяне дали неразрешената или случайната загуба на достъп до лични данни е за определен период от време или постоянна; възстановяване на личните данни от резервни копия или от други източници; определяне дали има негативно въздействие върху правата и свободите на засегнатите физически лица от загубата на наличността; други мерки с превантивен или последващ характер.

5.2. Ако не е възможно да бъдат идентифицирани подходящи мерки за овладяване на нарушението на сигурността на личните данни, се предприема незабавно уведомяване на надзорния орган.

6. Уведомяване на надзорния орган за нарушението на сигурността на личните данни

6.1. На основание чл. 33 от Регламент (ЕС) 2016/679 администраторът уведомява надзорния орган – за Република България Комисията за защита на личните данни, адрес София 1592, бул. „Проф. Цветан Лазаров“ № 2, електронна поща kzld@cpdp.bg, интернет страница www.cpdp.bg. Задължението за уведомяване на надзорния орган се прилага в случай, че съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Без значение какво е нивото на риска, но такъв трябва да е идентифициран. Например няма да има риск, респ. не се изисква уведомяване на надзорния орган, ако е откраднатa/изгубена флаш памет с криптирани данни и уникалният код не е разкрит. Ако кодът е разкрит по-късно, уведомяването е задължително. Не се изисква уведомяване при краткотрайна загуба на наличността, например при прекъсване на електрозахранването, но такъв инцидент подлежи на вписване в регистъра на нарушенията на сигурността на личните данни.

6.2. Уведомяването на надзорния орган се извършва без ненужно забавяне и по възможност най-късно до 72 часа след узнаване за нарушението. Ако не могат да бъдат предприети мерки за ограничаване на неблагоприятните последици, надзорният орган се уведомява незабавно.

6.3. Информацията до надзорния орган трябва да съдържа обстоятелствата по чл. 33, пар. 3 от Регламент (ЕС) 2016/679, като за уведомяването се използва формулярът, утвърден от Комисията за защита на личните данни, публикуван на уеб сайта на Комисията cpdp.bg:

https://www.cpdp.bg/userfiles/file/Documents_2021/UVEDOMLENIE%20po%20chl_%2033%20GDPR.pdf

Ако уведомлението е подадено след изтичане на 72-часовия срок от узнаването, в него трябва да се съдържат и причините за забавянето.

6.4. Регламент (ЕС) 2016/679 допуска информацията в уведомлението да се подава поетапно, когато и доколкото не е възможно да се даде едновременно. Поетапното уведомяване вероятно ще се прилага при по-сложни инциденти, при които пълното изясняване на обстоятелствата не е възможно в срока за уведомяване.

7. Съобщаване на засегнатите от нарушението субекти на данни

7.1. Съобщаване на засегнатите от нарушението на сигурността субекти на данни се изисква, когато *има вероятност нарушението да породи висок риск за правата и свободите на физическите лица.* При определянето на риска се вземат предвид всички обстоятелства по т. 4 от настоящата процедура, както и нововъзникнали, новонастъпили или узнати, открити или по друг начин станали впоследствие известни на администратора обстоятелства след извършването на анализа на риска.

7.2. Не е предвиден срок за съобщаване на нарушението на субекта на данни, но това се прави, когато е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват дадените от него насоки.

7.3. Съобщението трябва да се направи на ясен и прост език и да съдържа:

а) описание на естеството на нарушението на сигурността на личните данни;
б) посочване на името и координатите за връзка с длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
в) описание на евентуалните последици от нарушението;
г) описание на предприетите или предложените от администратора мерки за справяне с нарушението и за намаляване на евентуалните неблагоприятни последици.

7.4. В чл. 34, пар. 3 от Регламент (ЕС) 2017/679 са посочени три алтернативни условия, при които съобщаване на нарушението на субекта на данни не се изисква:

а) администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
в) съобщаването би довело до непропорционални усилия, в който случай Регламентът изисква да се направи публично съобщение или да се вземе друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

Ако реши да се позове на някое от тези условия, администраторът трябва да е в състояние да докаже на надзорния орган, че са налице съответните предпоставки. Предвид това е целесъобразно да бъдат документирани обстоятелствата, послужили като основание да не се съобщи нарушението на засегнатите субекти на данни.

