НАРУШЕНИЯ НА СИГУРНОСТТА НА ДАННИТЕ И ДИГИТАЛИЗАЦИЯТА

Христо Аламинов
началник отдел „Международно сътрудничество и
управление на проекти“
Комисия за защита на личните данни

DATA BREACHES AND DIGITALISATION

Hristo Alaminov
Head of International Cooperation
and Project Management Department
Commission for Personal Data Protection

Резюме: Докладът представя общ преглед на значението и ползите от изследване на нарушенията на сигурността на личните данни в контекста на глобална тенденция, каквато е дигитализацията. Независимо от крайно отрицателните последици, които нарушенията на сигурността имат както за физическите лица, чиито данни са засегнати, така и за администраторите/ обработващите лични данни, те са ценен източник на информация.

Ключови думи: *Нарушение на сигурността на данните, защита на личните данни, дигитализация.*

Abstract: The report provides an overview of the importance and benefits of examining personal data breaches in the context of a global trend such as digitalisation. Regardless of the extremely negative consequences that security breaches have, both for the individuals whose data are affected and for the data controllers / processors, data breaches are valuable sources of information.

Key words: *Data breaches, protection of personal data, digitalisation*

DOI: <https://doi.org/10.36997/PPDD2021.29>

Изложение

Легална дефиниция за понятието „нарушение на сигурността на личните данни“ е предоставена в член 4 на Регламент (ЕС) 2016/679, а именно, това е „всяко 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“. Нарушение на сигурността на данни възниква, когато данните, за които дружество/организация (администратор или обработващ лични данни) отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта.

Съгласно Приложение № 1 към Инструкция за практическото осъществяване на надзорната дейност на Комисия за защита на личните данни. Методика за определяне нивото на риска при нарушения на сигурността на личните данни на Комисията за защита на личните данни, „нарушение на сигурността на данните е всяка една комбинация или самостоятелно проявление на някой от следните три типа нарушения – *нарушение на поверителността, нарушение на целостта и/или нарушение на наличността*“.

Нарушението на поверителността представлява неправомерно преднамерено или случайно разкриване или достъп до лични данни. Това включва разкриване на лични данни пред (или достъп до тях на) получатели, които не са оправомощени да ги получат (или да имат достъп до тях), или всеки друг вид обработване, което се явява нарушение на ОРЗД.

Нарушение на целостта е преднамерено или случайно повреждане на лични данни. *Повреждане* е налице, когато личните данни са променени, подправени или са станали вече непълни.

Нарушение на наличността е преднамерена или случайна загуба на данни, унищожаване на данни или неналичена услуга. *Загуба* на лични данни е състояние, при което данните може да са все още налични, но администраторът на лични данни е загубил контрол или достъп до тях или вече не ги притежава. *Унищожаване* на лични данни е налице, когато данните са във вид, в който не може да бъдат използвани или вече не са налични.

Важно е да се отбележи, че нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен на-

чин, да доведе до физически, материални или нематериални вреди за физическите лица. Сред тези вреди са загубата на контрол върху личните им данни или ограничаването на правата им, дискриминацията, кражбата на самоличност или измамата с фалшива самоличност, финансовите загуби, неразрешеното премахване на псевдонимизация, накърняването на репутацията, нарушаването на поверителността на лични данни, защитени от професионална тайна, както и всякакви други значителни икономически или социални неблагоприятни последици за засегнатите физически лица.

Във връзка със започване прилагането на ОРЗД, Европейската комисия публикува на институционалната си интернет страница два примера за нарушение на сигурността на данните:

1. Данните на служителите на текстилно дружество са разкрити. Данните включват личните адреси, членове на семейството, месечната заплата и медицински бележки на всеки служител. В този случай текстилното дружество трябва да информира надзорния орган за нарушението. Тъй като личните данни включват чувствителни данни като например данни за здравословното състояние, дружеството трябва да уведоми и служителите.

