

СИГУРНОСТ И ОТБРАНА

**АКТУАЛНО СЪСТОЯНИЕ, ВЪЗМОЖНОСТИ
И ПЕРСПЕКТИВИ**

**ЗА БУКВИТЕ
О ПИСМЕНОСТЪ**

**СИГУРНОСТ И ОТБРАНА
АКТУАЛНО СЪСТОЯНИЕ, ВЪЗМОЖНОСТИ И ПЕРСПЕКТИВИ**

**SECURITY AND DEFENCE
CURRENT STATUS, OPPORTUNITIES AND PERSPECTIVES**



Научната конференция и сборникът са реализирани в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с РМС № 731 от 21.10.2021 г. и съгласно Споразумение № Д01-74/19.05.2022 г. е финансирана от Министерството на образованието и науката на Република България.

The scientific conference and the proceedings have been realized in implementing the National Scientific Program “Security and Defense”, approved by Resolution of the Council of Ministers № 731 dated 21.10.2021 and in compliance with agreement № Д01-74/19.05.2022 funded by the Ministry of Education and Science of the Republic of Bulgaria.

СИГУРНОСТ И ОТБРАНА АКТУАЛНО СЪСТОЯНИЕ, ВЪЗМОЖНОСТИ И ПЕРСПЕКТИВИ

СБОРНИК С ДОКЛАДИ

от Национална научна конференция с международно участие,
проведена на 21 април 2023 г. в Университета по библиотекознание
и информационни технологии

SECURITY AND DEFENCE CURRENT STATUS, OPPORTUNITIES AND PERSPECTIVES

PROCEEDINGS

from the National Scientific Conference with International
Participation held
on the 21st of April 2023 at the University of Library Studies
and Information Technologies

© Проф. д-р Евгени Манев, доц. д-р Диана Стоянова,
д-р Ралица Йотова, д-р Стелиана Йорданова, съставители, 2023
© Проф. д.ик.н. Стоян Денчев, научен редактор, 2023
© Доц. д-р Пламен Богданов, научен рецензент, 2023
© Д-р Ралица Йотова, дизайн на корицата, 2023
© Академично издателство „За буквите – О писменехъ“, 2023
ISBN 978-619-185-593-3

Академично издателство „За буквите – О писменехъ“
София * 2023 * Sofia

ПРАВНИ ГАРАНЦИИ ЗА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ ОТ КОМПЕТЕНТНИТЕ ОРГАНИ ЗА ПОЛИЦЕЙСКИ И НАКАЗАТЕЛНИ ДЕЙНОСТИ

Маргин Захариев

Университет по библиотекознание и информационни технологии,
Фондация „Право и Интернет“,
Адвокатско дружество „Димитров, Петров и Ко.“

Резюме: Компетентните органи по предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване (полицейска и наказателна дейност), обработват редица лични данни за разнообразен кръг субекти – заподозрени, обвиняеми, осъдени лица, свидетели (включително защитени свидетели), пострадали от престъпления, агенти под прикритие и много други. Опазването на техните лични данни от неразрешено или незаконосъобразно обработване и от случайна загуба, унищожаване или повреждане е ключова предпоставка за нормалната и законосъобразна полицейска и наказателна дейност. Нещо повече, компрометирането на сигурността на тези данни е от естество да застраши живота, здравето, правата и свободите на тези и други лица. Ето защо компетентните органи са призвани да прилагат подходящи технически и организационни мерки за сигурността на тези лични данни. Настоящото изложение има за цел да изследва някои основни гаранции за сигурността на данните, закрепени в законодателството на ЕС и българското право, по-специално в Директива 2016/680 и Закона за защита на личните данни.

Ключови думи: лични данни, полицейска и наказателна дейност, сигурност, компетентни органи, Директива 2016/680, ЗЗЛД

1. Въведение в проблематиката на сигурността на личните данни

Предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване (сполучливо наричани в теорията за краткост „полицейска и наказателна дейност“ [1]), предполагат обработването на различни категории лични данни за разнообразен кръг субекти – заподозрени, обвиняеми, осъдени лица, свидетели (включително защитени свидетели), пострадали от престъпления, лица, подали сигнали за престъпления, агенти под прикритие и много други. Без обработването на те-

зи лични данни компетентните органи, като органите на МВР, разследващите митнически инспектори, прокуратурата, следствието и съдът (накратко „компетентните органи“), не могат да реализират своите законоустановени правомощия в сферата на полицейската и наказателната дейност. В същото време опазването на посочените категории лични данни от неразрешено или незаконосъобразно обработване и от случайна загуба, унищожаване или повреждане е ключова предпоставка за нормалната и законосъобразна полицейска и наказателна дейност. Нещо повече, компрометирането на сигурността на тези данни е от естество да застраши живота, здравето, правата и свободите на тези и други лица. Ето защо компетентните органи са призвани да прилагат подходящи технически и организационни мерки за сигурността на тези лични данни.

