УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ
И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

БИТ

СЪВРЕМЕННИ ИЗМЕРЕНИЯ

НА ЕВРОПЕЙСКОТО ОБРАЗОВАТЕЛНО
И НАУЧНО ПРОСТРАНСТВО

Сборник с доклади

13

Том 13

ЗА БУКВИТЕ
О ПИСМЕНЕХЪ

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ЕВРОПЕЙСКОТО ОБРАЗОВАТЕЛНО И НАУЧНО ПРОСТРАНСТВО

Том 13
2025

MODERN DIMENSIONS IN THE EUROPEAN EDUCATIONAL AND RESEARCH AREA

Volume 13
2025

За буквите
О. Писменех

Сборникът и научната конференция са реализирани в рамките на проект „Ежегоден пътуващ научен семинар с международно участие „Съвременни измерения на европейското научнообразователно пространство“ по Договор № ПЧФНП-2025-06 от 21.03.2025 г. с научен ръководител гл. ас. д-р Ива Стоилова Костадинова по вътрешен конкурс за разработка на проекти за издаване на научни трудове по Наредбата за условията и реда за оценката, планирането, разпределението и разходването на средствата от държавния бюджет за финансиране на присъщата на държавните висши училища научна или художественотворческа дейност на Министерството на образованието и науката на Република България.

Всички доклади са изцяло авторски, изразените мнения са на авторите.

ISSN 2367-7988

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА ЕВРОПЕЙСКОТО ОБРАЗОВАТЕЛНО И НАУЧНО ПРОСТРАНСТВО

БЪЛГАРО-ТУРСКИ КУЛТУРНИ ОБЩУВАНИЯ

СБОРНИК С ДОКЛАДИ
ОТ ДЕВЕТНАДЕСЕТИ МЕЖДУНАРОДЕН ПЪТУВАЩ СЕМИНАР
НА УниБИТ,
ПРОВЕДЕН В ГР. АЙВАЛЪК, ТУРЦИЯ

25 – 31 май 2025 г.

Академично издателство „За буквите – О писменехъ“
София • 2025 • Sofia

ПРАВНА И ИНСТИТУЦИОНАЛНА РАМКА ЗА ДОКЛАДВАНЕ НА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ: АНАЛИЗ НА ЕВРОПЕЙСКИТЕ ИЗИСКВАНИЯ И НАЦИОНАЛНИТЕ МЕХАНИЗМИ ЗА ПРИЛАГАНЕ

Мартин Захариев, Панайот Гиндев, Даниела Павлова
Университет по библиотекознание и информационни технологии

Резюме: *Настоящото изследване има за цел да анализира нормативната уредба, приложима при нарушения на сигурността на личните данни съгласно чл. 33 и чл. 34 от Общия регламент относно защитата на данните (GDPR), както и тълкуванията и насоките на национални и европейски органи. Във фокуса на анализа попадат както правните изисквания към администраторите на лични данни за уведомяване на надзорния орган и субектите на данни, така и приложимите насоки от Европейския комитет по защита на данните (ЕКЗД), както и Методиката на Комисията за защита на личните данни в България за оценка на риска. Използван е документален метод и нормативно-сравнителен анализ. Направен е опит за критично осмисляне на нормативната уредба и съществуващите практики, като се акцентира върху основните характеристики на правната рамка и начините, по които тя се прилага от надзорните органи. Резултатите очертават необходимостта от повишаване на готовността на организациите в Р България да реагират ефективно при инциденти, като акцентът е поставен върху ясното разбиране на рисковете и задълженията, произтичащи от нарушението на сигурността на личните данни.*

Ключови думи: *лични данни; нарушение на сигурността; докладване; GDPR; надзорни органи*

ВЪВЕДЕНИЕ

В условията на глобална дигитална трансформация личните данни се превръщат в ключов ресурс в съвременното информационно общество. Масовото събиране, съхранението и обработването на данни създават възможности за иновации, повишаване на ефективността и развитие на нови бизнес модели, но едновременно с това се увеличават рисковете за информационна сигурност и защита на данните. Основните заплахи включват несанкциониран достъп, загуба, изменение или разкриване на лични данни, което може да доведе до сериозни последици като кражба на самоличност, измами, дискриминация или нарушаване на личната неприкосновеност. Тези рискове се задълбочават при използването на нови технологии за електронна идентификация, включително биометрични данни и дистанционна верификация, които, макар и да оптимизират процесите и да намаляват грешките, създават потенциал за злоупотреби и киберпрестъпления.

