

Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 1 (94), януари 2022 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода ноември и декември 2021 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
ВАС постанови решение, в което формулира критерии за преценка на баланса между правото на свобода на изразяване и информация и правото на защита на личните данни	3
КЗЛД публикува информационно-разяснителен материал относно действията на АЛД при настъпване на нарушение на сигурността на личните данни	4
КЗЛД издаде информационна брошура “Шенгенското пространство и защитата на личните данни”	9
Заседания на Европейския комитет по защита на данните	11
Европейският парламент и Съветът постигнаха предварително споразумение относно Акта за управление на данните	12
Европейската комисия приема мерки в полза на киберсигурността на безжичните устройства и продукти	14
Състоя се 43-тото издание на Глобалната асамблея по въпросите на неприкосновеността	15
Заседание на Консултативния комитет на Конвенция 108 на Съвета на Европа ..	18
Успешно завърши изпълнението на проект AI-Trans, финансиран от ЕС	20
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	22
РЕШЕНИЯ НА КЗЛД	23
СТАНОВИЩА НА КЗЛД	30
АНАЛИЗИ	42
Обобщена практика на КЗЛД след 25 май 2018 г. по въпроси, свързани с осъществявано видеонаблюдение	42

СЪБИТИЯ И ИНИЦИАТИВИ

ВАС ПОСТАНОВИ РЕШЕНИЕ, В КОЕТО ФОРМУЛИРА КРИТЕРИИ ЗА ПРЕЦЕНКА НА БАЛАНСА МЕЖДУ ПРАВОТО НА СВОБОДА НА ИЗРАЗЯВАНЕ И ИНФОРМАЦИЯ И ПРАВОТО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ



На 16.11.2021 г. Върховният административен съд (ВАС) постанови решение по дело на КЗЛД срещу електронна медия, заведено във връзка с публикуването на лични данни на физическо лице за целите на журналистически материал.

Решението на ВАС е особено ценно с това, че **формулира критерии за преценка на баланса между две конкуриращи се права** - правото на свобода на изразяване и информация и правото на защита на личните данни, доколкото и двете не са абсолютни.

Председателят на КЗЛД Венцислав Караджов изрази очакванията си медиите да отчетат принципните разсъждения в това съдебно решение и припомни, че през 2019 г. Конституционният съд отмени текстове от Закона за защита на личните данни, с които бе направен опит да се въведат критерии за използване на лични данни за журналистически цели, с които журналистите трябва да се съобразяват в публикациите си, за да не нарушават Общия регламент за защита на данните (GDPR). По думите на г-н Караджов *„На практика чрез отмяната Конституционният съд даде приоритет на съдебната практика, която в случая представя прецедент, който трябва внимателно да бъде разгледан от медиите в България.“* Председателят на КЗЛД подчерта, че случаи като конкретния, са показателни за начина, по който следва медиите да разсъждават, когато обработват личните данни. Освен това, съгласно чл. 25з, ал. 1 от Закона за защита на личните данни (ЗЗЛД), обработването на лични данни за журналистически цели е законосъобразно, когато се извършва за осъществяване на свободата на изразяване и правото на информация, при зачитане на неприкосновеността на личния живот, т. е. отново при преценка на баланса на двете права, като следва да бъде зачитан принципа на „свеждане на данните до минимум“.

През 2020 г. в КЗЛД е подадена жалба от публична личност срещу електронна медия, която е публикувала „за журналистически цели“ информация относно физическата идентичност на жалбоподателя (три имена, част от ЕГН/рождена дата, адрес), икономическа идентичност (имотно и финансово състояние, участие и членство в неправителствена организация), социална идентичност (професия, месторабота, трудова дейност, информация за принадлежност) - лични данни по смисъла на чл. 4, т. 1 от Регламент (ЕС) 2016/679.

Както е посочено в решението на ВАС, понятието „журналистически цели“ не е дефинирано от законодателя, но е тълкувано в съдебната практика, като съществено за дейността е събирането, анализирането, интерпретирането и разпространяването чрез средствата за масова информация на актуална и обществено значима информация и всяка журналистическа дейност е проява на свободата на словото в правовата държава.

