Детска градина „Радост”
ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

З А П О В Е Д

№ РД-09-328

гр. Севлиево, 11.03.2024 г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование и чл. 33 и 34 от Регламента (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. и във връзка с необходимостта от защитата на физическите лица при обработването на лични данни

I. УТВЪРЖДАВАМ:

1. Инструкция за действие при пробив в сигурността на личните данни с приложения, както следва:
   1.1. Методология за оценка на тежестта на пробив в сигурността на личните данни;
   1.2. Уведомление до надзорния орган;
   1.3. Съобщение до субекта на данните за нарушение на сигурността на личните данни;
   1.4. Регистър на нарушения на сигурността на личните данни.

II. НАРЕЖДАМ:

2. В срок до десет работни дни от издаването на настоящата заповед, утвърдената Инструкция за действие при пробив в сигурността на личните данни с приложенията ѝ да се доведе до знанието на служителите в институцията за сведение и изпълнение, което се удостоверява лично с подпис.

3. Изпълнението по т. 2 възлагам на Виолета Монева – ЗАС, длъжностното лице по защита на данните.

4. За неизпълнение на разпоредбите на утвърдената Инструкция за действие при пробив в сигурността на личните данни с приложенията ѝ, виновните лица носят дисциплинарна отговорност.

5. Контролът по изпълнението на заповедта ще изпълнявам лично.

ЦАНКА НЕНЧЕВА

Директор на ДГ ”Радост” – Севлиево

Детска градина „Радост"
ПК 5400, гр.Севлиево, ул."Здравец" №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

ИНСТРУКЦИЯ ЗА ДЕЙСТВИЕ ПРИ ПРОБИВ В СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Данни за администратора

Администратор	Детска градина „Радост", град Севлиево
Адрес	ПК 5400, гр.Севлиево, ул."Здравец" №1
E-mail	info-701351@edu.mon.bg
Телефон	0675/ 3-28-46; 8-90-02

Процедура

Раздел I. Предназначение на процедурата

1. Тази процедура следва да се прилага при пробив в сигурността, в съответствие с предвиденото в чл. 33 и 34 от ОРЗД, при който възниква нарушение на сигурността на лични данни, обработвани от институцията.
2. „Нарушение на сигурността на лични данни" означава 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.
3. Констатирането на пробив в сигурността може да наложи предприемане на действия от страна на институцията, свързани с уведомяване на:
   3.1. надзорния орган (напр. КЗЛД), когато институцията е администратор на данните;
   3.2. субекта на данни, който е засегнат от пробива в сигурността, когато институцията е администратор на данните;
   3.3. администратора на данни, когато институцията е обработващ данните.
4. Процедурата следва да се тълкува и прилага в контекста на ОРЗД и приложимото към него законодателство.

Раздел II. Субектен обхват

5. Процедурата се прилага съответно от всички лица, участващи в процеса по обработване на данни, включително персонала на институцията, обработващите данни, трети страни, ръководители на институцията.

Раздел III. Докладване и обобщаване на информация

6. Лицата по т. 5 следва да докладват за установени пробиви в сигурността без забава на директора и на *длъжностното лице по защита на личните данни по заповед – лицето което заема длъжността Завеждащ административна служба.* В случай, че институцията действа в качеството си на обработващ данни, отговорното лице по т. 6 информира за пробива засегнатия от пробива администратор на данни.

7. Отговорното лице по т. 5 следва да обобщи цялата информация, свързана с пробива в сигурността, както следва:

   7.1. когато **институцията е администратор на лични данни**, в съответствие с изискванията на поддържания за целта Регистър на нарушенията на сигурността на личните данни;

   7.2. когато **институцията е обработващ данни**, обобщаването на информацията се извършва съгласно договорността с администратора на данни без ненужно забавяне.

8. Уведомяванията се извършват по следния начин: чрез е-поща или по телефон. По същия начин съответната насрещна страна потвърждава, че е била уведомена.

Раздел IV. Оценка на необходимостта от уведомяване

9. Институцията, в приложимите случаи, проверява дали са налице основания за уведомяване на Надзорен орган и субектите на данни, относно установения пробив в сигурността.