8. Документиране на нарушението

Администраторът е задължен да документира всяко нарушение на сигурността на личните данни, без значение дали съществува вероятност от него да се породи риск или да настъпи висок риск за правата и свободите на физическите лица. Регламент (ЕС) 2016/679 изрично

посочва значението на тази документация – да дава възможност на надзорния орган да провери дали са спазени изискванията на чл. 33 от Регламент (ЕС) 2016/679. За целта длъжностното лице по защита на данните своевременно попълва регистъра на нарушенията на сигурността на личните данни, предвиден като образец във Вътрешните правила за защита на личните данни.

Приложение 1
Към т. 4.5 от
Процедура за действия при нарушения
на сигурността на личните данни

ПРЕПОРЪКИ ЗА МЕТОДОЛОГИЯ НА ОЦЕНКА НА ТЕЖЕСТТА НА НАРУШЕНИЯТА НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

1. Ниво на риск

Тежестта на нарушението на сигурността на личните данни в контекста на тази методика се определя като ***„оценка на степента на потенциалното въздействие върху лицата, в резултат от нарушаването на сигурността на данните“.*** С използването на тази методика администраторът на лични данни се ръководи през процеса от конкретни количествени критерии, за да направи цялостно оценката. Съобразено с възможните изисквания за уведомяване (съгласно чл. 33 и чл. 34 от Регламент (ЕС) 2016/679), нивата на риск се определят, както следва:

1.1. без риск;
1.2. риск;
1.3. висок риск.

2. Критерии

Основните критерии, взети под внимание при оценката на тежестта на дадено нарушаване на сигурността на личните данни, са:

2.1. контекст на обработването на данни **(КО) –** Отнася се до вида на нарушените данни, заедно с редица фактори, свързани с общия контекст на обработка;
2.2. възможност за идентификация на субекта на данни **(ВИ)**: Определя колко лесно може да се установи идентичността на лицата от данните, участващи в нарушението;
2.3. обстоятелства относно нарушението **(ОН)**: Отнася се до конкретните обстоятелства, свързани с нарушението, които са свързани с вида на нарушението, в това число най-вече загубата на сигурността на данните, както и всяка свързана злонамерена умисъл.

3. Формула за изчисляване на тежестта на риска от нарушение на сигурността на личните данни

Въз основа на горните критерии подходът на тези методика е следният:

3.1. КО е в основата на методиката и оценява критичността на даден набор от данни в конкретен контекст на обработване;
3.2. ВИ е коригиращ фактор на **КО.** Общата критичност на нарушението на защитата на личните данни може да бъде намалена в зависимост от стойността на **ВИ.** Колкото е по-ниска възможността за идентифициране, толкова по-ниска се получава общата оценка. Комбинацията от КО и ВИ (умножение) два първоначалния резултат за тежестта на нарушената сигурност на данните.
3.3. ОН количествено определя конкретни обстоятелства на нарушението, които в определена ситуация могат да са налице или не. Когато са налице определени обстоятелства

относно пробива, те само могат да увеличат тежестта на конкретното нарушение. Поради тази причина първоначалната оценка може да бъде допълнително коригирана от обстоятелствата относно нарушението.

Изчисляването на риска се извършва по следната формула: **РИСК = КО х ВИ + ОН**

4. Оценка на критериите

4.1. Оценка на контекста на обработването на данни (КО)

Определянето на резултата от контекста на обработването (КО) се извършва в две последователни стъпки:

Стъпка 1 – Определяне на базова оценка на КО - Определяне на видовете лични данни, участващи в нарушението и тяхното класифициране в една от четирите категории: обикновени, поведенчески, финансови, специални категории лични данни.

Стъпка 2 – Оценка на появата на определени фактори, които биха могли да увеличат или съответно да намалят основния резултат.