Настоящото изложение има за цел да изследва някои основни гаранции за сигурността на данните, закрепени в законодателството на ЕС и българското право, по-специално в Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (Директива 2016/680)¹, и транспониращата я глава осма от Закона за защита на личните данни (ЗЗЛД)².

Познаването на посочените правни гаранции е от ключово значение за това компетентните органи да подобрят начина, по който функционират, и в крайна сметка да осигурят по-високо ниво на защита на обработваните от тях лични данни, което следва да е идентично с нивото в останалите държави членки на ЕС. Това е така, защото компрометирането на сигурността на личните данни, респективно неприлагането на подходящи технически и организационни мерки (ТОМ) за сигурност на данните, се оказва нарушението на правилата за защита на личните данни, довело на най-съществените санкции в Република България. По-специално, ноторно известни са следните случаи:

- През 2019 г. Националната агенция за приходите (НАП) **бе санкционирана с 5,1 милиона лева** от Комисията за защита на личните данни (КЗЛД) за изтичане на лични данни [2];
 - През 2019 г. българска банка **бе санкционирана с 1 милион лева** от КЗЛД за изтичане на лични данни [3];
 - През 2022 г. „Български пощи“ ЕАД **беше санкционирано с 1 милион лева** от КЗЛД за неприлагане на подходящи ТОМ [4].
- Размерът на тези санкции не е случаен – причината е, че админис-

тратори на лични данни (АЛД) от такъв мащаб поддържат огромни масиви от лични данни, за да осъществяват своята дейност. Съответно компрометирането на сигурността на информационните системи или фондове на такива АЛД обикновено е от естество да засегне изключително голям брой записи с лични данни за множество субекти на данни, съответно да генерира високи рискове за техните основни права и свободи. Не по-различна е ситуацията при обработването на личните данни за целите на полицейската и наказателната дейност. Нещо повече, в някои случаи потенциалното компрометиране на информационните фондове на компетентните органи може да създаде директна заплаха за живота и здравето на лицата, чиито данни се обработват, или на свързани с тях лица (защитени свидетели, агенти под прикритие и под.). Това налага внимателното изследване на нормативните изисквания, регламентиращи задълженията на АЛД в полицейската и наказателната сфера да прилагат подходящи ТОМ с цел гарантиране на сигурността на данните.

2. Сигурността като принцип, свързан с обработването на лични данни

Обработването на лични данни традиционно се подчинява на определени ръководни идеи и обобщени изисквания, наречени принципи. В правната теория те се дефинират по различен начин – проф. Георги Димитров определя принципите като „правила, които, макар и формулирани по общ начин, създават преки задължения към администраторите на лични данни – своеобразен критерий за дължима грижа при обработване на данните“ [5]. Десислава Тошкова-Николова дефинира принципите като „седем основни начала, които поради основополагащия си характер следва да бъдат спазвани през целия „жизнен цикъл“ на данните – от създаването им до тяхното изтриване или унищожаване на техните носители“ [6]. Едно от тази най-важни изисквания е изискването за сигурност на личните данни, формулирано както в Директива 201/680 (чл. 4, пар. 1, б. „е“), така и в ЗЗЛД (чл. 45, ал. 1, т. 6). Текстът на Директивата е транспониран в ЗЗЛД без каквито и да изменения, т.е. двете норми са идентични. Според посочените норми личните данни трябва да бъдат обработвани по начин, който гарантира **подходящо ниво на сигурност** на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи ТОМ.

Цитираното правило очертава възможните видове непозволено въздействие спрямо личните данни, което може да компрометира тяхната сигурност и за предотвратяването на което компетентните органи трябва да прилагат подходящите ТОМ, а именно:

- **Неразрешено или незаконосъобразно обработване**, което най-общо може да се изрази в каквото и да е обработване в нарушение на законовите изисквания. Това може да означава обработване без правно основание, нарушение на някой от принципите за обработка на данните и много други. В контекста на информационната сигурност едно от основните проявления на неразрешеното или незаконосъобразно обработване е **нарушението на поверителността**;

- **Нарушение на целостта (неразрешено или случайно повреждане)**;

- **Нарушение на наличността (неразрешено или случайно унищожаване или загуба)**.

КЗЛД е имала възможност да дефинира тези понятия, макар и в контекста на нарушения на сигурността на личните данни по Общия регламент относно защита на данните (ОРЗД)³. Въпреки това, предвид относително идентичния терминологичен апарат между ОРЗД и Директива 2016/680 (съответно ЗЗЛД), тези разяснения на КЗЛД са напълно релевантни и при тълкуването на принципа за сигурност по Директивата. Този извод се подкрепя и от правната теория, където се посочва, че „европейската правна уредба в областта на защитата на личните данни борави с унифицирани понятия за „лични данни“ [...] „нарушение на сигурността на личните данни“. Дадените в Регламент (ЕС) 2016/679 легални дефиниции на тези понятия са напълно идентични с определенията в чл. 3 от Директива (ЕС) 2016/680“ [1].