В отговор на тези предизвикателства Европейският съюз въвежда строги нормативни изисквания за защита на личните данни, като основополагащ акт е Регламент (ЕС) 2016/679 – Общият регламент относно защитата на данните (GDPR). Този регламент въвежда задължителни принципи като законосъобразност, добросъвестност и прозрачност, минимизация на данните, прозрачност, цялостност и поверителност, както и права за физическите лица като право на достъп, корекция, изтриване, ограничаване на обработката и преносимост на данните.

Общият регламент въвежда и специфични задължения за администраторите и обработващите лични данни при инциденти, засягащи сигурността. Централно място в тази регулация заемат разпоредбите на чл. 33 и чл. 34, които уреждат задълженията за уведомяване на надзорния орган и на субектите на данни при нарушение на сигурността.

Настоящата публикация има за цел да анализира правната уредба относно докладването на нарушения на сигурността на личните данни съгласно чл. 33 и 34 от GDPR, като се отделя специално внимание на тяхното практическо приложение. Разглеждат се също тълкува-

телните насоки на Европейския комитет по защита на данните (ЕКЗД), както и Методиката на Комисията за защита на личните данни (КЗЛД) в Република България относно оценката на риска и изпълнението на задълженията за уведомяване. Изследването цели да изясни основните затруднения, пред които се изправят организациите в реални ситуации, както и да очертае институционалните очаквания при прилагане на разпоредбите.

Публикацията е осъществена в рамките на Работен пакет 1 от научноизследователския проект *„Управление на процесите за реакция при нарушение на сигурността на личните данни в дейността на организациите в Република България“*. Проектът е насочен към формиране на фундаментални научни знания относно механизмите за организационно поведение при инциденти със сигурността на данните. Изследването се основава на интердисциплинарен подход, обединяващ правна перспектива, теории за информационната сигурност и принципи на управление на информационни процеси и технологии.

Актуалността на темата се потвърждава от практиката в Република България, където значителна част от административните санкции, наложени по линия на защитата на личните данни, произтичат от неправилна или липсваща реакция при нарушения на сигурността. Това подчертава необходимостта от ясно структурирани методики и практически приложими указания за поведение при подобни инциденти. Настоящата публикация се стреми да допринесе за по-задълбочено разбиране на тези регулаторни и институционални изисквания.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Методологичната основа на настоящото изследване се изгражда върху правнодогматичния подход, приложен към разпоредбите на чл. 33 и чл. 34 от Регламент (ЕС) 2016/679 (European Parliament and Council of the European Union 2016). В допълнение изследването взема предвид насоките на Европейския комитет по защита на данните, наследник на Работната група по чл. 29 от Директива 95/46/ЕО (Article 29 Data Protection Working Party 2017), включително и „Насоки 01/2021“ (European Data Protection Board 2021), които конкретизират критериите за оценка на риска (напр. категория на данните, брой и уязвимост на засегнатите субекти, потенциални последици) и предоставят примери за типови инциденти. Анализът се допълва и от Методиката за оценка на риска на Комисията за защита на личните данни (КЗЛД 2020). Тя представлява официален механизъм за определяне нивото на риска за правата и свободите на физическите лица при нарушение на сигурността на личните им данни. Приета е като Приложение № 1 към Инструкцията за практическото осъществяване на надзорната дейност на КЗЛД и се използва при анализа на уведомления за инциденти, подадени от администратори на лични данни. Методиката предлага количествена рамка за преценка – чрез матрица (вероятност евентуалното въздействие да настъпи × тежест на въздействието), където резултат над 1,25 води до задължително докладване (а има аргументи да се приеме, че дори и под тази стойност, т.е. при ниско ниво на риск, също трябва да се направи докладване, за да може Комисията да провери верността на направената оценка). Насоките на европейските органи нямат обвързващ правен характер, но служат за интерпретация на GDPR в съответствие с принципите на правна сигурност и предвидимост, като в допълнение с цитираната Методика на КЗЛД формират процедурната и правна рамка за докладване на нарушения на сигурността на данните в България.