2. Болничен служител решава да копира данните на пациентите на компактдиск и да ги публикува онлайн. Болницата разбира за това няколко дни по-късно. Веднага след като болницата разбере, тя има 72 часа, за да информира надзорния орган, и тъй като личните данни съдържат чувствителна информация като например дали даден пациент е болен от рак, дадена пациентка е бременна и т.н., тя трябва да информира и пациентите. В този случай би било под въпрос дали болницата е въвела подходящи технически и организационни мерки за защита. Ако тя действително е въвела подходящи мерки за защита (например криптиране на данните), би било малко вероятно рискът да се осъществи и тя би могла да бъде освободена от изискването за уведомяване на пациентите.

Сред общите елементи на двата примера, освен нарушението на сигурността на данните, е и задължението на администраторът/ обработващият лични данни да информира националния надзорен орган по защита на данните за нарушението. Макар да не е нова концепция в защитата на лични данни, уведомлението за нарушение на сигурността на данните намира значително място в общата парадигма на Регламент (ЕС) 2016/679. По-наблюдателните вероятно са открили същест-

уването му в Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации, където към онзи момент се съдържат правилата относно съобщаването на нарушения на сигурността на личните данни от доставчиците на общественодостъпни електронни съобщителни услуги, в случай че личните данни на клиентите са изгубени, откраднати или компрометирани по друг начин.

Наличието на подобна правна разпоредба във връзка с електронните комуникации демонстрира, че европейският законодател е преценил, още в края на първото десетилетие на XXI в., технологиите и, в частност, електронните съобщения и свързаната с тях дигитализация като област, в която биха възникнали нарушения на сигурността на данните. Ето защо задължение на организациите, обработващи лични данни, е, веднага след като се установи нарушение на сигурността на личните данни, да уведомят надзорния орган за нарушението на сигурността на личните данни. Действието следва да се осъществи без ненужно забавяне и когато това е възможно – не по-късно от 72 часа, след като той е разбрал за него.

Както всяко правило, и настоящото задължение има изключение, ако администраторът е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Във всички случаи процесът следва да бъде документиран с оглед последващо доказване на адекватността на мерките. От съществено значение е да се сподели, че когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне.

Сред основните причини, които предопределят важноста на уведомлението, е, че чрез него може да установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки (задължение на администратора/ обработващия лични данни съгласно чл. 24 от Общия регламент относно защитата на данните). Съдържанието на уведомлението е определено в чл. 33, пар. 3 от Регламент (ЕС) 2016/679. Всяко уведомление следва да съдържа най-малко:

а) описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) 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;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително и мерки за намаляване на евентуалните неблагоприятни последици.

При установяване на подробни правила за формата и процедурите, приложими за уведомяването за нарушения на сигурността на личните данни, следва да се отдаде необходимото внимание на обстоятелствата, свързани с нарушението, включително дали личните данни са били защитени чрез подходящи технически мерки за защита, ефективно ограничаващи вероятността за измама с фалшива самоличност или други форми на злоупотреба. Заслужава внимание и хипотезата, в която при такива правила и процедури следва да се отчитат законните интереси на правоприлагащите органи, когато ранното разкриване може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността на личните данни.

Предвид широкото определение на понятието „лични данни“ съвсем логично и процесът по преобразуване (конвертиране) на аналогови данни под всякаква форма – текст, снимки, глас, в цифрова информация, с възможност да бъде репродуцирана неограничено във времето без промяна на качеството ѝ чрез общодостъпни комуникационни канали, може да попадне в обхвата на Общия регламент относно защитата на данните. След нейното цифровизиране същата може да бъде събрана, записана, организирана, структурирана, съхранявана, адаптирана, променяна чрез извличане, консултиране, употребяване, разкриване чрез предаване, разпространяване или друг начин, по който информацията става достъпна, подредена или комбинирана, ограничавана, изтривана или унищожавана – операции по обработване, които съвпадат с дефиницията на „обработване“ съгласно Регламент (ЕС) 2016/679.

При прилагане на второто значение на термина „дигитализи-рам“ – интегрирането на дигиталните технологии в ежедневието на хората също попада в обсега на регламента и дори в по-голяма степен представлява интерес от гледна точка защитата на личните данни. Тук следва да се представи възможността за профилиране на субектите на данните. По определение „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно – за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

Независимо кой от 6-те елемента на дигитализацията (съдържа-телен модел, концепция за дигитална конверсия, технологични решения, бюджетиране и финансиране, човешки ресурси и партньорства) се изследва, със сигурност може да се открият условия за нарушения на сигурността на данните. Тези предпоставки трябва да се анализират и да се въведат подходящи технически и организационни мерки.