Според КЗЛД:

- **Нарушение на поверителността** означава „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 е в нарушение на ОРЗД“ [7]. В контекста на полицейската и наказателната дейност такива неоправомощени получатели могат да бъдат както трети лица, външни за съответния компетентен орган (например хакери), така и лица от самата структура на компетентния орган, които обаче нямат служебни правомощия да достъпят съответните данни;

- **Нарушение на целостта** означава „преднамерено или случайно повреждане на лични данни.“, като „повреждане“ според КЗЛД означава „личните данни [да] са променени, подправени или станали вече непълни“ [7]. В контекста на полицейската и наказателната дейност това например може да случи, ако трето лице непозволено или случайно измени съдържанието на записи, съхранени от компетентен орган в даден информационен фонд или система;

- **Нарушение на наличността** означава „преднамерена или случайна загуба на данни, унищожаване на данни или неналичие на услуга“. „Загуба“ се дефинира като „състояние, при което данните може да са все още налични“, но АЛД „е загубил контрол или достъп до тях или вече не ги притежава“, а „унищожаване“ – като ситуация, при която „данните вече ги няма или ги няма във вид, в който може да бъдат използвани“ [7]. В контекста на полицейската и наказателната дейност това например може да случи, ако трето лице непозволено достъпи и впоследствие изтрие съдържанието на записи, съхранени от компетентен орган в дадени информационен фонд, или ако същите бъдат унищожени в резултат на бедствие – пожар, наводнение, земетресение и под., засегнали техническата инфраструктура, поддържаща съответен информационен фонд.

С оглед гарантиране на принципа на сигурност и недопускане на горните проявни форми на нарушения Директивата и ЗЗЛД предвиждат **конкретни нормативни изисквания**, които АЛД с правомощия в полицейската и наказателната дейност са длъжни да прилагат. По-долу са разгледани по-съществените от тях.

3. Специфични изисквания за сигурността на личните данни съгласно Директива 2016/680 и ЗЗЛД

3.1. Защита на данните на етапа на проектирането и по подразбиране и прилагане на подходящи ТОМ за сигурност

Чл. 59, ал. 1 ЗЗЛД (в унисон с чл. 20 от Директивата) **задължава АЛД да прилагат подходящи ТОМ**, за да гарантират и да са в състояние да докажат, че обработването се извършва в съответствие със закона. При необходимост тези мерки се преразглеждат и актуализират. Критерии за това кои ТОМ са подходящи, са естеството, обхватът, контекстът и целите на обработването, както и рисковете за правата и свободите на физическите лица. В допълнение и когато това е пропорционално на дейностите по обработване, тези ТОМ могат да включват прилагане от АЛД на подходящи политики за защита на данните (чл. 59, ал. 2 ЗЗЛД). Изискването за пропорционалност предоставя определена гъвкавост на АЛД, т.е. същите имат възможността да преценят дали и доколко са целесъобразни създаването и поддържането на подобни политики. Идеята на законодателя по всяка вероятност е да не се стига до прекален формализъм и АЛД да бъдат задължени във всички случаи да имат такива политики, защото в определени ситуации това може да се окаже ненужно и нуждата да отговорят на подобно задължение, да бъде прекален формализъм, който да създаде пречки пред нормалната им оперативна дейност.

В допълнение, ал. 3 и 4 на същата разпоредба въвеждат т.нар.

принципни изисквания за **защита на личните данни на етапа на проектирането и по подразбиране**, които да се реализират чрез посочените ТОМ. Тези ТОМ трябва да са съобразени с принципите за обработване на лични данни, да се планират към момента на определяне на средствата за обработването на лични данни, т.е. към един момент, **предхождащ** самото обработване, и впоследствие се прилагат при самото обработване. Мерките според ЗЗЛД може да включват (i) псевдонимизация, (ii) свеждане на данните до минимум и (iii) въвеждане на необходими гаранции в процеса на обработване на лични данни. Чрез ТОМ също така АЛД следва да гарантират, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това изискване се разглежда в следните направления: обем на събраните лични данни, степен на обработването, срок на съхраняването им и достъпност на данните. Важна гаранция за сигурността на данните е и правилото, че чрез тези ТОМ по подразбиране, без намеса от страна на физическото лице, личните данни не следва да са достъпни за неограничен брой физически лица. Това пряко кореспондира с аспекта „поверителност“ на данните, анализиран по-горе в т. 2 от настоящото изложение, а именно данните да са достъпни и на разположение само на оторизирани лица при спазване на принципа „необходимост да се знае“.