РЕЗУЛТАТИ

Докладването на нарушения на сигурността на личните данни е един от най-критичните механизми за защита на субектите на данни и гарантиране на отчетност от страна на организациите. Разпоредбите на чл. 33 и чл. 34 от GDPR уреждат два различни, но взаимносвързани аспекта на уведомяването – към надзорния орган и към засегнатите лица. Те са инструмент не само за правна реакция при инцидент, но и за превенция на по-нататъшни вреди и възстановяване на доверието в администратора. Настоящата част от изследването анализира правната логика, практическите предизвикателства и тълкувателните насоки, свързани с прилагането на тези задължения, като се основава на анализа на регулаторни документи на европейско и национално ниво.

Уведомяване на надзорния орган по чл. 33 от GDPR

Член 33 от Общия регламент относно защитата на данните налага на администратора задължението да уведоми компетентния надзорен орган за нарушение на сигурността на личните данни в срок до 72 часа след узнаване за инцидента. Целта на това уведомяване е да се гарантира своевременна реакция, прозрачност и минимизиране на вредите за засегнатите лица. Изключение се предвижда единствено когато е малко вероятно нарушението да изложи на риск личната неприкосновеност и свободите на субектите на данни.

Уведомлението до надзорния орган следва да съдържа определена минимална информация, включително: описание на естеството на нарушението; категории и приблизителен брой на засегнатите субекти и записи; възможните последици от инцидента, както и мерките, които администраторът е предприел или възнамерява да предприеме за справяне с нарушението на сигурността на личните данни, включително, ако е целесъобразно, мерки за намаляване на евентуалните неблагоприятни последици. Ако е определено длъжностно лице по защита на данните (ДЛЗД), следва да се посочат и неговото име и координатите за връзка, а ако такова не е определено – на друга точка за контакт, от която може да се получи повече информация. Идеята е по този начин КЗЛД да може да осъществи контакт с най-компетентното звено в засегната организация и да може да получава своевременно релевантна и актуална информация във връзка с докладваното нарушение. При невъзможност за предоставяне на цялата информация едновременно GDPR допуска тя да бъде подадена поетапно, без необосновано забавяне.

Съгласно насоките на Европейския комитет по защита на данните срокът започва да тече от момента, в който администраторът е „узнал“ за нарушението, което означава разумно основание да счита, че такова нарушение е настъпило – а не непременно от момента на неговото възникване. Това изискване предполага вътрешна способност на организацията да идентифицира инцидента и да го квалифицира като нарушение, попадащо в обхвата на регламента. При ползване на обработващ моментът на узнаване е неговото уведомяване към администратора, затова е от съществено значение задължението на обработващия да информира администратора „без ненужно забавяне, след като узнае за нарушението“ (чл. 33, пар. 2 от GDPR).

Практическо предизвикателство възниква при преценката кога едно събитие представлява „нарушение на сигурността на личните данни“. Съгласно чл. 4, т. 12 от GDPR това е всяко нарушение, което води до неразрешено разкриване, загуба, изменение или достъп до лични данни – независимо дали е причинено умишлено или по невнимание. Следователно както злонамерени атаки (напр. кибератаки), така и човешки грешки (напр. изпращане на чувствителна информация до грешен получател) подлежат на оценка и потенциално на докладване. Също така случайни събития като наводнения, пожари, земетресения и други природни бедствия също биха могли да доведат до подобно нарушение, ако в резултат на тях се засяга целостта и/или наличността, и/или поверителността на обработвани от администратора лични данни.

Допълнително изискване по чл. 33, ал. 5 от регламента е воденето на вътрешна документация за всички нарушения – включително и за тези, които не подлежат на докладване. Тази задължителна регистрация е част от по-широкия принцип на отчетност и има значение при последващ контрол от страна на надзорния орган.

В България уведомяването по чл. 33 се извършва до Комисията за защита на личните данни, като съответната информация може да бъде подадена по няколко начина – лично или по пощата на хартиен носител, по електронна поща с квалифициран електронен подпис (КЕП) или чрез Системата за сигурно електронно връчване, поддържана от Министерството на електронното управление. С цел улесняване на процеса КЗЛД предоставя утвърден формуляр, публикуван на официалния ѝ уебсайт (Komisiya za zashtita na lichnite danni n.d.).