Както вече беше посочено, уведомлението за нарушение на сигурността на данните съдържа необходимите данни, които да позволят на националния надзорен орган по защита на данните да изпълнява задачите и и да упражнява правомощия, вменени с ОРЗД. Те обхващат обработването в контекста на дейностите на мястото на установяване на администратора или обработващия лични данни на територията на неговата държава членка, обработването на лични данни, извършвано от публични органи или частни структури, действащи в обществен интерес, обработване, което засяга субекти на данни на неговата територия, или обработване, извършвано от администратор или обработващ лични данни, който не е установен в Европейския съюз, когато субектите на данни, към които това обработване е насочено, са с местопребиваване на територията на Съюза.

Въпреки настоящите предизвикателства, светът се глобализира. По силата на европейското законодателство държавите членки прилагат общи правила за защита на личните данни. Като част от единния пазар на Европейския съюз икономическите субекти често развиват своята дейност в държава – членка на ЕС, която е различна от държавата по регистрация.

За да се гарантира последователното прилагане на територията на Европейския съюз за Регламент (ЕС) 2016/679, се създаде механизъм за съгласуваност за осъществяване на сътрудничество между надзорните органи. Този механизъм се прилага, когато даден надзорен орган възнамерява да приеме мярка, целяща да породи правни последици по отношение на операции по обработване на данни, които засягат съществено значителен брой субекти на данни в няколко държави членки. Това се прилага също, когато засегнатият надзорен орган или Европейската комисия поиска този въпрос да бъде разгледан чрез механизма за съгласуваност.

Прилагането на подобен механизъм е условие за законосъобразността на мярка, целяща да породи правни последици, издадена от надзорния орган в случаите, когато прилагането му е задължително. В други случаи с трансгранично значение следва да се прилага механизмът за сътрудничество между водещия надзорен орган и засегнатите надзорни органи и могат да се осъществяват взаимопомощ и съвместни операции между засегнатите надзорни органи на двустранна или многостранна основа, без да се задейства механизмът за съгласуваност.

При прилагането на механизма за съгласуваност Европейският комитет по защита на данните (ЕКЗД, Комитета) излиза със становище в срок, при условие че бъде взето решение с мнозинство от неговите членове след искане от засегнат надзорен орган или от Европейската комисия. В допълнение, Комитетът приема решения със задължителен характер в случай на спорове между надзорни органи. При противоречиви становища от страна на националните надзорни органи ЕКЗД приема решение със задължителен характер. Това важи особено за условията на механизма за сътрудничество, между водещия надзорен орган и засегнатите надзорни органи по съществуването на спора относно възможното нарушение на Регламент (ЕС) 2016/679.

С времето тези данни започват да се обобщават, а Комитетът, подпомаган от експерти от националните надзорни органи, издава насоки, препоръки и най-добри практики по отношение на обстоятелствата, при които нарушението на сигурността на личните данни има вероятност да доведе до висок риск за правата и свободите на физическите лица. Този процес демонстрира значението, което нарушенията на сигурността на данните имат, като спомага за предотвратяване на бъдещи нарушения на разпоредбите на Общия регламент,

благодарение на използването на нарушенията на сигурността на данните като източник на информация. Практически пример в тази посока са Насоки 01/2021 на ЕКЗД относно примери, свързани с уведомлението за нарушение на сигурността на данните.

Използвана литература

Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации).

Закон за защита на личните данни на Република България. // ДВ, №1, 2002; посл. изм. ДВ, №7, 2018.

Приложение № 1 към Инструкция за практическото осъществяване на надзорната дейност на Комисия за защита на личните данни. Методика за определяне нивото на риска при нарушения на сигурността на личните данни.

Проект № 2007СВ16ІРО007-2011-2-06 Дигитална култура за регионално сближаване, съфинансиран от ЕС чрез Програма за ТГС по ИПП № 2007СВ16ІРО007.

Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации.

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Guidelines 01/2021 of the European Data Protection Board on Examples regarding Data Breach Notification.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_bg

За контакти: Христо Аламинев
Комисия за защита на личните данни
e-mail: halaminov@cpdp.bg