ЗЗЛД и Директивата, подобно на ОРЗД, възприемат подход, основан на риска при определяне на подходящите ТОМ. Иначе казано, всеки АЛД следва да отчете рисковете за правата и свободите на физическите лица, чиито данни обработва, и да приеме ТОМ, отговарящи на това ниво на риск. Критерии за това решение са достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването. Както се посочва и в теорията, „независимо че уредбата в глава осма от ЗЗЛД е технологично неутрална, са детайлизирани конкретни изисквания по отношение на **автоматизираното обработване**“ [1]. По всяка вероятност законодателят е преценил, че развитието на технологиите предполага тенденция към засилено автоматизирано обработване от страна на АЛД с правомощия в сферата на полицейската и наказателната дейност, респективно завишени рискове при обработване с такива средства. Ето защо е предвидил **конкретни типове ТОМ**, които да гарантират обсъдените по-горе поверителност, цялостност и наличност. Тези конкретни ТОМ са очертани в чл. 66, ал. 2 ЗЗЛД, както следва:

- контрол върху достъпа до оборудване – да се откаже достъп на неоправомощени лица до оборудването, използвано за обработване на лични данни;
- контрол върху носителите на данни – да се предотвратят чете-

нето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица;

- контрол върху съхраняването – да се предотврати въвеждането на лични данни от неоправомощени лица, както и извършването на проверки, изменянето или изтриването на съхранявани лични данни от неоправомощени лица;

- контрол върху потребителите – да се предотврати използването на автоматизирани системи за обработване от неоправомощени лица чрез използване на оборудване за предаване на данни;

- контрол върху достъпа до данни – да се гарантира, че лицата, на които е разрешено да използват автоматизирана система за обработване, имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп;

- контрол върху комуникацията – да се гарантира възможността за проверка и установяване на кои органи са били или могат да бъдат предадени лични данни, или кои органи имат достъп до лични данни чрез оборудване за предаване на данни;

- контрол върху въвеждането на данни – да се гарантира възможността за последваща проверка и установяване какви лични данни са били въведени в автоматизираните системи за обработване, както и кога и от кого са били въведени;

- контрол върху пренасянето – да се предотвратят четенето, копирането, изменянето или изтриването на лични данни от неоправомощени лица при предаването на лични данни или при пренасянето на носители на данни;

- възстановяване – да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на функциите на системите;

- надеждност – да се гарантират изпълнението на функциите на системата и докладването за появили се във функциите дефекти;

- цялостност – да се гарантира недопускане на увреждане на съхраняваните лични данни вследствие на неправилно функциониране на системата.

Извън горепосочените ТОМ подходът, основан на риска, не предполага нормативното уреждане на конкретни ТОМ, които да са общозадължителни за всички АЛД. Иначе казано, няма унифициран набор ТОМ, които всеки АЛД да прилага. Това бе и причината **КЗЛД да отмени действащата в миналото Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни**, считано от 25.05.2018 г. – датата, от която започна да се прилага ОРЗД [8] (по-рано същия месец, а именно до 06.05.2018 г., следваше да се транспонира в законодателст-

вото на държавите членки Директива 2016/680). Това е така, защото нормативното закрепване на общозадължителни ТОМ противоречи на идеята на подход, основан на риска, закрепена от ОРЗД и Директивата.

На последно място следва да се отбележи, че при ангажиране на обработващ личните данни (ОЛД) АЛД е длъжен да **ползва само обработващи, които предоставят достатъчни гаранции, че ще прилагат подходящи ТОМ** по такъв начин, че обработването да отговаря на изискванията на глава осма от ЗЗЛД и да се гарантира защитата на правата на субекта на данни (чл. 61, ал. 1 ЗЗЛД). Съответно конкретните ТОМ, прилагани от АЛД или обработващия в съответствие с принципа на отчетност, следва (когато е възможно) **да са закрепени в регистрите по чл. 62, ал. 1 и 2 ЗЗЛД**. Това са допълнителни нормативни изисквания, обезпечаващи реализацията на принципа на сигурност при обработването за целите на полицейската и наказателната дейност.

3.2. Съхраняване на системни дневници (логове)

