Приложение № 1 Методология за оценка на тежестта на пробив в сигурността

Приложение № 1

към раздел IV, т. 11 Методология за оценка на тежестта на пробив в сигурността на личните данни

Методология за оценка на тежестта на пробив в сигурността на личните данни

Въведение

1. Настоящата методология за оценка на тежестта на пробив в сигурността на личните данни разглежда изискванията, посочени в чл. 33 и чл. 34 от ОРЗД за уведомяване на надзорните органи и субекти на данни за установени пробиви в сигурността в контекста на адаптирана Методология за оценка на степента на тежест на нарушение на сигурността на личните данни, разработена и публикувана от European Union Agency for Network and Information Security (Агенция за мрежова и информационна сигурност на Европейския съюз).

Нормативни ограничения

2. Уведомленията по чл.33 и чл.34 **са задължителни само** в следните случаи:

   2.1. надзорният орган се уведомява само ако пробивът **може да доведе до риск** за правата и свободите на субектите на данни, засегнати от този пробив;

   2.2. субектът на данни се уведомява само ако пробивът **може да доведе до висок риск** за правата и свободите на субектите на данни, засегнати от този пробив.

Пробив в сигурността

3. Под **пробив в сигурността** следва да се разбира пробив в:

   3.1. достъпа до информацията (конфиденциалност) - неразрешено или случайно разкриване на или достъп до лични данни;

   3.2. целостта на информацията (интегритет) - неразрешена или случайна промяна на личните данни;

   3.3. наличността на информацията (наличност) - случайна или неразрешена загуба на достъп до или унищожаване на лични данни.

Рискове

4. Съгласно ОРЗД рискът за правата и свободите на физическите лица, с различна вероятност и тежест произтича от обработване на лични данни:

   4.1. което би могло да доведе до физически, материални или нематериални вреди, по-специално когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване

на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия;

4.2. когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни;

4.3. които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална институция, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност;

4.4. оценяващо лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили;

4.5. на уязвими лица, по-специално на деца;

4.6. включващо голям обем лични данни и засяга голям брой субекти на данни.

Ниво на риск

5. Следните нива на риска се припознават от институцията, съобразено с възможните изисквания за уведомяване:

5.1. без риск;

5.2. нисък риск;

5.3. висок риск.

Оценка на риска

6. Критериите, използвани за оценка на риска, са:

6.1. контекст на обработването на данни (КО)

6.2. възможност за идентификация на субекта на данни (ВИ)

6.3. обстоятелства относно пробива (ОП)

7. Изчисляването на риска се извършва по следната формула

РИСК = КО x ВИ + ОП

8. 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

		информация, раздразнение, объркване и т.н.)
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 изпитат значителни последствия, които биха преодолели, макар и със сериозни трудности или необратими последици, които не могат да преодолеят (злоупотреби с финансови средства, черни списъци от финансови институции, имуществени щети, загуба на работа, призовка, влошаване на здравето, неработоспособност, дългосрочни психологически или физически заболявания, подлагане на дискриминация, смърт)

Обстоятелства относно пробива

9. Обстоятелствата, относно пробива се изчисляват въз основа на вида на пробива в сигурността и неговия характер (случаен или целенасочен/злонамерен).

9.1. злонамерен характер предполага, че пробивът не е в следствие на грешка, човешка или техническа, или е причинен от умишлено действие на злонамерено намерение.

9.2. незлонамерените нарушения включват случаи на случайна загуба, неадекватно изхвърляне, човешка грешка и софтуерни грешки или неправилно конфигуриране.

9.3. злонамерените нарушения могат да включват (неизчерпателно):

а) случаи на кражба и „хакване“ с цел да се навреди на субектите (например чрез излагане на личните им данни на неупълномощени трети страни);

б) прехвърляне на лични данни на трети страни с цел печалба (например продажба на списъци на лични данни);

в) действия, целящи да навредят на администратора на данни (например чрез кражба и предаване на лични данни на неразрешени страни).

9.4. възможно е да са налице повече от едно обстоятелство. В този случай, общото обстоятелство е равно на сбора на стойностите на отделните обстоятелства.

9.5. примери за оценка на обстоятелства, относно пробива по категории (бази):

Приложение № 1 Методология за оценка на тежестта на пробив в сигурността

База	Стойност	Примери
Конфиденциалност	0	Примери за данни, изложени на риск **без доказателства за настъпила незаконна обработка:** • при пренос се загубва хартиен файл или лаптоп; • оборудването е изхвърлено без унищожаване на личните данни.
	0.25	Примери за данни, предоставени на **известни** получатели: • 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	Примери за данни, предоставени на **неизвестен** брой получатели: • данните се публикуват в интернет съвет за съобщения; • данните се качват на P2P сайт; • служител продава CD ROM с данни за клиента; • неправилно конфигуриран уеб сайт ги прави публично достъпни чрез интернет данни на вътрешни потребители
Интегритет	0	Примери за **променени 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	Примери за **данни, променени и евентуално използвани по неправилен или незаконен начин**, но с възможност да се възстановят: • записът, необходим за предоставянето на онлайн социална услуга, е променен и лицето трябва да поиска услугата по офлайн начин; • документ, който е важен за точността на файла на индивида в онлайн медицинска услуга, е променен
	0.5	Примери за данни, **променени и евентуално използвани по неправилен или незаконен начин,** без възможност за това възстановяване: • предишните примери, но оригиналите не могат да бъдат възстановени.
Наличност	0	Примери за **възстановяване на данни без**

