УВЕДОМЯВАНЕ ЗА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Гл. ас. д-р Живка Матеева
Икономически университет – Варна

NOTIFICATION OF BREACH OF PERSONAL DATA SECURITY

Chief Assist. Prof. Zhivka Mateeva, PhD
University of Economics - Varna

Резюме: Уведомяването за нарушения на сигурността на данните е нов момент, който е част от въведения ефективен механизъм за защита на личните данни, предвиден изрично в Регламент 2016/679 ЕО. Нарушенията на сигурността на данните могат да доведат до най-различни отрицателни последици за субектите на личните данни, както и да въздействат неблагоприятно върху правото на неприкосновеност на личността и личния живот. Несъмнено бързото и адекватно вземане на мерки за гарантиране на сигурността на обработването на личните данни, както и ограничаване нарушенията на сигурността на данните е въпрос с голямо практическо приложение. В настоящото изложение се изследва процедурата по уведомяването за нарушения на сигурността на данните. Акцент в разработката е поставен върху актуалните и модернизирани процедури за уведомяване при нарушения на сигурността на личните данни, явяващи се гаранция за по-голям контрол и сигурност на данните, в съвременния дигитален свят. Въз основа на анализа се конкретизират основните моменти, свързани с тяхното практическо приложение.

Ключови думи: *лични данни, защита, надзорен орган, субект на лични данни, уведомяване*

Abstract: The notification of data security breaches is a new moment, which is part of the introduced effective mechanism for personal data protection, explicitly provided for in Regulation 2016/679 EC. Violations of data security can lead to a variety of negative consequences for data subjects, as well as adversely affect the right to privacy and private life. Undoubtedly, the rapid and adequate taking of measures to ensure the security of the processing of personal data, as well as the reduction of data security breaches, is a matter of great practical application. This statement examines the procedure for notifying data breaches. Emphasis in the development is placed on the current and modernized procedures for notification of breaches of personal data security, which are a guarantee for

greater control and security of data in the modern digital world. Based on the analysis, the main points related to their practical application are specified.

Key words: *personal data, protection, supervisor, personal data subject, notification*

Doi: https://doi.org/10.36997/LBCS2021.259

Въведение

Изискването за уведомяване на компетентния национален надзорен орган и съобщаването в определени случаи на физическите лица, когато е налице нарушение на сигурността на личните данни, е изрично въведено с приемането на Регламент 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните – ОРЗД)[1]. Съгласно чл. 4, т.12 от ОРЗД, нарушение на сигурността на личните данни означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни. Нарушението може евентуално да предизвика редица значителни неблагоприятни последици за физическите лица, които могат да породят физически, материални или нематериални вреди (Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, WP250, 3 октомври 2017, с. 10). Възможните последици са загуба на контрол върху личните данни или ограничаване на правата на физическите лица, 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 (вж. съображения 75 и 85 от ОРЗД). Нарушаването на правото на личността във връзка с разкриването на личните ѝ данни е посегателство върху неприкосновеността на личността и личния живот. От което следва, че в ерата на информационното общество възможностите за възникване на нарушения на сигурността на данните, свързани

[1] ОВ, L119/1 от 4 май 2016 г., с. 1-88.

с опасността и заплахата от неблагоприятни последици за личността, е изключително голяма. Въпреки че новите технологии, като например криптиране, вече осигуряват повече възможности за гарантиране на сигурността на обработването, нарушенията на сигурността на данните продължават да са често явление (Наръчник по европейско право в областта на защитата на данните, 2018, с. 204). Естеството на данните и огромните рискове за нарушения на сигурността изискват и предприемането на съответни мерки, които да осигурят по-високо ниво на защита на личните данни. Несъмнено бързото и адекватно вземане на мерки за гарантиране на сигурността на данните и навременното овладяване на обстоятелствата, при възникване на нарушения от страна на администраторите, е въпрос с голямо практическо приложение.

1. Уведомяване на националния надзорен орган от администратора на лични данни

С цел да се ограничи въздействието на нарушенията на сигурността на данните и да се утвърдят правата на физическите лица разпоредбата на чл. 33 от ОРЗД налага на администраторите изискване за уведомяване при определени обстоятелства. Съгласно посочената разпоредба, когато администраторът на лични данни установи, че е настъпило нарушение на сигурността на данните, то той трябва да уведоми компетентния надзорен орган, освен ако не съществува вероятност нарушението да породи риск за правата и свободите на физическите лица. Уведомяването на надзорния орган е задължително за администратора по ОРЗД и неизпълнението му ще доведе до налагането на административни наказания[2] по силата на чл. 83 от ОРЗД или коригиращи мерки по чл. 58, пар. 2 от ОРЗД.

