ИНСТРУКЦИЯ ЗА ДЕЙСТВИЕ ПРИ ПРОБИВ В СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Данни за администратора

Администратор	ПГПЧЕ „ ЕКЗАРХ ЙОСИФ“
Адрес	гр. Разград, ул. Н.Й.ВАПЦАРОВ‘ №10
E-mail	info-1702608@edu.mon.bg
Телефон	0878684525

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. Лицето - Живко Димитров Павлов по т. 5 следва да докладват за установени пробиви в сигурността.

7. 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.

8. Отговорното лице по т. 6 следва да обобщи цялата информация, свързана с пробива в сигурността, както следва:

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

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

9. Уведомяванията се извършват по следния начин телефон (е-поща в резервен случай). По същия начин съответната насрещна страна потвърждава, че е била уведомена.

Раздел IV. Оценка на необходимостта от уведомяване

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

11. Във връзка с посоченото в т. 10 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).

12. За целите на т. 11 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

13. В случай, че бъде установено, че **съществува риск**, по смисъла на т. 11, институцията докладва за пробива в сигурността на данните на надзорния орган (КЗЛД) в рамките на **72 часа** от установяване на пробива (Приложение № 2).

14. 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.

15. 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.

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

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

17.1. описание на пробива в сигурността;

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

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

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

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

17.6. 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.

18. 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

19. 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. 11, институцията уведомява незабавно тези лица (Приложение № 3).

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

20.1. естеството на нарушението на сигурността на личните данни;

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

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

20.4. 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.

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

22. 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.

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

23.1. 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;

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

23.3. 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.

24. 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

25. 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

26. 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

27. Уведомяванията по т. 13 и т. 19 се извършват посредством използването на утвърдени образци – приложения към тази инструкция, доколкото Надзорният орган не е определил други такива.

28. 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

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

30. 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