10. Във връзка с посоченото в т. 9 институцията извършва оценка на това, дали пробивът в сигурността на данните може да доведе до риск за правата и свободите на субектите на данни, засегнати от този пробив. Оценката се извършва посредством Методология за оценка на тежестта на пробива (Приложение № 1).

11. За целите на т. 10 лицето по т. 6 може да сформира работна група, включваща квалифицирани служители в областта на установеното нарушение, задължително собственика на информацията в институцията (отговорното лице). **Когато се предполагат злонамерени действия, произхождащи от служители на институцията, независимо от момента на допускане на предположението, с цел избягване на конфликт на интереси, лицата, за които е направено предположението, не могат да бъдат част от тази работна група.**

Раздел V. Уведомяване на Надзорен орган

12. В случай, че бъде установено, че **съществува риск**, по смисъла на т. 10, институцията докладва за пробива в сигурността на данните на надзорния орган (КЗЛД) в рамките на **72 часа** от установяване на пробива (Приложение № 2).

13. Доколкото липсват основания за уведомяване на други надзорни органи, институцията изпраща уведомления до Комисията за защита на личните данни в

Република България (КЗЛД), в случаите, когато е необходимо да се извърши такова уведомяване, съгласно начина и реда, определен от нея.

14. В случай, че срокът по предходната точка не бъде спазен, представляващият институцията или отговорното лице по т. 6. следва да изпрати уведомлението до Надзорния орган, като изложи и причините за забавянето.

15. При невъзможност да се представи цялата необходима информация едновременно, институцията следва да предоставя информацията на части и без необосновано забавяне.

16. На надзорния орган следва да бъде предоставена следната информация:

    16.1. описание на пробива в сигурността;

    16.2. категориите и приблизителния брой на засегнатите субекти на данни;

    16.3. категориите и приблизителния брой на засегнатите записи на лични данни;

    16.4. име и данни за контакт на отговорното лице по т. 6;

    16.5. описание на евентуалните последици от нарушението на сигурността на личните данни;

    16.6. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

17. Комуникацията с надзорния орган се извършва в съответствие с правилата на последния. При липса на други указания, институцията уведомява надзорния орган по е-поща на посочения на официалната електронна страница на надзорния орган e-mail за контакт.

Раздел VI. Уведомяване на субектите на данни

18. В случай, че пробивът в сигурността на личните данни може да доведе до **висок** риск за правата и свободите на засегнатите от него субекти на данни по смисъла на т. 10, институцията уведомява незабавно тези лица (Приложение № 3).

19. Уведомяването следва да бъде направено ясно, точно и разбираемо за субекта на данни и да включва:

    19.1. естеството на нарушението на сигурността на личните данни;

    19.2. име и данни за контакт на отговорното лице по т. 6;

    19.3. описание на евентуалните последици от нарушението на сигурността на личните данни;

    19.4. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително

по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

20. Отговорното лице по т. 6 предприема необходимите мерки, за да гарантира, че рисковете за правата и свободите на субектите на данни са своевременно предотвратени.

21. В случай, че са засегнати голям брой субекти на данни и тяхното уведомяване един по един (индивидуално) би отнело твърде много време (т.е. би довело до неоправдано забавяне), институцията може да публикува съобщение на своята уеб-страница или по друг начин, който осигурява еквивалентно ниво на публичност, с което уведомява всички лица едновременно.

22. Изключения от необходимостта за уведомяване на субектите на данни се допускат при поне едно от следните обстоятелства:

    22.1. институцията е предприела 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 мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;

    22.2. институцията е взела впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

    22.3. уведомяването води до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

23. В случай, че субектите на данни не са били уведомени от институцията, но надзорният орган прецени, че е налице висок риск от пробива в сигурността на данните, институцията следва да извърши действията по този раздел, веднага след като получи въпросната информация от страна на надзорния орган.

Раздел VII. Уведомяване на администратор на данни

24. В случай, че институцията е обработващ данни, процедурата за уведомяване на администратора се извършва съгласно постигнатите договорености с него.

VIII. Уведомяване на ръководството на институцията

25. Лицето по т. 6 докладва на директора/ръководителя на институцията до 24 часа от регистриране на пробива в сигурността.