Уведомяване на субектите на данни по чл. 34 от GDPR

Член 34 от GDPR предвижда допълнителен механизъм за защита на правата и свободите на физическите лица чрез пряко уведомяване на засегнатите субекти при наличие на „висок риск“ вследствие на нарушение на сигурността на личните данни. Това задължение надгражда уведомяването към надзорния орган по чл. 33 и е израз на принципа на прозрач-

ност в обработването на лични данни.

Според регламента уведомяването трябва да се извърши „без ненужно забавяне“ след установяване на високия риск и следва да бъде формулирано на ясен, разбираем и достъпен език. В съобщението задължително се включва информация за естеството на нарушението, потенциалните последици, предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, вкл. препоръки към субектите за ограничаване на вредите (напр. смяна на пароли или контакт с доставчик на услуги), както и координати за контакт с администратора (ДЛЗД или друга точка за контакт).

Насоките на Европейския комитет по защита на данните конкретизират кога уведомяването е необходимо, като предлагат критерии за преценка на високия риск: чувствителност на засегнатите данни (напр. здравни, биометрични, финансови), брой и уязвимост на субектите, вероятност от вреди като кражба на самоличност, дискриминация или загуба на контрол върху лична информация.

Регламентът също така предвижда три основания, при които администраторът може да бъде освободен от задължението да уведоми субектите:

1. Когато са приложени подходящи технически и организационни мерки, които правят данните неразбираеми за неоторизирани лица (напр. ефективно криптиране);

2. Когато след инцидента са предприети мерки, които елиминират вероятността от настъпване на висок риск;

3. Когато индивидуалното уведомяване изисква непропорционални усилия – в този случай следва да се използва публично съобщение или еквивалентна мярка.

На практика прилагането на чл. 34 често създава сериозни трудности за организациите. От една страна, определянето на „висок риск“ е силно контекстуално и предполага не само правна, но и техническа експертиза. От друга страна, формулирането на уведомление, което да отговаря на законовите изисквания и същевременно да бъде разбираемо за широк кръг субекти, изисква специфичен комуникационен капацитет, т.е. умения за ефективно и достъпно предаване на информация.

Допълнително усложнение възниква в случаите, в които администраторът решава да не уведоми засегнатите лица, позовавайки се на някое от основанията за освобождаване. В отсъствие на задължителна съдебна практика и систематизирана надзорна дейност преценката остава в значителна степен на неговата отговорност, което крие риск от санкции при неправилна интерпретация. Отделно риск се корени и в обстоятелството, че според чл. 34, пар. 4 от GDPR надзорният орган може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението на засегнатите субекти на данните, ако последният все още не е направил това. Това е мощен инструмент за пресичане на недобросъвестни действия от администраторите и за защита на субектите, но излага на допълнителни правни и репутационни рискове организациите.

С оглед на това адекватното изпълнение на задълженията по чл. 34 изисква не само нормативно познаване, но и организационна готовност – ясно разписани процедури, предварително подготвени шаблони за уведомление и вътрешна координация между отговорните звена. Само така може да се гарантира навременно, ефективно и законосъобразно информиране на засегнатите субекти при реален инцидент.

Роля на Методиката на КЗЛД в оценката на риска и процеса на докладване

С оглед на общия характер на разпоредбите на чл. 33 и чл. 34 от GDPR необходимостта от практически инструменти за прилагането им на национално равнище придобива особена важност. Методиката на Комисията за защита на личните данни за определяне на нивото на риска при нарушения на сигурността на личните данни представлява ключов елемент от националната административна рамка. Тя е широко възприета като легитимен помощен инструмент за организациите при вземане на решения относно докладването на инциденти.

Методиката предлага структуриран и количествено измерим подход, базиран на два ключови параметъра:

– Вероятност за евентуалното настъпване на негативни въздействия (ВЕР) – стойност от 0 до 1;

– Тежест на въздействието (ТВ) – стойност от 1 до 5.