Законът позволява да се публикуват лични данни за журналистически цели, но при добросъвестна преценка във всеки отделен случай на баланса между правото на свобода на изразяване и на информация и правото на защита на личните данни.

В решението си от 16 ноември 2021 г. ВАС за първи път обяснява как се извършва преценката при всеки конкретен случай за това кои данни е допустимо да бъдат публикувани за целите на журналистическата публикация.

В решението на съда се дава смисълът на ограничението, което налага принципът на „свеждане на данните до минимум“. За целите на журналистическото разследване следва да се публикуват необходимите и достатъчни лични данни, с което свободата на изразяване и информация може да бъде удовлетворена. Не трябва да се допуска непропорционална намеса в личния живот на физическите лица, производно от което е и правото на защита на личните данни. В решението се посочва, че фактът, че източник на част от информацията е Имотния регистър, не прави публикуването на данните законосъобразно, защото регистърът има различни цели от журналистическите, а освен това данните не са непосредствено публично достъпни. В този смисъл обработването на лични данни за целите на журналистическата дейност са операция по ново обработване на данни, с нова цел, които следва да отговарят на изискванията на ОРЗД, в това число и на принципа за свеждане на данните до минимум.

Във връзка с постановеното решение, в последващ коментар, председателят на КЗЛД допълва, че настоящото решение на ВАС се отнася не само за публични личности, но и за всеки друг гражданин, който стане обект на журналистическо разследване. Едно такова разследване трябва да представи на обществото необходимата информация, която позволява да се направи обективна и информирана преценка дали даден човек е извършил нещо неправомерно, обществено или морално осъдително, но без да се засяга непропорционално неприкосновеността на личния му живот.

Председателят на КЗЛД Венцислав Караджов пояснява *„Необходим е баланс между правото на информация на обществеността и правото на защита на личен живот на физическото лице. Противното би означавало целенасочено действие за увреждане авторитета на лицето, предмет на журналистическото разследване. Фактът, че в случая се използва информация от публични източници, не значи, че тя е пропорционална на целите на разследването. Информацията в Имотния регистър е събрана за друга цел - тя дава информация за това кой е собственикът на конкретен имот, къде се намира, има ли тежест. Когато тази информация се обработва от журналистите за други цели, следва да се направи преценка от медията дали и в каква степен публично достъпната информация е несъотнесима към журналистическите цели на разследването и в този смисъл - дали трябва да бъде детайлно публикувана или само тази част от нея, която допринася за изясняване целта на разследването“.*

КЗЛД ПУБЛИКУВА ИНФОРМАЦИОННО-РАЗЯСНИТЕЛЕН МАТЕРИАЛ ОТНОСНО ДЕЙСТВИЯТА НА АДЛ ПРИ НАСТЪПВАНЕ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Утвърдена практика на КЗЛД е по достъпен и разбираем начин да разяснява на обществото основните положения от правната рамка в ЕС в областта на личните данни, както и националното законодателство в тази сфера. Информационно-разяснителните дейности на КЗЛД са с постоянен характер и тяхната цел е посланията да достигнат до максимално широк кръг заинтересовани лица – граждани, администратори на лични данни, длъжностни лица по защита на данните. За тази цел на институционалния сайт и в информационния бюлетин на КЗЛД се публикуват редица информационни материали – насоки, указания, разяснения и т.н., като целта е в максимална степен да се обхванат различните категории потребители на тази информация – граждани, администратори, потребители с различна степен на познания и ориентиране в сферата на опазване сигурността на личните данни и гарантиране правата на гражданите.

През ноември 2021 г. КЗЛД публикува на своя институционален сайт информационно-разяснителния материал „Действия на администраторите на лични данни при настъпване на нарушение на сигурността на личните данни“. Целта на материала е да се въведат разяснения относно основните

действия на АЛД при настъпване на нарушение на сигурността на данните - уведомяване на надзорния орган; уведомяване на субектите на данни; съдържание на уведомлението до надзорния орган; оценка на риска за правата и свободите на субектите на данни, извършвана от АЛД; приложими мерки за минимизиране на неблагоприятните въздействия върху правата и свободите на субектите на данни; документиране на нарушенията на сигурността на данните от АЛД/ОЛД. В настоящия бюлетин публикуваме материала, който е достъпен и на сайта на КЗЛД – [ТУК](#).