Раздел IX. Образци на документи
Документиране на пробиви в сигурността на данните

26. Уведомяванията по т. 12 и т. 18 се извършват посредством използването на утвърдени образци – приложения към тази инструкция, доколкото Надзорният орган не е определил други такива.

27. Пробивите в сигурността на данните се отразяват в Регистър от лицето по т. 6, утвърден от институцията, включително приложенията към него. Регистърът съдържа и информация за предприетите мерки за справяне с нарушението от страна на институцията (Приложение № 4).

Раздел X. Свеждане до знание на служители и обработващи данни

28. Настоящата инструкция се свежда до знанието на всички служители на институцията.

29. В случай на обработващи данни от името на институцията, дейностите свързани с пробиви в сигурността се уреждат в договор с тях.

Приложения

№	Наименование на приложенията
1	Приложение № 1 към раздел IV, т. 11 Методология за оценка на тежестта на пробив в сигурността на личните данни
2	Приложение № 2 към раздел V, т. 13 Уведомяване на надзорния орган за нарушение на сигурността на личните данни
3	Приложение № 3 към раздел VI, т. 19 Съобщение до субекта на данните за нарушение на сигурността на личните данни
4	Приложение № 4 към раздел X, т. 28 Регистър на нарушения на сигурността на личните данни

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

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

		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**

		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**.

Приложение № 2:

към раздел V, т. 13 Уведомяване на надзорния орган за нарушение на сигурността на личните данни

УВЕДОМЛЕНИЕ ДО НАДЗОРНИЯ ОРГАН ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Детска градина „Радост”

ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02

info-701351@edu.mon.bg; сайт: www.dg-radost.org

ДО

Председателя на

Комисията за защита на личните данни,

бул., „Проф. Цветан Лазаров“ № 2

София, 1592

Уважаеми господин/госпожо Председател на КЗЛД,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, в изпълнение на чл. 33 от Общия регламент за защита на данните (ОРЗД - Регламент (ЕС) 2016/679), Ви уведомяваме, че е констатирано следното нарушение/я:

Данни за нарушението

Описание на естеството на нарушението	..... *(свободен текст)*
Категории засегнати субекти на данни и техният приблизителен брой	..... *(съобразно описаното в Регистъра на дейностите по обработка на личите данни и наличната техническа информация)*
Категории засегнати лични данни и приблизително количество на засегнатите записи	..... *(съобразно описаното в Регистъра на дейностите по обработка на личните данни и наличната техническа информация)*
Дата и час на установяване на нарушението	..... *(свободен текст)*

Приложение № 2 Уведомяване на надзорния орган

Причини за забавяне на настоящото уведомление (когато не е подадено в срок от 72 часа)	..... *(свободен текст – ако е приложимо)*

Описание на евентуалните последици от нарушението, според категориите лични данни

№	Категория лични данни	Описание
1	.....	.....
2	.....	.....

Технически и организационни мерки за справяне с нарушението и последиците от него

№ на последица	Описание на мерките
	.....
	.....

Данни за администратора

Наименование на администратора	..... *(наименование на институцията)*
Координати за връзка	..... *(имейл адрес, телефон)*
Съвместни администратори	..... *(наименование, координати за връзка – ако е приложимо)*
Длъжностно лице по защита на личните данни / Отговорно лице в съответствие с вътрешните процедури на институцията	..... *(име, фамилия, координати за връзка)*

С уважение,

Директор: .....
(подпис, печат)
.....
(име, фамилия)

Приложение № 3:

към раздел VI, т. 19 Съобщение до субекта на данните за нарушение на сигурността на личните данни

СЪОБЩЕНИЕ ДО ЗАСЕГНАТИ ЛИЦА

Детска градина „Радост”

ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02

info-701351@edu.mon.bg; сайт: www.dg-radost.org

ДО

.....

Субекта на данните (имена)

Уважаеми господин/госпожо,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, в изпълнение на чл. 34 от Общия регламент за защита на данните (ОРЗД - Регламент (ЕС) 2016/679), Ви уведомяваме, че е констатирано следното нарушение/я:

Данни за нарушението

Описание на естеството на нарушението	..... *(свободен текст)*

Описание на евентуалните последици от нарушението, според категориите лични данни

№	Категория лични данни	Описание	Възможни последици
	.....	.....	.....
	.....	.....	.....