Нивото на риска (НР) се изчислява по формулата:

$$НР = ТВ \times ВЕР \quad (1)$$

Резултатът се класифицира в три категории:

– Ниско ниво: 0 – 1

– Средно ниво: 1,25 – 2,25

– Високо ниво: 2,5 – 5

Според Методиката на КЗЛД резултат от оценката над 2,5 показва наличие на висок риск, което води до задължително уведомяване на Комисията и субектите на данни. Прави впечатление ниската стойност, при която даден резултат се класифицира като риск с високо ниво и дори средно ниво, което може да създаде сериозни практически трудности и тежки юридически последици за организациите при относително тривиални ситуации. Отделно Методиката допуска известна гъвкавост чрез възможността за адаптиране на оценката спрямо спецификата на конкретната организация и характера на нарушението, но липсва изрично разграничение на прагове над нивото „висок риск“, като например „много висок“ или „катастрофален“ риск. Това може да създаде предизвикателства при интерпретацията и приоритизирането на действията при сериозни инциденти.

Практическата приложимост на формулата за изчисляване на нивото на риска (НР) може се демонстрира чрез следния хипотетичен пример, базиран на Методиката на КЗЛД. При киберинцидент от типа **ransomware атака** тежестта на въздействието (ТВ) се оценява на **4**, а вероятността от настъпване на неблагоприятни последици (ВЕР) – на **0,75**. Прилагането на формулата води до резултат **3**, което попада в категорията „висок риск“ и задейства задължението за уведомяване на КЗЛД и съответните субекти на данни. Примерът илюстрира как количественият модел подпомага администраторите при вземането на информирани решения в ситуации, изискващи правна и организационна реакция в кратки срокове. Методиката балансира между техническа прецизност (чрез количествената формула) и практическа гъвкавост, позволявайки адаптация според спецификата на всеки инцидент.

Методиката заема важно място в българската практика, тъй като допринася за намаляване на правната несигурност, възникваща от липсата на стандартизирани механизми за оценка на риска при нарушения на сигурността на личните данни. Нейните структура и количествена логика предоставят ориентир на администраторите при вземане на решения за докладване. Въпреки това следва да се подчертае, че прилагането ѝ не освобождава администратора от индивидуална отговорност за правилна интерпретация и действие във всеки конкретен случай. КЗЛД не е обвързана с резултатите от вътрешната оценка и запазва правото си самостоятелно да прецени дали е нарушено задължението за уведомяване, включително чрез налагане на санкции при наличие на непълно или закъсняло докладване. Също така в рамките на горепосочения научноизследователски проект, по който се прави настоящата публикация, тепърва предстои да се изясни дали и доколко подобни инструменти, приети от надзорните органи, функционират в другите държави – членки на ЕС, и то спрямо всички администратори на данни. Методиката създава практически затруднения пред администратори – микро, малки и средни предприятия, които не разполагат с нужната техническа и юридическа експертиза адекватно да оценят последиците от съответното нарушение, нито имат финансов ресурс да ангажират външна такава. Удачно е да се обмисли в бъдеще евентуално освобождаване на микро, малки и средни предприятия от някои от задълженията във връзка с докладването на нарушенията и прилагането на Методиката, доколкото това би намалило административната тежест за бизнеса.

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

За подпомагане на прилагането на разпоредбите на чл. 33 и 34 от GDPR, както и за осигуряване на хармонизирана практика, в рамките на Европейския съюз са издадени няколко ключови тълкувателни документа от европейските надзорни органи. Първоначално през октомври 2017 г. т.нар. Работна група по чл. 29 (предшественик на настоящия Европейски комитет по защита на данните) приема *„Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679"*. Документът доразвива легалните дефиниции за „нарушение на сигурността" и „висок риск" и предоставя практически насоки за администраторите на лични данни.

Според насоките всяко нарушение следва да бъде оценено индивидуално, като се вземат предвид фактори като:

- естество и чувствителност на данните (например здравни, финансови, биометрични);
- обхват на инцидента (брой и уязвимост на засегнатите лица);
- възможни последици (напр. кражба на самоличност, дискриминация, загуба на контрол).

Допълнително документът посочва, че 72-часовият срок по чл. 33 започва да тече от момента, в който администраторът „разумно е установил", че е настъпило нарушение – а не непременно от датата на самото събитие. Това уточнение е от съществено значение в практиката и често се подценява от организациите.