Действия на администраторите на лични данни при настъпване на нарушение на сигурността на личните данни – чл.33 и чл.34 от Регламент (ЕС) 2016/679

Какво да правим при нарушение на сигурността на личните данни?

Предлагаме на вниманието на администраторите и обработващите лични данни кратък материал с отговор на въпроси като - кога има нарушение на сигурността и какви са видовете нарушения. Каква последователност на действия, следва да се предприемат от при настъпване на нарушение на сигурността на личните данни. Защо уведомяването по чл.33 от Регламент (ЕС) 2016/679 е важен инструмент за засилване на спазването на заложените в Регламента изисквания за защита на личните данни. Кога се изисква уведомяване на надзорния орган и кога на засегнатите субекти на данни, в съответствие с чл. 34 от Регламент (ЕС) 2016/679. Какво е минималното съдържание на уведомлението. Какви технически и организационни мерки за минимизиране вероятността от настъпване на нарушение следва да се предприема и какви технически и организационни мерки се предприемат за преодоляване на последиците от евентуално такова. Оценка на риска и нейното място при нарушенията. Какво и как се документира при нарушение на сигурността на данните.

1. Нарушения на сигурността на личните данни.

1.1. Уведомяването за нарушение на сигурността на личните данни по чл.33 от Регламент (ЕС) 2016/679 (ОРЗД, Регламента) е изцяло нов момент, въведен от Регламента и е със задължително действие за всички администратори на лични данни (АЛД, администратора). Обработващите лични данни (ОЛД, обработващия) имат задължение да уведомяват за нарушение на сигурността своя АЛД. В определени хипотези, посочени в чл.34 от ОРЗД, АЛД уведомяват и субектите на лични данни. Уведомяването по чл.33 и/или по чл.34 от ОРЗД трябва да се разглеждат като важен инструмент за отчитане на спазването на Регламента.

1.2. Всеки АЛД/ОЛД следва предварително да планира действията си и да въведе процедури, които да му гарантират бързото откриване и ограничаване на нарушението на сигурността на лични данни, за да може своевременно да оцени риска за субектите на лични данни и съответно да предприеме задължителните действия, посочени в ОРЗД.

1.3. Легалната дефиниция е посочена в чл. 4, пар.12 от ОРЗД - „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

Важно! Ключов момент е оценката, която АЛД/ОЛД ще направи на настъпилото събитие и преценка на неговите евентуални последици.

2. Уведомяване на надзорния орган по чл.33 от ОРЗД.

2.1. Уведомяването на КЗЛД от АЛД става без ненужно забавяне, но не по-късно от 72 часа от узнаване за настъпване на нарушението (чл. 33, пар.1 от ОРЗД), а ОЛД уведомява своя АЛД без ненужно забавяне от узнаване за настъпване на нарушението (чл. 33, пар.2 от ОРЗД). При съвместни

администратори следва предварително да се определят отговорностите, които всеки от тях има по отношение на спазването на задълженията по чл. 33 от ОРЗД.

2.2. При необходимост АЛД може да предостави допълнителна информация (чл. 33, пар. 4 от ОРЗД), а при забавено уведомление (по-късно от 72 часа) следва задължително да се посочат причините за това.

3. Уведомяване на субектите на данни по чл.34 от ОРЗД.

3.1. При вероятност нарушението на сигурността да породи висок риск за правата и свободите на физическите лица, АЛД следва на ясен и прост език да съобщи на субектите на данните за нарушението, като им предостави информация относно рисковете, възникнали в резултат на нарушението, и стъпките, които могат да предприемат, за да се предпазят от възможните негативни последици от него (чл.34, пар.1 и 2 от ОРЗД).

Важно! АЛД трябва да споделя информация със субектите на данни при нарушение на сигурността, за да могат и самите лица да предприемат допълнителни и адекватни мерки за защита на личните си данни, които да допълнят вече взетите от АЛД технически и организационни мерки за справяне с последиците от нарушението.