Специфично изискване, което не е изрично уредено в ОРЗД, но присъства в Директивата и ЗЗЛД, е това за **водене на системни дневници (логове) в системите за автоматизирано обработване**, поддържани от АЛД и ОЛД. Тези логове съгласно чл. 63 ЗЗЛД се водят най-малко за следните операции по обработване: (i) събиране, (ii) промяна, (iii) справки, (iv) разкриване, включително предаване, (v) комбиниране и (vi) изтриване. Законът изисква при извършване на справка или разкриване на данни тези логове да дават възможност за установяване на основанието, датата и часа на тези операции и доколкото е възможно – идентификацията на лицето, което е направило справка или е разкрило личните данни, както и данни, идентифициращи получателите на тези лични данни. Воденето на логове съгласно Работната група по чл. 29 има „**двойна цел**“, тъй като може да се използва като „възпиращо действие срещу неразрешена употреба, което може да бъде ефективно само ако се въведе правило за анализ на записи, и като наказателно действие при откриване на нарушение“, и като подпомагачо „укрепването на дейността за самоодитиране на администраторите чрез периодични доклади за анализи на записи, които могат да се изготвят по автоматизиран начин и да са съобразени с конкретни области на правоприлагането“ [9]. Това тълкуване е намерило разрешение и в нормата на чл. 63, ал. 3 ЗЗЛД, според която логовете се използват единствено за проверка на законосъобразността на обработването, за самоконтрол, за гарантиране на целостността и сигурността на личните данни и при наказателни производства. АЛД е длъжен да определи подходящи срокове за съхранение, включително архивиране на посочените логове, а при поискване АЛД и ОЛД са длъжни да пре-

доставят логовете на контролните органи – КЗЛД или Инспектората към ВСС. Това задължение е разбираемо, доколкото логовете може да съдържат важна информация във връзка с хронологията на дадени събития, имащи значение за законосъобразността на дадено обработване – обект на проверка (одит) от посочените надзорни органи.

Следва да се отбележи, че по силата на § 45 от Преходните и заключителни разпоредби на ЗЗЛД (в съответствие с възможността за делегация по чл. 63, пар. 2 от Директивата) изискванията за водене на логове по чл. 63, ал. 1 и 2 ЗЗЛД, приложими към системите за автоматизирано обработване, използвани от компетентните органи и създадени преди 6 май 2016 г. (първия ден след влизане в сила на Директива 2016/680), следва да се изпълнят до 6 май 2023 г. Ето защо за компетентните органи е налице определен гратисен период, в който да направят нужните технически трансформации, така че да адаптират системите си в съответствие с посочените изисквания.

3.3. Оценка на въздействието върху защитата на данните и предварителна консултация с надзорен орган

Членове 64 и 65 ЗЗЛД регламентират извършването на **оценка на въздействието върху защитата на данните (ОВЗД) и необходимостта от извършването на предварителна консултация** с КЗЛД съответно Инспектората към ВСС. Това са важни инструменти за гарантиране на сигурността на данните. Причината е, че ОВЗД се извършва при операции по обработване, при които се използват нови технологии, и предвид естеството, обхвата, контекста и целите им има вероятност да възникне висок риск за правата и свободите на физическите лица. ОВЗД се извършва преди самото обработване. ОВЗД има минимално установено законово съдържание, а именно: общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, **мерки за сигурност и механизми за гарантиране на защитата на личните данни** и за доказване на съответствие с правилата на глава осма ЗЗЛД, като се вземат предвид правата и законните интереси на субектите на данните и другите засегнати лица. Доколкото мерките за сигурност и механизмите за гарантиране на защита на личните данни са част от законоустановеното съдържание на ОВЗД, това е важна законова гаранция АЛД да адресират въпроса за сигурността на данните още на този предварителен оценъчен етап, предхождащ започването на самото обработване.

Процедурата по предварителна консултация се инициира от АЛД/ОЛД преди обработването на лични данни, което ще бъде част от

нов регистър с лични данни, предстоящ да се създаде, когато: 1. съгласно ОВЗД обработването **ще породи висок риск** въпреки предприетите от АЛД мерки за ограничаване на риска или 2. видът обработване, поспециално когато се използват нови технологии, механизми или процедури, **включва висока степен на риск за правата и свободите на субектите на данните**. Също така при изготвянето на проекти на закони и на подзаконовни нормативни актове, съдържащи мерки относно обработването, се провеждат консултации с КЗЛД, съответно с Инспектората към ВСС. КЗЛД в съответствие с чл. 65, ал. 3 ЗЗЛД е приела и **списък на операциите, при които е задължителна предварителна консултация**. Тези операции са следните:

- Редовно и систематично обработване на данни за местоположение на лица с технически средства с цел осъществяване на контрол по спазването на мярка за неотклонение по чл. 58 от Наказателнопроцесуалния кодекс;

- Мащабно обработване на лични данни на деца за целите на предотвратяване, разследване или разкриване на противообществени прояви или престъпления, извършени от или срещу малолетни и непълнолетни, включително за целите на прилагане на възпитателни мерки или наказания;

- Мащабно обработване на специални категории лични данни по чл. 51, ал. 1 от ЗЗЛД, когато това е свързано с автоматизирано вземане на решения, включително с цел извършване на криминологичен анализ;

- Осъществяване на систематично мащабно наблюдение на публично достъпни зони, когато това е свързано с автоматизирано вземане на решения, включително лицево разпознаване;

- Осъществяване на миграция на данни от съществуващи към нови технологии, когато това е свързано с мащабно обработване на данни [10].