За да изпълни задължението си, администраторът на първо място трябва да е „разбрал“ за даденото нарушение на сигурността на данните и да може да го разпознае като такова. Работната група за защита на личните данни по член 29 от ОРЗД приема, че администраторът е узнал за настъпването на нарушението на сигурността,

[2] Повече за административните наказания вж. Цанков, П. и др. (2006). Основи на публичното право. Варна: Наука и икономика, с. 124-130; Андреева, А., Йолова, Г., Димитрова, Д. (2021). Основи на публичното право. Варна: Наука и икономика, с. 197-207.

когато той е установил с разумна степен на увереност, че е настъпил инцидент, свързан със сигурността, който е повлиял на личните данни (Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, WP250, 3 октомври 2017, с. 12). В зависимост от обстоятелствата на конкретното нарушение администраторът следва да направи преценка относно това дали има, или не нарушение на сигурността. Но невинаги още от самото начало ще бъде сравнително ясно за администратора, че е настъпило нарушение. В други случаи възможно е да отнеме известно време, за да се установи дали личните данни са били компрометирани по някакъв начин. Например нарушение на сигурността на данните ще е налице в случаите на загубено или откраднато устройство, съдържащо копие от база данни за студенти или служители от даден университет. Няма да е нарушение, ако обаче данните им временно не са налични при извършване на планова поддръжка на системата от база данни, предназначена да подпомага и дигитализира работната дейност на администрацията. Ключова е преценката на администратора за всеки конкретен случай.

Независимо от това администраторът трябва да предприеме незабавни действия за разследване на всеки инцидент с оглед на това дали сигурността на данните е била наистина нарушена, да събере необходимите доказателства и да предприеме действия за справяне със ситуацията. За да може да се определи незабавно дали е налице нарушение, то ОРЗД задължава администратора да оцени рисковете с различна вероятност и тежест и да приложи всички подходящи технически и организационни мерки за осигуряване на високо ниво на сигурност на данните. Това изискване е в съответствие с принципа за цялостност и поверителност, установен в нормата на чл. 5, пар. 1, б. „е“ от ОРЗД. Той въвежда задължението на администратора да обработва личните данни по начин, който да гарантира подходящо ниво на сигурност. Този принцип е нов, макар че изисквания за осигуряване на защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане чрез прилагане на подходящи технически или организационни мерки бяха предвидени и в действащата досега уредба (Александров 2018: 49-50). Важно е да се отбележи, че този принцип се отнася до сигурността във всеки аспект на обработката на лични данни и се стреми да не допусне настъпването на неблагоприятни последици от неразрешено

или незаконосъобразно обработване, случайна загуба, унищожаване или повреждане на данните.

Нарушенията по сигурността на информацията може да доведат до реални вреди на физическите лица. Вредите, причинени от злоупотребата с лични данни, в повечето случаи са свързани с кражба на самоличност, фалшиви транзакции с кредитни карти, ипотечни измами и др. Поради това нарастват необходимостта и интересът на администраторите на данни да предприемат ефективни мерки за осигуряване на реална защита на данните. ОРЗД не съдържа изчерпателен списък на подходящи мерки за защита, а само насоки за възможни такива. От което следва, че преценката за това кои мерки се явяват подходящи, за да бъдат прилагани, е предоставена изцяло на администратора.

При определянето на конкретните мерки, които да са подходящи за съответния случай, администраторът следва да извърши оценка на рисковете, свързани с обработването. В тази връзка е необходимо да се вземат предвид достиженията на техническия прогрес, разходите за прилагане на мерките, естеството на данните, обхватът и целите на обработването, както и рисковете за правата и свободите на физическите лица. Въз основа на оценката на риска администраторът трябва да предприеме реални и ефективни вътрешни механизми за защита с оглед осигуряването на сигурността на данните. Например данните да се обработват само от упълномощени за това лица; сградите и помещенията, където се съхраняват данните, да са осигурени срещу взлом, пожар, природни бедствия; паролите за достъп до данните да са известни само на упълномощените лица и да се сменят редовно, също така да има възможност за възстановяването на лични данни в случай на загуба или унищожение. Изискването за цялостност и поверителност не е еднократно действие от страна на администратора, а задължение, което следва да бъде изпълнявано през целия жизнен цикъл на данните (Тошкова-Николова, Фети 2019: 101).