По отношение на уведомяването на субектите по чл. 34 насоките съдържат типови сценарии, при които съществува „висок риск" и се налага незабавно уведомление. Например: изтичане на нешифровани здравни досиета, публикуване на чувствителни данни онлайн, загуба на преносими устройства без защита.

Насоките подчертават и ролята на вътрешната организация – необходимо е наличие на процедури, разпределение на отговорности и способност за бързо идентифициране на рисковете и последиците.

Макар да нямат обвързваща правна сила, Насоките на работната група се възприемат от надзорните органи в ЕС, включително КЗЛД, като стандарти за добро прилагане на чл. 33 и 34. Те са ключов ориентир за администраторите, особено в ситуации, в които националната практика е все още ограничена или фрагментарна.

През декември 2021 г. Европейският комитет по защита на данните приема „Насоки 01/2021" относно примерни случаи, свързани с уведомяването за нарушение на сигурността на личните данни, които допълват по-ранните насоки, приети от Работната група по чл. 29. Новият документ представя надградена, практически ориентирана рамка, базирана на конкретни казуси, въз основа на случаи, идентифицирани в регулаторната практика след прилагането на GDPR.

Насоките обхващат редица реалистични сценарии – от атаки с ransomware и изтичане на данни до човешки грешки и загуба на устройства, – като за всеки случай са описани: предишни мерки, оценка на риска, последствия и регулаторни задължения. Централно място заема оценката на риска за правата и свободите на субектите на данни, като се предоставят критерии за определяне на нивото на риска (напр. чувствителност на данните, възможност за злоупотреба, брой засегнати лица).

Важен принос на „Насоки 01/2021" е въвеждането на структуриран подход за вземане на решение относно уведомяването на надзорния орган и субектите на данни чрез съпоставка между тежестта на инцидента и предприетите технически и организационни мерки. Документът препоръчва използването на вътрешна документация и планове за действие при инциденти, включително подготовка на „наръчник" на администратора за справяне с нарушения.

Насоките съдържат таблица на действията за всяка ситуация (вътрешна документация, уведомяване на надзорния орган, уведомяване на субектите), което прави документа ценен инструмент за практическо прилагане на чл. 33 и чл. 34 от GDPR. Те не притежават обвързващ характер, но служат като утвърдена тълкувателна рамка съгласно принципите на правна сигурност и предвидимост в прилагането на регламента.

Насоките, приети от Работната група по чл. 29, имат фундаментално значение за изграждането на първоначалната правна рамка относно задълженията за докладване на наруше-

ния на сигурността по чл. 33 и 34 от Регламент (ЕС) 2016/679. Те поставят акцент върху систематичен правен анализ, дефиниране на основни понятия, условия и процедури, както и ролята на администратора в процеса на уведомяване. „Насоките 01/2021“, приети от Европейския комитет по защита на данните, представляват естествено надграждане на предходните чрез въвеждането на практико-приложен анализ и разглеждане на конкретни казуси въз основа на реални инциденти от надзорната практика в държавите – членки на Европейския съюз. Те предоставят допълнителни ориентири за оценка на риска и съдържат практически препоръки, които подпомагат администраторите при вземането на навременни и адекватни решения. В съвкупност насоките формират интегрирана тълкувателна рамка, която допринася за уеднаквяване на практиката в Европейския съюз и улеснява спазването на нормативните изисквания от страна на администраторите и обработващите лични данни.

ИЗВОДИ/ДИСКУСИЯ

Анализът на разпоредбите на чл. 33 и чл. 34 от Общия регламент относно защитата на данните в съпоставка с тълкувателните насоки на Европейския комитет по защита на данните и Методиката на КЗЛД разкрива наличието на относително добре изградена регулаторна рамка по отношение на задълженията за докладване при нарушения на сигурността на личните данни. Въпреки това практическото прилагане на тази рамка от страна на организациите поражда съществени затруднения, свързани най-вече с оперативната преценка на риска, сроковете за реакция и координацията между технически и правни звена.

Докато текстът на Регламента предоставя основните параметри на задълженията за уведомяване, реалните сценарии често изискват прецизни и контекстуално обвързани интерпретации, особено при определянето на това дали дадено нарушение „вероятно ще доведе до риск“ или „висок риск“. Насоките на ЕКЗД представляват важен ориентир, но тяхното прилагане предполага наличие на експертен капацитет, който не е еднакво развит във всички организации, особено в по-малките и извън сферата на технологиите.