Таблица за оценка на контекста на обработване на данните (КО)

Група	Описание	Резултат
Обикновени данни	**Биографични данни, данни за контакт, пълно име, данни за образование, данни за семеен живот, професионален опит и т.н.**	**1**
	Предварителен основен резултат: когато нарушението включва „обикновени данни“ и администраторът не знае за утежняващи фактори	**1**
	Резултатът на КО може да бъде увеличен с 1, когато обемът на „обикновените данни“ и/или характеристиките на администратора са такива, че може да се даде възможност за изготвянето на определени профили на индивида или да се направят предположения за социалното/финансовото състояние на лицето.	**2**
	Резултатът на КО може да бъде увеличен с 2, когато обикновените данни и/или характеристиките на администратора могат да доведат до предположения за здравословното състояние на индивида, сексуалните предпочитания, политическите или религиозните вярвания	**3**
	Резултатът на КО може да бъде увеличен с 3, когато поради определени характеристики на индивида (например уязвими групи, непълнолетни), информацията може да бъде от решаващо значение за тяхната лична безопасност или физическо/психологическо състояние.	**4**
Поведенчески данни	**Данни за местонахождение, данни за интернет трафик, данни за лични предпочитания и навици и др.**	**2**
	Предварителен основен резултат: когато нарушението включва „поведенчески данни“ и администраторът не знае за утежняващи или намаляващи фактори	**2**
	Резултатът на КО може да бъде намален с 1, когато естеството на масива от данни не осигурява съществено разбиране за поведенческата информация на лицето или данните могат да бъдат събирани лесно (независимо от нарушението) чрез публично достъпни източници (например комбинация от информация от търсения в мрежата).	**1**
	Резултатът на КО може да бъде увеличен с 1, когато обемът на „поведенческите данни“ и/или характеристиките на администратора са такива, че може да се създаде профил на индивида, излагайки подробна информация за неговия ежедневен живот и навици.	**3**
	Резултатът на КО може да бъде увеличен с 2, когато може да бъде създаден потребителски профил, основан на чувствителните данни на лицето.	**4**
Финансови данни	**Всички видове финансови данни (например доходи, финансови транзакции, банкови извлечения, кредитни карти, фактури и т.н.), включително данни за социалното благосъстояние, данни за притежавано имущество, данни свързани с финансова информация за лицето.**	**3**

	Предварителен основен резултат: когато нарушението включва „финансови данни“ и администраторът не знае за утежняващи или намаляващи фактори	**3**
	Резултатът на КО може да бъде намален с 2, 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**
	Резултатът на КО може да бъде намален с 1, когато конкретният набор от данни съдържа известна финансова информация, но все още не дава никакво съществено разбиране за финансовото състояние/ситуацията на лицето (например числа на обикновени банкови сметки без допълнителни подробности).	**2**
	Резултатът на КО може да бъде увеличен с 1, поради характера и/или обема на конкретния набор от данни се разкрива пълна финансова информация за лицето (например кредитна карта), която би могла да позволи измами или да бъде създаден подробен социален/финансов профил	**4**
Специални категории лични данни	**Данни за расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни за разпознаване, здравословно състояние, сексуален живот, сексуална ориентация**	**4**
	Предварителен основен резултат: когато нарушението включва „чувствителни данни“ и администраторът не знае за ограничаващи риска фактори	**4**
	Резултатът на КО може да бъде намален с 3, когато естеството на масива от данни не осигурява съществено разбиране за поведенческа информация за лицето или данните могат да бъдат събирани лесно (независимо от нарушението) чрез публично достъпни източници (например комбинация от информация от търсения в мрежата).	**1**
	Резултатът на КО може да бъде намален с 2, когато естеството на данните може да доведе само до общи предположения.	**2**
	Резултатът на КО може да бъде намален с 1, когато естеството на данните може да доведе до предположения за чувствителна информация.	**3**

В случай, че данните принадлежат към повече от една категория, те се изследват във всяка от тях и се взема най-високия получен резултат.