Ако надзорният орган прецени, че планираното обработване ще наруши правилата на ЗЗЛД, същият предоставя писмено становище на АЛД/ОЛД. Това не засяга възможността надзорният орган да упражни надзорните си правомощия по чл. 80 ЗЗЛД. Намесата на компетентния надзорен орган в рамките на посочената процедура също е важна законова гаранция за гарантиране на високо ниво на защита на данните, включително за спазване на принципа за сигурност на данните.

3.4. Действия при нарушение на сигурността на личните данни

В случай на нарушение на сигурността на личните данни (НСЛД) ЗЗЛД урежда няколко групи задължения за уведомяване. **Първо**, ако НСЛД има вероятност да доведе **до риск** за правата и свободите на субектите на данни, АЛД без излишно забавяне, но не по-късно от 72 ча-

са след като е разбрал за нарушението, уведомява КЗЛД, съответно Инспектората към ВСС, за него с минимално установено от ЗЗЛД съдържание (чл. 67, ал. 3). Когато уведомлението е подадено след срока по изречение първо, в него се посочват причините за забавянето. **Второ**, ОЛД уведомява АЛД без излишно забавяне, но не по-късно от 72 часа след като е установил НСЛД. Тук следва да се отбележи, че подобен срок не е фиксиран по ОРЗД. Идеята е ОЛД да уведоми във възможно най-бърз порядък АЛД, за да може последният да предприеме нужните мерки за справяне с НСЛД и неблагоприятните последици от него. **Трето**, ако НСЛД засяга лични данни, които са изпратени от или на АЛД от друга държава членка на ЕС, информацията от задължителното съдържание на уведомлението до надзорен орган се съобщава на този АЛД без излишно забавяне, но не по-късно от 7 дни от установяването на нарушението. Логиката е компетентният АЛД от друга държава от своя страна да предприеме мерки за ограничаване на неблагоприятните последици от НСЛД – да предупреди субектите на данни, да предприеме действия съобразно правомощията си и т.н. **Четвърто**, когато има вероятност НСЛД да доведе до висок риск за правата и свободите на субектите на данни, АЛД уведомява и субекта на данните за нарушението не по-късно от 7 дни от установяването му с минимално установена от закона информация (чл. 68, ал. 2, вр. чл. 67, ал. 3, т. 2, 3 и 4 ЗЗЛД).

Изключения от задължението за уведомяване са предвидени, ако: 1. АЛД е предприел подходящи ТОМ за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението, по-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране; 2. АЛД е взел впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни; 3. уведомяването би довело до непропорционални усилия, като в този случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да са в еднаква степен ефективно информирани. Надзорният орган може да изиска от АЛД да уведоми субекта на данните, отчитайки спецификите на съответната ситуация. АЛД може да не уведоми субекта на данните за НСЛД, да го уведоми след законовия срок, както и да ограничи предоставената информация по важни съображения, очертани в закона, като: (i) недопускане на възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури; (ii) недопускане на неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; (iii) защита на обществеността и сигурност; (iv) защита на националната сигурност; (v)

защита на правата и свободите на други лица. Отделно АЛД документира всяко НСЛД, като включва фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него. Тези изисквания по уведомяване и документиране са допълнителна гаранция за реализиране на принципа на сигурност, макар и във възможно най-нежеланата ситуация, при която вече се е стигнало до компрометиране на сигурността в рамките на конкретно НСЛД. Те спомагат за повишаване на отчетността, както и за превенция с оглед недопускане на бъдещи подобни нарушения.

Заклучение

В заключение следва да се отбележи, че разбирането за това какво представлява принципът на сигурност на данните и какви конкретни изисквания същият предполага да се реализират при обработването на лични данни, е важна предпоставка пред осигуряването на високо ниво на защита на данните от компетентните органи с правомощия в сферата на полицейската и наказателната дейност. Съществена в този ред на мисли е необходимостта гореописаните правила и принципи да не останат разписани само документално, без реално да се прилагат и спазват в съответната организация, а да се трансформират в реално действащи процеси в рамките на компетентните органи.

Представеният анализ няма характера на правен съвет или консултация и не следва да бъде възприеман като достатъчен за разрешаването на конкретни правни проблеми, казуси и др. Мненията, изразени тук, са единствено на автора и не отразяват непременно тези на УниБИТ, Фондация „Право и Интернет“, Адвокатско дружество „Димитров, Петров и Ко.“, техните филиали или служители. Материалът е съобразен с действащото българско законодателство и законодателство на ЕС към 02.12.2022 г.