В допълнение към задължението за уведомяване ОРЗД изисква при нарушения на сигурността на данните администраторът да ги овладее по подходящ и навременен начин. Това ще е възможно само ако той има предварителна подготовка, т.е. администраторът трябва да има разписани правила и процедури за реакция при евентуални нарушения на сигурността на данните. Основната им цел е да се намали или ограничи въздействието от нарушението върху субектите

на лични данни, като се:

- дефинира къде и каква е същността на нарушението;
- определи системата от мерки и средства за откриване и своевременното реагиране на нарушенията;
- прецени и оцени рискът за физическите лица;
- определят стъпките, които се предприемат в такива случаи.

Уведомяването за настъпило нарушение на сигурността на личните данни до надзорния орган може да бъде първоначално и последващо. Съответно администраторът трябва да изпрати уведомлението до надзорния орган без ненужно забавяне, а когато това е осъществимо – не по-късно от 72 часа след като е разбрал за нарушението. Минималната информация, която трябва да бъде включена в уведомлението, е изрично посочена в чл. 33, пар. 3 от ОРЗД. Съгласно посочената разпоредба уведомлението трябва да съдържа:

- описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- 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.

Определеният от ОРЗД първоначален срок е сравнително кратък. Нещо повече, невинаги администраторите ще имат цялата необходима информация и пълни подробности за даденото нарушение през този първоначален период. Например при кибератака, която може да наложи по-задълбочено разследване за пълното изясняване на естеството на нарушението и степента, в която са били засегнати личните данни. Поради това разпоредбата на чл. 33, пар. 4 от ОРЗД допуска информацията за нарушения на сигурността да бъде детайлизирана и по-късно от администраторите, т.е. в случаите, когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненуж-

но забавяне.

Един от важните елементи в контролната дейност на Комисията за защита на личните данни (КЗЛД) в качеството ѝ на национален надзорен орган е свързан с уведомленията за нарушения на сигурността на личните данни по чл. 33 от ОРЗД. За 2020 г. в КЗЛД са получени общо 60 уведомления за нарушения на сигурността на данните. От регистрираните пробиви на сигурността на данните 23% засягат публични институции (държавни и образователни структури), а останалите са от частния сектор. Основните нарушения са свързани с външни злонамерени атаки към системите на администраторите, представляващи различни по вид киберпрестъпления, включително кражби на бази данни, съдържащи лични данни. Също така не малък процент са инцидентите, свързани с разкриването на данни пред трети лица вследствие на неволни технически грешки и възникнали технически проблеми в информационните системи, предизвикани от човешкия фактор. В сравнение с 2019 г. през отчетния период се наблюдава тенденция на нарастване на относителния дял на тези нарушения при запазване на съотношението между тях (Годишен отчет на КЗЛД за дейността ѝ през 2020 г., с. 51-55). Като положителна насока, с цел осведомеността на администраторите и физическите лица, следва да се отбележи фактът, че през 2021 г. КЗЛД разработи и утвърди формуляр на Уведомление за нарушаване на сигурността на данните на основание чл. 33 от ОРЗД, който е публикуван на институционалния сайт на комисията. С оглед избягване на последващи искания за допълнителна информация и унифициране на уведомленията се препоръчва неговото попълване.

Администраторът е задължен да документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него, съгласно чл. 33, пар. 5 от ОРЗД. Той може да бъде освободен от задължението за уведомяване при настъпили нарушения на сигурността на данните само ако докаже, че няма вероятност нарушението да доведе до риск за правата и свободите на засегнатите лица.

2. Съобщаване на субекта на данните за нарушения на сигурността на личните данни

Разпоредбата на чл. 34, пар. 1 от ОРЗД изисква администраторът да съобщи на субекта на данните при нарушения на сигурността на личните данни независимо от задължението му за уведомяване на надзорния орган, когато има вероятност нарушението да породи висок риск за правата и свободите на засегнатите физически лица. Съобщаването трябва да се извърши във възможно най-кратък срок – без ненужно забавяне. Своевременното информиране на субектите на данните зависи от спецификата на конкретното нарушение на сигурността на данните. Например при необходимост да се ограничи непосредственият риск от вреди е разумно незабавното уведомяване на субектите на данните, докато необходимостта от предприемането на целесъобразни мерки срещу продължаването на нарушения на сигурността на личните данни или срещу подобни нарушения би оправдало по-дълги срокове за уведомлението (съображение 86 от ОРЗД). Администраторът трябва да оцени риска от гледна точка на самите физически лица, а не от гледна точка на неговите действия. Целта на съобщаването е да се даде възможност на засегнатите физически лица от нарушението да предприемат необходимите предпазни мерки, за да се предпазят от евентуални неблагоприятни последици от нарушението.