Приложение № 1 Методология за оценка на тежестта на пробив в сигурността

		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	Примери за **временна неналичност**: • базата данни е повредена, но може да бъде възстановена от други бази данни, макар чрез допълнителна обработка; • файлът е изгубен, но информацията може да бъде предоставена отново от субекта.
	0.5	Примери за **пълна липса на данни** (данните не могат да бъдат възстановени от администратора или от физически лица): • 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: • служител на институцията умишлено споделя частни данни публично в социалните медии; • служител на институцията продава частни данни на друга компания; • членовете на дадена социална мрежа умишлено изпращат информация до други членове на семейството на субекта, за да им навредят

Контекст на обработването на данни

10. Контекстът на обработваните данни се определя от тяхната дефиниция и свързване с една от следните групи, на базата на която се получава базовата стойност:

Група	**Описание**	**Базова стойност**
Прости данни	биографични данни, данни за контакт, пълно име, данни за образованието, семейния живот, професионалния опит и т.н.	1
Поведенчески данни	местоположение, данни за трафика, данни за личните предпочитания и навици и др.	2
Финансови	всички видове финансови данни (например доходи, финансови транзакции, банкови	3

данни	извлечения, инвестиции, кредитни карти, фактури и т.н.), вкл. данни за социалното благосъстояние, свързани с финансовата информация	
Чувствителни данни	съгласно ОРЗД 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

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

12. Базовата стойност е възможно да бъде адаптирана, отчитайки други контекстни фактори

    12.1. Увеличаващи риска фактори

    а) обем на данните (включително като време и/или съдържание);

    б) особености на администраторите (по отношение на сектора и продуктите/услугите, които предлагат);

    в) особености на физическите лица (по отношение на обхващането на специфични групи от субекти напр. неравностойно положение, деца);

    г) ключови данни (част от данните позволяват при комбинирането им с други такива, вкл. публично достъпна информация, да се получат завършени профили или предположения).

    12.2. Намаляващи риска фактори

    а) невалидност/неточност на данните (поради давност във времето или неточност или непълнота на съдържанието);

    б) публична наличност (данните са били публично достъпни преди нарушението);

    в) естество на данните (данни от общ оценъчен характер без допълнителни данни за изграждащото ги съдържание – например общ успех).

13. Следната таблица показва възможна контекстуална адаптация на базовата стойност на отделните групи:

Група	**Адаптиране**	**Нова стойност**
Прости данни (БС:1)	Обемът на „простите 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	2

Приложение № 1 Методология за оценка на тежестта на пробив в сигурността

	социалното/финансовото състояние на лицето.	
	„Простите данни“ и/или характеристиките на администратора могат да доведат до предположения за здравословното състояние на индивида, сексуалните предпочитания, политическите или религиозните вярвания.	3
	Поради определени характеристики на индивида (например уязвими групи, непълнолетни), информацията може да бъде от решаващо значение за тяхната лична безопасност или физически/психологически условия.	4
Поведенчески данни (БС:2)	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
	Обемът на „поведенческите данни“ и/или характеристиките на контролера са такива, че може да се създаде профил на индивида, излагайки подробна информация за неговия ежедневен живот и навици.	3
	Може да бъде създаден потребителски профил, основан на чувствителните данни на лицето.	4
Финансови данни (БС:3)	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
	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
	Поради характера и/или обема на конкретния набор от данни се оповестява пълна финансова информация (например кредитна карта), която би могла да позволи измами или да бъде създаден подробен социален/финансов профил.	4
Чувствителни данни	Естеството на масива от данни не осигурява съществено разбиране за поведенческата информация на лицето или данните могат да бъдат събирани лесно (независимо от	1

(БС:4)	нарушението) чрез публично достъпни източници (например комбинация от информация от търсения в мрежата).	
	Естеството на данните може да доведе само до общи предположения.	2
	Естеството на данните може да доведе до предположения за чувствителна информация.	3

Възможност за идентификация на субекта на данни

14. Дефинирани са четири нива на оценка на възможната идентификация на субекта на данни. Най-ниската оценка е в случай, че изключително може трудно да се установи субектът, макар и да е възможно. Най-високата оценка предполага директно идентифициране на субекта от придобитите данни.

Ниво	Пренебрежимо	Ограничено	Значително	Максимално
Стойност	0.25	0.5	0.75	1

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

16. При придобиване на криптирани данни, без ключа за декриптиране да е станал достояние, възможността за идентификация се приема за 0.

Специфични фактори

17. В случай, че се касае за **нарушение на интегритета 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**, то нивото на риска се приема за **високо**.