Бележки

¹ **Direktiva** (ES) 2016/680 на Evropeyskiya parlament i na Saveta ot 27 april 2016 godina odnosno zashtita na fizicheskite litsa vav vrazka s obrabotvaneto na lichni dannii ot kompetentnite organi za tselite na predovratyavaneto, razsledvaneto, razkrivaneto ili nakazatelnoto presledvane na prestapleniya ili izpalnenieto na nakazaniya i odnosno svobodnoto dvizhenie na takiva dannii i za otmyana na Ramkovo reshenie 2008/977/PVR na Saveta, obn. OJ L 119, 4.5.2016, s. 89 – 131.

[**Директива** (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказател-

ното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, обн. OJ L 119, 4.5.2016, с. 89 – 131.]

² **Закон** за zashtita na lichnite dannii, obn. DV, br. 1 ot 4 yanuari 2002 g., posl. izm. DV, br. 93 ot 26.11.2019 g. s Reshenie № 8 ot 15.11.2019 g. na KS na RB po k.d. № 4/ 2019 g.

[**Закон** за защита на личните данни, обн. ДВ, бр. 1 от 4 януари 2002 г., посл. изм. ДВ, бр. 93 от 26.11.2019 г. с Решение № 8 от 15.11.2019 г. на КС на РБ по к. д. № 4 / 2019 г.]

³ **Reglament** (ES) 2016/679 na Evropeyskiya parlament i na Saveta ot 27 april 2016 godina otosno zashtitata na fizicheskite litsa vav vrazka s obrabotvaneto na lichni dannii i otosno svobodnoto dvizhenie na takiva dannii i za otmyana na Direktiva 95/46/EO (Obsht reglament otosno zashtitata na dannite) (Tekst ot znachenie za EIP), obn. OJ L 119, 4.5.2016, s. 1 – 88.

[**Регламент** (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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) (Текст от значение за ЕИП), обн. OJ L 119, 4.5.2016, с. 1 – 88.]

Литература/References

[1] **Feti, N., D. Toshkova-Nikolova.** Prilagane na zashtitata na lichnite dannii. Sofia: Trud i pravo, 2020.

[**Фети, Н., Д. Тошкова-Николова.** Прилагане на защитата на личните данни. София: Труд и право, 2020.]

[2] **KZLD.** Informatsia za izwurshena proverka v Natsionalnata agentsia za prihodite, 2019 [vidiano na 21 noemvri 2022 g.]. Dostupno na: https://www.cdpd.bg/index.php?p=news_view&aid=1519.

[**КЗЛД.** Информация за извършена проверка в Националната агенция за приходите, 2019 [видяно на 21 ноември 2022 г.]. Достъпно на: https://www.cdpd.bg/index.php?p=news_view&aid=1519.]

[3] **KZLD.** Predsedateliat na Komisiata za zashtita na lichnite dannii izdade Nakazatelno postanovlenie na „Banka DSK“ EAD, 2019 [vidiano na 21 noemvri 2022 g.]. Dostupno na: https://www.cdpd.bg/?p=news_view&aid=1514https://www.cdpd.bg/index.php?p=news_view&aid=1519.

[**КЗЛД.** Председателят на Комисията за защита на личните данни издаде Наказателно постановление на „Банка ДСК“ ЕАД, 2019 [видяно на 21 ноември 2022 г.]. Достъпно на: https://www.cdpd.bg/?p=news_view&aid=1514.]

[4] **Stoianova, Ts.** 1 mln. lv. globa za „Balgarski poshti“ zaradi lipsa na kiberzashtita, 2022 [vidiano na 21 noemvri 2022 g.]. Dostupno na: <https://bnr.bg/horizont/post/101682506/1-mln-lv-globa-za-balgarski-poshti-zaradi-lipsa-na-kiberzashtita>.

[**Стоянова, Ц.** 1 млн. лв. глоба за „Български пощи“ заради липса на киберзащита, 2022 [видяно на 21 ноември 2022 г.]. Достъпно на:

<https://bnr.bg/horizont/post/101682506/1-mln-lv-globa-za-balgarski-poshti-zaradi-lipsa-na-kiberzashtita>.]

[5] **Dimitrov, G.** Pravo na informatsionnite i komunikatsionnite tehnologii. Chast II. Administrativnopravni i tehnologichni aspekti. Elektronno upravlenie. Praven rezhim na informatsiata. Praven rezhim na kriptografiyata. Standartizatsiya v oblastta na IKT. Sofia: Fondatsiya Pravo i Internet, 2014.

[**Димитров, Г.** Право на информационните и комуникационните технологии. Част II. Административноправни и технологични аспекти. Електронно управление. Правен режим на информацията. Правен режим на криптографията. Стандартизация в областта на ИКТ. София: Фондация „Право и Интернет“, 2014.]

[6] **Toshkova-Nikolova, D., N. Feti.** Zashtita na lichnite dannii. Sofia: Trud i pravo, 2019.

[**Тошкова-Николова, Д., Фети, Н.** Защита на личните данни, С., ИК „Труд и право“, 2019.]