3.2. ОРЗД допуска АЛД сам да избере какъв да бъде начина на уведомяване на субектите, като (без да е изчерпателно) напр.: изпращане на имейли, лични контакти, съобщение на сайта на администратора или чрез средствата за масова информация, както и други подходящи начини, съобразно дейността на администратора, но при спазване на принципа на отчетност

3.3. ОРЗД допуска АЛД да не уведоми субектите на данни, ако е налице някое от условията, изрично посочени в чл.34, пар.3 от ОРЗД.

3.4. Когато АЛД не е съобщил на субектите на лични данни за нарушението, ОРЗД предвижда възможността КЗЛД, след като прецени, че е вероятно нарушението на сигурността да породи висок риск за правата и свободите на физическите лица, да изиска от администратора да съобщи за нарушението на субектите. (чл.34, пар.4 от ОРЗД).

4. Съдържание на уведомлението до надзорния орган.

4.1. По отношение съдържанието на уведомлението следва да се спазват изискванията на чл.33, пар.3 от Регламент (ЕС) 2016/679. За допълнителни методически разяснения, препоръчваме да се ползват „Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679” на Работната група по чл. 29, приети на 3 октомври 2017 г., последно преработени и приети на 6 февруари 2018 г.(WP250, rev.01), впоследствие потвърдени от Европейския комитет по защита на данните на 25 май 2018 г. Насоките са публикувани на сайта на КЗЛД [тук](#).

4.2. На сайта на КЗЛД е налична и бланка за уведомление по чл.33 от ОРЗД, която, без да е задължителна, е изготвена с оглед подпомагане на АЛД да се ориентират по-подробно за необходимата информация, която да подадат във връзка с нарушението, както и да се улеснят при изпълнението на това тяхно задължение. Бланката е налична [тук](#).

5. Оценка на риска за правата и свободите на субектите на данни, извършвана от АЛД.

5.1. Риск за правата и свободите на субектите на данни по смисъла на Регламента е съществуването на възможност да се случи събитие, което само по себе си представлява вреда (включително необоснована намеса в правата и свободите на физическите лица) или което може да доведе до допълнителни щети на едно или повече физически лица.

5.2. На първо място АЛД следва да определи естество на нарушението - категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни (чл.33, пар.3, б.„а“ от ОРЗД)

5.3. На следващо място е определянето на риска от възникване на неблагоприятни последици за субектите на данни - физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица (съображение 85 от ОРЗД). Рискът може да се изрази в профилиране, лишаване от права и свободи или от упражняване на контрол върху своите лични данни, както и в нарушени мерки за сигурност при обработка на чувствителни данни, обработка на данни за уязвими категории лица или на голям брой данни и лица.

5.4. Накрая АЛД следва да направи оценка на риска, която има две измерения: тежест на щетите и вероятността да настъпи събитието и произтичащите от това щети.

5.4.1. За определяне на **тежестта** следва да се вземат предвид:

- **Категории засегнати данни** – основни/ профилиращи/ финансови/ чувствителни/ биометрични/ позволяващи кражба на самоличност/ застрашаващи живота на лицето;
- **Възможност за идентификация на субектите** - не е възможна идентификация/ необходими си допълнителни данни или достъп до други системи/ директна идентификация;
- **Засегнатите категории субекти** – граждани/ деца/ лица в неравностойно положение;
- **Брой засегнати субекти на данни**
- **Повторяемост спрямо субекти и данни**

5.4.2. За определяне на **вероятността** да настъпи събитието следва да се вземат предвид:

- **характера на нарушението** - наличие на умисъл/ по непредпазливост/ случайност
- **действия на администратора** - не може да се ограничи въздействието/ при определени действия се ограничава въздействието/ ограничени са последствията.

5.5. След определяне от АЛД на тежестта (по т.5.4.1.) и на вероятността (по т.5.4.2.) се получава **оценката на риска**, която може да бъде:

- **нисък риск**, т.е. няма риск за правата и свободите на субекти на данни, въпреки че е установено нарушение;
- **среден риск** – следва да се уведоми КЗЛД;
- **висок риск** - следва да се уведоми КЗЛД, както и засегнатите субекти на данни.

5.6. На подаденото от АЛД уведомление се извършва анализ съгласно приета от КЗЛД „Методика за определяне нивото на риска при нарушение на сигурността на личните данни“ (Методиката). Методиката е вътрешен документ, подпомагащ работата по обработване на постъпващите в КЗЛД уведомления, приета на основание чл. 62, ал. 2, буква „в“ от Правилника за дейността на КЗЛД и е налична на сайта на комисията [тук](#).