При оценката на КО, следва да се вземат предвид някои фактори, които биха увеличили или съответно намалили риска от нарушението:

1. **Увеличаващи риска фактори**
   - **а) обем на данните** (количеството засегната информация за всеки отделен субект на данни, отчитайки времевия период и съдържанието) - обемът на нарушените данни (за едно и също лице) може да увеличи основния резултат на КО, поради увеличаването на количеството на нарушената информация (т.е. действа като утежняващ фактор). Обемът трябва да се разглежда както по отношение на времето (напр. един и същ вид данни за определен период от време), така и по отношение на съдържанието (допълващи данни от същия вид). Например, в случай на нарушение на сигурността на данните за трафика при интернет доставчик, резултатът на КО би бил по-висок (за едно и също лице), ако данните обхващат период от една година, отколкото ако са ограничени до една седмица (време). Като друг пример, в случай на нарушение в банка, резултатът на КО на пълното досие на дадено лице би бил по-висок от този на един документ от същото досие (съдържание).
   - **б) особености на администратора** (по отношение на сектора и услугите, които предлагат);
   - **в) особености на физическите лица** (по отношение на обхващането на специфични групи, например субекти в неравностойно положение, деца, други);

г) ключови данни (част от данните позволяват при комбинирането им с други такива, вкл. публично достъпна информация, за да се получи завършено поведенческо профилиране на субекта).

2. Намаляващи риска фактори

а) невалидност/неточност на данните (поради давност във времето или неточност или непълнота на съдържанието) - основният резултат на КО за определен набор от данни може да бъде намален, ако невалидността или неточността на данните са известни на администратора (например поради тяхната давност или съдържание) и по този начин тяхната значимост е намалена. Администраторът трябва да е сигурен в това обстоятелство, за да го включи в оценката.

б) обществена достъпност основният резултат на КО за набор от данни също може да бъде намален в случай, че нарушените данни вече са били обществено достъпни преди нарушението или могат лесно да бъдат събрани и / или достъпни чрез обществено достъпни източници;

в) естество на данните (данни от общ оценъчен характер без допълнителни данни за изграждащото ги съдържание) - друг понижаващ фактор може в някои случаи да бъде самото естество на определен набор от данни, който, въпреки първоначалния си резултат за КО, е с по-малка значимост по отношение на информацията, която може да разкрие за лицето. Такъв е например случаят с медицинско свидетелство, което само удостоверява, че физическото лице е в добро здравословно състояние, без да разкрива друга информация. В този случай, въпреки че основният резултат ще се дължи на това, че данните за здравето са чувствителни данни, крайният резултат на КО за набора от данни ще бъде 1, тъй като той сам по себе си не може да повлияе на личния живот. Този фактор обаче трябва да се разглежда с голямо внимание и ясно обяснение на причината, поради която определено обработване на данни по своята същност е по-ниско от основната резултат на КО.

4.2. Оценка на възможността за идентификация на субекта на данни (ВИ)

Възможността за идентификация на субекта на данни (ВИ) оценява колко лесно ще бъде за дадена страна, която има достъп до набора от данни, да ги съпостави еднозначно с определено лице.

За целите на тази методика са дефинирани четири нива на ВИ (пренебрежимо, ограничено, значимо и максимално) с линейно увеличение на резултата. Най-ниска оценка се дава, когато възможността за идентифициране на лицето е пренебрежима, което означава, че е изключително трудно да се съпоставят данните с конкретно лице, но въпреки това би могло да бъде възможно при определени условия. Най-високата оценка се дава, когато идентифицирането е възможно директно от нарушаването на сигурността на данните, без да са необходими специални проучвания, за да се открие самоличността на лицето.

Когато се определя ВИ, трябва да се вземе предвид, че идентификацията може да бъде пряка (например, въз основа на дадено име) или косвена (например, въз основа на идентификационен номер) вследствие на нарушаването на сигурността на данните, но може да зависи и от конкретния контекст на нарушението.

Нивото е производно и на възможността за комбиниране на придобитите данни с публични такива или на трети страни, което да позволи идентифицирането на субекта.