[7] **KZLD.** Prilozhenie No 1 kum Instruksia za prakticheskoto osushtestviavane na nadzornata dejnost na Komisiata za zashtita na lichnite dannii – Metodika za opredliane na nivoto na riska pri narushenia na sigurnostta na lichnite dannii, 2021 [vidiano na 21 noemvri 2022 g.]. Dostupno na: <https://www.cdpd.bg/userfiles/file/Kontrolna%20dejnost/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BA%D0%B0%20%D0%B7%D0%B0%20%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B0%20%D0%BD%D0%B0%20%D1%80%D0%B8%D1%81%D0%BA%D0%B0%20%D0%BF%D1%80%D0%B8%20%D0%BD%D0%B0%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BD%D0%B0%20%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82%D1%82%D0%B0.pdf>

[**КЗЛД.** Приложение № 1 към Инструкция за практическото осъществяване на надзорната дейност на Комисията за защита на личните данни – Методика за определяне нивото на риска при нарушения на сигурността на личните данни, 2021 [видяно на 21 ноември 2022 г.]. Достъпно на: <https://www.cdpd.bg/userfiles/file/Kontrolna%20dejnost/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BA%D0%B0%20%D0%B7%D0%B0%20%D0%BE%D1%86%D0%B5%D0%BD%D0%BA%D0%B0%20%D0%BD%D0%B0%20%D1%80%D0%B8%D1%81%D0%BA%D0%B0%20%D0%BF%D1%80%D0%B8%20%D0%BD%D0%B0%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BD%D0%B0%20%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82%D1%82%D0%B0.pdf>.]

[8] **KZLD.** Naredba № 1 ot 30 ianuari 2013 za minimalnoto nivo na tehicheski i organizatsionni merki i dopustimia vid zashtita na lichnite dannii – otmenena, schitano ot 25.05.2018, 2018 [vidiano na 22 noemvri 2022 g.]. Dostupno na: <https://www.cdpd.bg/?p=element&aid=1151>.

[**КЗЛД.** Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни – отменена, считано от 25.05.2018, 2018 [видяно на 22

ноември 2022 г.]. Достъпно на: <https://www.cdpd.bg/?p=element&aid=1151>.]

[9] **RG29.** Stanovishte относно nkiakoi kliuchovi vuprosi vuv vruzka s Direktiva (ES) 2016/680 относно pravoprilaganeto, WP 258, prieto na 28 noemvri 2017 g. [vidiano na 22 noemvri 2022 g.]. Dostupno na: <https://ec.europa.eu/newsroom/article29/items/610178>.

[**РГ29.** Становище относно някои ключови въпроси във връзка с Директива (ЕС) 2016/680 относно правоприлагането, WP 258, прието на 29 ноември 2017 г. [видяно на 22 ноември 2022 г.]. Достъпно на: <https://ec.europa.eu/newsroom/article29/items/610178>.]

[10] **KZLD.** Spisuk na operatsiite po obrabotvane na lichni dannii, za koito e zaduljitelna predvaritelnata konsultatsia po chl. 65, al. 3 ot Zakona za zashtita na lichnite dannii, 2022 [vidiano na 22 noemvri 2022 g.]. Dostupno na: <https://www.cdpd.bg/?p=element&aid=1151>.

[**КЗЛД.** Списък на операциите по обработване на лични данни, за които е задължителна предварителна консултация по чл. 65, ал. 3 от Закона за защита на личните данни, 2022 [видяно на 22 ноември 2022 г.]. Достъпно на: <https://www.cdpd.bg/?p=element&aid=1368>.]

LEGAL GUARANTEES FOR THE SECURITY OF PERSONAL DATA PROCESSED BY THE COMPETENT AUTHORITIES FOR LAW ENFORCEMENT ACTIVITIES

Abstract: The competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection from threats to public order and security and their prevention (police and criminal activity) process a number of personal data for a diverse range of subjects – suspects, accused, convicted persons, witnesses (including protected witnesses), victims of crimes, undercover agents and many others. Protecting their personal data from unauthorized or unlawful processing and from accidental loss, destruction or damage is a key prerequisite for the normal and lawful police and criminal activity. Moreover, compromising the security of this data is likely to endanger the lives, health, rights and freedoms of these and other individuals. Therefore, the competent authorities are called upon to implement appropriate technical and organizational measures for the security of these personal data. This paper aims to explore some basic data security guarantees enshrined in EU and Bulgarian law, in particular Directive 2016/680 and the Personal Data Protection Act.¹⁰

Keywords: personal data, law enforcement activity, security, competent authorities, Directive 2016/680, Personal Data Protection Act

Assoc. Prof. Martin Zahariev, PhD
Univeristy of Library Studies and Information Technologies
E-mail: m.zahariev@unibit.bg