Допълнително, макар Методиката на КЗЛД да предлага полезен инструментариум за количествена оценка на риска, тя все пак създава трудности пред администратори – микро, малки и средни предприятия, които нямат нужния ресурс и експертиза прецизно и навреме да оценят риска от дадено нарушение, следвайки стандартите на Методиката. Това създава несигурност, при която дори добросъвестно взети решения могат да бъдат подложени на санкция.

Изследването показва, че ефективното изпълнение на задълженията по чл. 33 и 34 не се изчерпва с познаване на правната уредба, а изисква изградена вътрешна архитектура на организационно поведение при инциденти – включително наличие на предварително разработени политики, механизми за вътрешна комуникация, обучение на персонала и утвърдени процедури за оценка на риска и формулиране на уведомления.

Това поражда необходимост не само от повишаване на правната култура и институционална готовност сред администраторите, но и от по-ясни стандарти и тълкувателни практики от страна на националния надзорен орган, включително чрез обогатяване на методическите указания с повече конкретни казуси и решения.

ЗАКЛЮЧЕНИЕ

През декември 2018 г. и януари 2019 г. злонамерени лица успяват да осъществят неоторизиран достъп до Extranet системата на Booking.com, използвайки методи на социално инженерство спрямо служители на хотели в Обединените арабски емирства. Компрометирани са личните данни на 4109 потребители, включително имена, адреси, телефонни номера, данни за резервации и данни за кредитни карти на 283 лица, като при 97 от тях – със CVC код. Въпреки че компанията уведомява засегнатите субекти на 4 февруари 2019 г., съобщението до холандския надзорен орган (Autoriteit Persoonsgegevens) е изпратено едва на 7 февруари – 22 дни след узнаване за инцидента, което представлява съществено отклонение от 72-часовия срок, предвиден в чл. 33 от Общия регламент относно защитата на данните. След проведено разследване Autoriteit Persoonsgegevens стига до заключението, че Booking.com е

действала със закъснение и без основателно оправдание. Органът подчертава, че администраторът разполага с възможност да подаде уведомление и на етапи дори при непълна информация, когато рискът за правата и свободите на субектите е очевиден. В резултат компанията е санкционирана с глоба от 475 000 евро (Autoriteit Persoonsgegevens 2020).

Случаят е показателен за практическото прилагане на чл. 33 и чл. 34 от GDPR, като ясно откроява необходимостта от изграждане на ефективни вътрешни механизми за своевременно идентифициране, оценка и докладване на инциденти, засягащи сигурността на личните данни. Същевременно се потвърждава ключовото значение на навременната и адекватна комуникация както с надзорните органи, така и със субектите на данни – особено когато е налице висок риск за техните права и свободи.

Настоящото изследване предостави систематичен анализ на правната рамка относно задълженията за докладване на нарушения на сигурността на личните данни по чл. 33 и чл. 34 от Регламент (ЕС) 2016/679. Разгледани бяха както нормите на първичното европейско право, така и тълкувателните насоки на Европейския комитет по защита на данните и методическите указания на Комисията за защита на личните данни в Република България.

Анализът показва, че ефективното прилагане на правната уредба изисква не само юридическа прецизност, но и наличието на добре изградени вътрешни механизми за реакция при инциденти – включително ясни процедури за оценка на риска и организация на своевременното уведомяване. Макар насоките на ЕКЗД и методиката на КЗЛД да изпълняват важна подпомагаща функция, те не заместват необходимостта от индивидуализиран подход при всяко конкретно нарушение.

Съществуващите неясноти относно критериите за наличие на „риск“ или „висок риск“, кратките срокове за уведомяване и липсата на унифицирана практика очертават необходимостта от допълнителни разяснения, обучения и развитие на професионалната компетентност на администраторите и обработващите лични данни. В този смисъл гарантирането на правна сигурност и съответствие с регулаторните изисквания предполага по-тясно взаимодействие между правната доктрина, институционалната практика и административната координация на национално и европейско равнище.