Технически и организационни мерки за справяне с нарушението и последиците от него

№ на последица	Описание на мерките
	.....

Приложение № 3 Съобщение до засегнати лица

	.....

Данни за администратора

Наименование на администратора	*Детска градина „Радост"*
Координати за връзка	ПК 5400, гр.Севлиево, ул."Здравец" №1; тел. 0675/ 3-28-46; 8-90-02 info-701351@edu.mon.bg; сайт: www.dg-radost.org
Длъжностно лице по защита на личните данни / Отговорно лице в съответствие с вътрешните процедури на институцията	ЗАС /Виолета Монева/ - контакти: 0879066787; e-mail: zdg.radost_zas@abv.bg

С уважение,

Директор: .....
(подпис, печат)

.....
(име, фамилия)

Приложение № 4 Регистър на нарушения на сигурността на личните данни

Детска градина „Радост”
ПК 5400, гр.Севлиево, ул.”Здравец” №1; тел. 0675/ 3-28-46; 8-90-02
info-701351@edu.mon.bg; сайт: www.dg-radost.org

Приложение № 4

Към раздел IX, т. 28 Регистър на нарушения на сигурността на личните данни

РЕГИСТЪР НА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Данни за администратора

Администратор	**Детска градина „Радост”, град Севлиево**
Адрес	**ПК 5400, гр.Севлиево, ул.”Здравец” №1**
E-mail	**info-701351@edu.mon.bg**
Телефон	**0675/ 3-28-46; 8-90-02**

РЕГИСТЪР НА НАРУШЕНИЯТА

№	Описание на нарушението	Дата и час на установяване на нарушението	Засегнати субекти категория и брой	Категория засегнати лични данни и количество	Възможни последици от нарушението	Оценка на тежестта на пробива	Риск за правата и свободите на физ. лица	Предприети действия	Дата на изпълнение	Отговорни лица (ДЗЛД)	Дата на входиране в КЗЛД (ако е приложимо)	Причини на за забавяне (повече от 72 часа)

Приложение № 4 Регистър на нарушения на сигурността на личните данни

1												
2												
3												
4												
5												
6												
7												
8												

1. **За всяко установено нарушение към регистъра се добавя и оценката на риска и всякаква друга съпътстваща документация, включително кореспонденция с КЛЗД и изпратени уведомления до субектите на данни.**

Приложение № 4 Регистър на нарушения на сигурността на личните данни

2. **Във връзка с категориите, посочени в регистъра на нарушенията е препоръчително да се поддържа и следната допълнителна информация или тя да бъде включена в съответните колони на регистъра** *(посоченото в тази точка следва да се разглежда като разяснение и може да не присъства в окончателния документ на институцията)*:

2.1. Относно **„описание на нарушението“**: Посочване на лицата, които работят със съответната информация (лични данни), която е станала обект на нарушение (вкл. когато данните се обработват от друга институция – обработващ данни); Посочване на извършител на нарушението (ако е възможно); Дата и час на извършване на нарушението;

2.2. Относно **„дата и час на установяване на нарушението“**: посочване кога е установено нарушението, от кого и при какви обстоятелства.

2.3. Относно **„оценка на тежестта на пробива“**: Посочване на дейностите и резултатите, получени вследствие прилагане на методологията за оценка на тежестта на пробива.

2.4. Относно **„риска за правата и свободите на физическите лица“**: Посочване на това дали и какъв риск е установен вследствие на приложената методология за оценка на тежестта на пробива.

2.5. Относно **„предприети действия“**: Посочване на това, какви технически и организационни мерки са предприети за справяне с нарушението и последиците от него.

2.6. Относно **„дата на изпълнение“**: следва да се посочи, кога са изпълнени предприетите действия за справяне с нарушението.

2.7. Относно **„отговорни лица“**: Следва да се посочат лицата, отговорни за справяне с последиците от нарушението.

Директор: .....
(подпис, печат)
.....
(име, фамилия)