6. Приложими мерки за минимизиране на неблагоприятните въздействия върху правата и свободите на субектите на данни.

6.1. От АЛД следва да се предприемат предварителни технически и организационни мерки за **минимизиране вероятността от настъпване на нарушение** на сигурността на данните – това са отделните аспекти на информационната сигурност, които, например, са заложи в ISO 27 001 - персонална сигурност, управление на активите, управление на достъпа, физическа сигурност, сигурност на комуникациите, криптографска сигурност, оперативна сигурност, управление на инцидентите, управление на доставчиците, управление на непрекъсваемостта на функциониране и поддържане на постоянно съответствие.

6.2. **При настъпване на нарушение на сигурността** на данните техническите и организационни мерки следва да се разделят на:

6.2.1. Действия за минимизиране вредите за субектите на данни **в 72 часовия период от настъпване/узнаване** за нарушението на сигурността на данните

- проверка на вида нарушение - поверителност, цялостност, наличност
- спиране на уязвимостта
- възстановяване на услугата
- уведомяване на засегнатите от нарушението субекти на данни
- препоръки от АЛД за минимизиране вредите за засегнатите от нарушението субекти на данни

6.2.2. Действия за минимизиране вредите за субектите на данни **след 72 часовия период от настъпване/узнаване** за нарушението на сигурността на данните – това са приложимите мерки за минимизиране вероятността от настъпване на нарушение на сигурността на данните (по т.6.1.)от подобен характер без ненужно забавяне.

7. Документиране на нарушенията на сигурността на данните от АЛД/ОЛД- чл. 33, параграф 5 от ОРЗД.

7.1. Администраторът **документира всяко нарушение** на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него. Вътрешното документиране е задължение на АЛД независимо от нивото на рисковете, свързани с нарушението, което е свързано и с принципа на отчетност. Всеки АЛД е длъжен да поддържа документацията в актуален вид и ако надзорният орган поиска да му осигури достъп до тази документация.

7.2. **Процедура за документиране** на нарушенията на сигурността на данните.

Всеки администратор трябва да разполага с разписани планове и процедури за реакция при нарушения на сигурността и да са ясни каналите за докладване и отговорните за това лица. Обучението и запознаването на персонала с тези процедури е от съществено значение, като се обръща специално внимание на най-новите тенденции и примери за кибератаки или други инциденти.

7.3. **Съдържание на регистъра на нарушенията** на сигурността на личните данни.

Този регистър е част от регистрите на дейностите по обработване, които трябва да поддържа АЛД/ОЛД, съгласно чл. 30 от ОРЗД. Не е задължително да има отделен регистър на нарушенията, при условие че информацията е лесно разпознаваема и може да бъде предоставена при поискване.

Ключовите елементи, които следва да бъдат включени в регистъра на нарушенията са всички подробности, свързани с нарушението: причините за нарушението; какво точно се е случило; личните данни, които са били засегнати; последиците от нарушението, както и предприетите действия за справяне с него.

7.4. **Документиране на решенията, взети от АЛД/ОЛД.**

Администраторът трябва да документира своите решения, както и основанията за тяхно взимане, при реагиране на нарушението. Ако за дадено нарушение не се уведомява надзорният орган, следва да се документира и основанията за това решение. По същия начин следва да се документират и основанията, въз основа на които АЛД е приел, че няма вероятност нарушението да породи риск за правата и свободите на лицата, засегнати от нарушението, и които не са били информирани за него, включително и в хипотезата на чл.34, пар.3 от ОРЗД.

7.5. Срок за съхранение на документацията

Регламентът не посочва срок за съхранение на документацията, но следва да се спазва принципа за ограничение на съхранението на личните данни докато това е необходимо.

Всеки АДД/ОЛД следва да има предвид, че неизпълнение на задълженията по чл.33 и чл.34 от ОРЗД във връзка с нарушение на сигурността на данните, може да е основание надзорният орган да упражни всяко от правомощията си по член 58 от ОРЗД - било за разследване (чл.58, пар.1 от ОРЗД), било корективните си правомощия (чл.58, пар.2 от ОРЗД), а така също и/или да наложи административно наказание глоба/имуществена санкция в съответствие с член 83 от Регламента.