Таблица за оценка на възможността за идентификация на субекта на данни

Ниво	Пренебрежимо	Ограничено	Значително	Максимално
Стойност	0.25	0.5	0.75	1

4.3. Оценка на обстоятелствата относно нарушението на сигурността (ОН)

Обстоятелствата, относно нарушението се изчисляват въз основа на вида на нарушението на сигурността и неговия характер (случаен или целенасочен/злонамерен)**.** Елементите, които се разглеждат във връзка с ОП, са загубата на сигурност (конфиденциалност, цялостност, достъпност) и злонамереност, и допълват КО и ВИ, както следва:

1. **Нарушаване на поверителността:** Нарушаването на поверителност възниква, когато информацията се достъпва от страни, които не са упълномощени или нямат законна цел да получат достъп до нея. Степента на нарушаване на поверителността варира в зависимост от обхвата на оповестяване, т.е. потенциалният брой и вид на страните, които могат да имат незаконно достъп до информацията.
2. **Нарушаване на целостта**: нарушаването на целостта възниква, когато първоначалната информация е променена и замяната на данните може да бъде вредна за лицето. Най-тежката ситуация възниква, когато има сериозни възможности променените данни да бъдат използвани по начин, който може да навреди на лицето.
3. **Загуба на наличност:** Загуба на наличност възниква, когато оригиналните данни не могат да бъдат достъпни, когато има нужда от тях. Тя може да бъде временна (данните могат да бъдат възстановими, но ще отнеме време и това може да бъде пагубно за лицето), или постоянна (данните не могат да бъдат възстановени).
4. **Злонамереност:** Този елемент изследва дали нарушението се дължи на грешка, човешка или техническа, или е причинено от умишлено действие на злонамереност. Не злонамерените нарушения включват случаи на случайна загуба, неправилно унищожаване, човешка грешка и грешка в софтуера или неправилна конфигурация. Злоумишлените нарушения включват случаи на кражба и хакерство с цел да навредят на лицата (например, чрез представяне на личните им данни на неоторизирани трети страни). В други случаи злонамереността може да включва прехвърляне на лични данни на трети страни с цел печалба (например, продажба на списъци с лични данни). В някои случаи злонамереността може също да бъде подсказана от действия, целящи да навредят на администратора на данни (например, чрез кражба и представяне на лични данни на неоторизирани страни). Злоумишленото намерение е фактор, който увеличава вероятността данните да бъдат използвани по вреден начин, тъй като това е била първоначалната цел на нарушението.

Възможно е да са налице повече от едно от гореизброените обстоятелства. В тези случай, общото обстоятелство е равно на сбора на стойностите на отделните обстоятелства.

Таблица за оценка на обстоятелства, относно нарушението по категории

Категории	Стойност	Примери
Конфиденциалност	**0**	Личните данни, изложени на риск **без доказателства за настъпила незаконна обработка, например:** • при пренос се загубва документ или лаптоп; • оборудването е изхвърлено без унищожаване на личните данни
	0.25	Личните данни са предоставени на известни получатели, например:

		• e-mail с лични данни е изпратен неправилно до известен брой получатели; • някои клиенти имат достъп до акаунти на други клиенти в онлайн услуга.
	0.5	Личните данни са предоставени на неизвестен брой получатели, например: • данните са публикувани на общодостъпно място в интернет; • служител продава служебна информация, съдържащата лични данни; • неправилно конфигуриран уеб сайт прави лични данни публично достъпни чрез данни на вътрешни потребители
Цялостност	**0**	Променени лични данни, но без определена неправилна или незаконна употреба: • записите на база с лични данни са актуализирани неправилно, но оригиналът е възстановен, преди да е настъпило каквото и да е използване на променените данни
	0.25	Лични данни са променени и евентуално използвани по неправилен или незаконен начин, но с възможност да се възстановят, например: • записът, необходим за предоставянето на електронна услуга, е променен и лицето трябва да поиска услугата по офлайн начин; • документ, който е важен за точността на данните на субекта в електронна услуга, е променен;
	0.5	Личните данни са променени и евентуално използвани по неправилен или незаконен начин, без възможност за възстановяване: • предишните примери, но оригиналите не могат да бъдат възстановени
Наличност	**0**	Възстановяване на данни без затруднения: • копие от файла се губи, но има други копия; • базата данни е повредена, но може лесно да бъде възстановена от други бази данни
	0.25	Временна загуба на наличност: • базата данни е повредена, но може да бъде възстановена от други бази данни, макар да изисква допълнителна обработка; • файлът е изгубен, но информацията може да бъде предоставена отново от субекта
	0.5	Пълна липса на данни (данните не могат да бъдат възстановени от администратора или от субекта на данни): • файлът е изгубен, базата данни е повредена, няма резервно копие на тази информация и тя не може да бъде предоставена от субекта.
Злонамереност	**0.5**	Нарушението се дължи на умишлено действие, напр. за да причини проблем на администратора (например демонстриране на загуба на сигурност) и / или с цел да навреди на субектите. Например: • служител на администратора умишлено споделя лични данни публично, в социалните медии; • служител на администратора продава лични данни на трети страни;

В случай, че се касае за **нарушение на цялостността или наличността на лични данни, които не могат да бъдат възстановени поради тяхната уникалност** и те са **необходими за осъществяване на правата и свободите на субектите на данни,** нивото на риска директно се приема за **високо.**

5. Определяне на нивото на риска от нарушението на сигурността на личните данни

Общата тежест на риска от нарушението се изчислява по следната формула:

РИСК = КО x ВИ + ОН

Крайният резултат показва нивото на тежест на риска от нарушението, като се отчита въздействието върху лицата.

Извършва се следното приравняване на изчисления риск към нивото на риск и възможните последици

Ниво на риск	Приравняване	Възможни последици
Без риск	**РИСК < 2**	субектите на данни е възможно да изпитат няколко незначителни неудобства, които ще преодолеят без никакъв проблем (време, прекарано в повторно въвеждане на повторна информация, раздразнение, объркване)
Нисък риск	**2 ≤ РИСК < 3**	субектите на данни е възможно да изпитат значителни неудобства, които те ще могат да преодолеят въпреки някои трудности (допълнителни разходи, отказ от достъп до услуги, страх, липса на разбиране, стрес, дребни физически неразположения и т.н.)
Висок риск	**3 ≤ РИСК**	субектите на данни е възможно да се сблъскат със значителни последствия, които те би следвало да могат да преодолеят, макар и със сериозни затруднения или дори необратими последствия, които не могат да преодолеят (злоупотреби с финансови средства, поставяне в черни списъци от финансови институции, имуществени щети, загуба на работа, призовка, влошаване на здравето, загуба на работа, дългосрочни психологически или физически неразположения, подлагане на дискриминация, смърт)

6. Отчитане на специфични обстоятелства

След като бъде определено нивото на тежестта на риска от нарушението на сигурността, то може да бъде придружено от специфични обстоятелства, показващи определени елементи на нарушението, които, макар и да не засягат априори резултата, са важни за окончателната оценка. За целите на методиката са разгледани две специфични обстоятелства:

6.1. Брой на лицата, спрямо които е извършено нарушение. Данни за физическо лице, което е обект на нарушение в контекста на по-голям инцидент, потенциално могат да бъдат разкрити по-лесно, докато в същото време голям брой засегнати лица влияят върху общия мащаб на нарушението.

6.2. Данните са неразбираеми. Неразбираемостта (При придобиване на криптирани данни, без ключа за декриптиране да е станал достояние) може значително да намали въздействието върху лицата, тъй като силно намалява възможността на неоторизирани страни да имат достъп до данните.

В зависимост от полученият от оценката на риска, се предприемат действията предвидени в Процедурата за действия при нарушение на сигурността на личните данни в ДГ „Незабравка“

Тази процедура е утвърдена със Заповед №РД 01-05-141/04.10.2026г. на директора на ДГ „Незабравка“ и влиза в сила от датата на утвърждаването ѝ.