БЛАГОДАРНОСТИ

Настоящата публикация е изготвена в резултат на научноизследователската дейност по Работен пакет 1, осъществена в рамките на научния проект „Управление на процесите за реакция при нарушение на сигурността на личните данни в дейността на организациите в Република България“, финансиран от Фонд „Научни изследвания“ към Министерството на образованието и науката по „Конкурс за финансиране на фундаментални научни изследвания – 2024“, договор № КП-06-Н85/10 (BG-175467353-2024-11-0016-C01) от 5.12.2024 г.

ЛИТЕРАТУРА

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, 2020. *Методика за определяне нивото на риска при нарушения на сигурността на личните данни. [viewed 17 април 2025 г.]. Available from: https://cpdp.bg/userfiles/file/Kontrolna%20dejnost*

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, n.d. *Подаване на уведомление до КЗЛД по чл. 33 от Регламент (ЕС) 2016/679. [видяно на 17 април 2025 г.]. Достъпно от: https://cpdp.bg/подаване-на-уведомление-до-кзлд-33/*

REFERENCES

Autoriteit Persoonsgegevens, 2020. Decision of 10.12.2020 regarding Booking.com – personal data breach. [viewed 17 April 2025]. Available from: https://gdprhub.eu/index.php?title=AP_%28The_Netherlands%29_-_10.12.2020_%28Booking.com%29

Article 29 Data Protection Working Party, 2017. Guidelines on Personal Data Breach Notification under Regulation 2016/679 (WP250rev.01). 6 February 2017. [viewed 17 April 2025]. Available from: https://ec.europa.eu/newsroom/article29/items/612052/en

European Data Protection Board, 2021. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. [видяно на 17 април 2025 г.]. Достъпно от: https://www.edpb.europa.eu/our – work – tools/our – documents/guidelines/guidelines – 012021 – examples – regarding – personal – data – breach_en

European Parliament And Council Of The European Union, 2016. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 4.5.2016, pp. 1–88. [viewed 17 April 2025]. Available from: https://eur – lex.europa.eu/legal – content/EN/TXT/?uri=CELEX%3A32016R0679

Komisiya Za Zashtita Na Lichnite Danni, 2020. Metodika za opredelyane nivoto na riska pri narusheniya na sigurnostta na lichnite danni. [viewed 17 April 2025]. Available from: https://cpdp.bg/userfiles/file/Kontrolna%20dejnost

Komisiya Za Zashtita Na Lichnite Danni, n.d. Podavane na uvedomlenie do KZLD po chlen 33 ot Reglament (ES) 2016/679. [viewed 17 April 2025]. Available from: https://cpdp.bg/подаване-на-уведомление-до-кзлд-33/

LEGAL AND INSTITUTIONAL FRAMEWORK FOR REPORTING PERSONAL DATA BREACHES: ANALYSIS OF EUROPEAN REQUIREMENTS AND NATIONAL ENFORCEMENT MECHANISMS

Abstract: *This article examines the regulatory framework governing the use of Artificial Intelligence (AI) at both European and national levels, with a focus on its applicability in diplomatic activities. It also analyzes key international legal instruments, including the United Nations General Assembly Resolution (2024), recommendations of the Organisation for Economic Co-operation and Development (OECD), initiatives of the G7 and G20, as well as Regulation (EU) 2024/1689. The scope of the study further encompasses strategic documents adopted in the Republic of Bulgaria. An interdisciplinary methodological approach is applied, based on legal, comparative and normative analysis. The results of the study reveal the need for further improvement of the existing legal framework in order to ensure legal certainty, transparency, and ethical responsibility in the use of AI within public administration and international relations. The article has been developed as part of the first work package of the scientific project "Exploring the possibilities for the application of artificial intelligence in diplomatic activities".*

Keywords: *Artificial Intelligence; diplomatic activities; international relations; regulatory framework*

Prof. Martin Zahariev, PhD
Scopus Author ID: 57218354537
https://orcid.org/0000-0003-4108-6624,
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: m.zahariev@unibit.bg

Assist. Prof. Panayot Gindev
Scopus Author ID: 58811355300
https://orcid.org/0009-0003-7093-890X
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: p.gindev@unibit.bg

Assoc. Prof. Daniela Pavlova, PhD
Scopus Author ID: 57216650930
https://orcid.org/0000-0001-8078-6776,
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: d.pavlova@unibit.bg