Съобщението до субекта на данните трябва да бъде написано на ясен и прост език. В него следва да се опише естеството на нарушението на сигурността на личните данни и да се посочат най-малко информацията и мерките, посочени в чл. 33, пар. 3, б. „б“, „в“ и „г“ от ОРЗД. В съответствие с това администраторът следва да предостави най-малко следната информация:

- описание на естеството на нарушението;
- името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт;
- описание на евентуалните последици от нарушението и
- описание на предприетите или предложените от администратора мерки за справяне с нарушението, включително, когато е целесъобразно, мерки за намаляване на евентуалните неблагоприятни последици (Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, WP250,

3 октомври 2017, с. 23).

Работната група по чл. 29 препоръчва съобщението да се съобщи директно на засегнатите субекти на данни. Уточнява още, че с цел съобщението да бъде ясно и прозрачно, то не трябва да се изпраща съвместно с друга информация, като редовни актуализации, бюлетини или стандартни съобщения (Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679, WP250, 3 октомври 2017, с. 23). Невинаги обаче изпращането на индивидуализирани уведомления до субектите на данни ще бъде практически възможно и реализируемо. С цел субектите на данни да бъдат в еднаква степен ефективно информирани за настъпилото нарушение на сигурността на данните разпоредбата на чл. 34, пар. 3, б. „в“ от ОРЗД допуска извършването на публично съобщение или да бъде взета друга подобна мярка, когато изпращането на конкретното съобщение би довело до непропорционални усилия за администратора. Като цяло съобщенията до субектите на данни следва да бъдат изпратени веднага щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват насоките, предоставени от него или от други съответни органи, например правоприлагащите органи (съображение 86 от ОРЗД).

При определени обстоятелства администраторите могат да бъдат освободени от задължението за уведомяване на субектите на данни за нарушения на сигурността. Изключенията, въведени от чл. 34, пар. 3 от ОРЗД, се прилагат, когато:

- 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;

- администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

- уведомлението изисква несъразмерно големи усилия от страна на администратора, субектите на данни могат да бъдат информирани за нарушението чрез публично съобщение или друга подобна мярка.

В случай че администраторът реши да не съобщи на субекта на данните за настъпилото нарушение на сигурността, то надзорният

орган може да изисква от него да направи това, след като отчете че има вероятност нарушението да породи висок риск за физическите лица. Също така няма да се изисква уведомяване на физическите лица, ако надзорният орган реши, че са изпълнени условията в чл. 34, пар. 3 от ОРЗД.

Заключение

Уведомяването за нарушения на сигурността на личните данни е важен момент с голямо практическо приложение за защитата на личните данни. От една страна, чрез своевременното информиране на субектите на данни за нарушения на сигурността на данните се дава възможност на засегнатите от нарушението физически лица да предприемат мерки, които да ги предпазят от възможните последици от него. От друга страна, уведомяването на надзорния орган при настъпили нарушения на сигурността на данните е важен инструмент за засилване на спазването на заложените в ОРЗД изисквания за защита на личните данни. Целта на уведомлението на надзорния орган не се свежда единствено до получаване на насоки относно това дали засегнатите физически лица следва да бъдат информирани при нарушения на сигурността на данните, а преди всичко е защита на физическите лица и техните лични данни. Не на последно място уведомяването е важен фактор по отношение на последващите действия на надзорния орган с оглед изпълнението на правомощията му, предоставени от ОРЗД, по прилагането на ефективен механизъм за надзор в областта на защитата на личните данни.

Използвана литература

1. Александров, А. (2018). От 25 май 2018 година започва да се прилага Общият регламент за защита на личните данни. // Труд и право, №4(18), с. 44-51.

2. Андреева, А.; Йолова, Г.; Димитрова, Д. (2021). Основи на публичното право. Варна: Наука и икономика.

3. Годишен отчет на КЗЛД за дейността ѝ през 2020 г. (https://www.cpdp.bg/).

4. Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679 на Работната

група по чл. 29, приети на 3 октомври 2017 г., последно преработени и приети на 6 февруари 2018 г. (WP250, rev.01).

5. Наръчник по европейско право в областта на защитата на данните. (2018). Агенция на Европейския съюз за основните права и Съвет на Европа (https://fra.europa.eu/bg/publication/2020/narchnik-po-evropeysko-pravo-v-oblastta-na-zashchitata-na-dannite-izdanie-2018-g).

6. Тошкова-Николова, Д., Фети, Н. (2019). Защита на личните данни. София: Труд и право.

7. Цанков, П. и др. (2006). Основи на публичното право. Варна: Наука и икономика.

За контакти: гл. ас. д-р Живка Матеева
Икономически университет – Варна
jivkamateeva@ue-varna.bg