КЗЛД ИЗДАДЕ ИНФОРМАЦИОННА БРОШУРА “ШЕНГЕНСКОТО ПРОСТРАНСТВО И ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ”



Усилията за пълноправно членство в Шенген са приоритетна задача с постоянен характер в дейността на КЗЛД. Във връзка с нейното изпълнение на институционалния сайт е предоставена и се поддържа в актуален вид подробна информация относно Шенгенското пространство – правна рамка, права на физическите лица и защита на личните данни във връзка с Шенгенската информационна система, контакти с компетентни органи, отговори на често задавани въпроси и др. Публикувани са и 4 информационни брошури – три на Европейската комисия и една на КЗЛД. Брошурата на КЗЛД е издадена през ноември 2021 г. и е публикувана на сайта – [ТУК](#).

В настоящия брой публикуваме нейното съдържание.

Шенгенското пространство и защитата на данните

Лица, чиито лични данни се събират, съхраняват или обработват по друг начин в Шенгенската информационна система от второ поколение (ШИС II), имат права на информация и достъп, коригиране на неточни данни и заличаване на незаконно съхранявани данни. В настоящата брошура са описани начините за упражняване на тези права.

Какво представлява Шенгенското пространство?

Правната рамка регулираща Шенгенското информационно пространство се урежда с Регламент (ЕС) 1987/2006 и Решение 2007/533/ПВР на Съвета на Европейския съюз.

Шенгенското пространство гарантира свободно движение, без граничен контрол, на граждани на Европейския съюз (ЕС) и на граждани на държави извън ЕС, които легално пребивават на територията на Съюза. Свободното движение на хора дава възможност на всеки гражданин на ЕС да пътува, работи и живее в държава от ЕС, без да спазва специални изисквания.

Държавите, част от Шенгенското информационно пространство, трябва да отговорят на изискванията за осъществяване на ефективен граничен контрол на външните граници, както и да прилагат мерки за сигурност във връзка с премахване на контрола по вътрешните граници.

Към настоящия момент почти всички държави-членки на ЕС, както и Исландия, Норвегия, Швейцария и Лихтенщайн, прилагат изцяло Шенгенското законодателство. България е пълен ползвател на ШИС II, като изцяло прилага достиженията на правото на Шенген. Очаква се политическо решение за присъединяването ѝ *de jure*.

Шенгенска информационна система от второ поколение (ШИС II)

Шенгенската информационна система е създадена, за да помогне за поддържането на вътрешната сигурност в Шенгенското информационно пространство, и е достъпна само за компетентните органи – Министерство на вътрешните работи (МВР); Министерство на външните работи (МВнР); Държавна агенция „Национална сигурност“ (ДАНС) и институциите, натоварени с граничен и митнически контрол; Агенция „Митници“; Държавна Агенция за бежанците и съдебните органи при изпълнение на служебни им задължения в ШИС II. Системата се състои от:

- ✓ централна система (централна ШИС II);
- ✓ национална система (Н.ШИС II) във всяка държава-членка, която се свързва с централната ШИС II;
- ✓ комуникационна инфраструктура между централната система и националните системи, образувайки криптирана виртуална мрежа, предназначена за данни на ШИС II и обмен на данни между органите, отговарящи за обмена на всяка допълнителна информация (бюро СИРЕНЕ). Администратор на Н.ШИС II е Министърът на вътрешните работи, а бюро СИРЕНЕ е част от дирекция „Международно оперативно сътрудничество“ към МВР.

Права на физическите лица в ШИС II

Физическите лица имат право на информация и достъп до своите лични данни в ШИС II, както и да поискат тяхното коригиране или заличаване.

- ✓ Право на информация – дали данните на физическото лице се обработват в системата;
- ✓ Право на поправка или заличаване на данни – личните данни могат да се коригират, когато те са фактически неточни или непълни, и да се поиска тяхното заличаване, ако са били незаконно съхранявани.

Право на достъп на физическото лице може да бъде осъществено: пряко до бюро СИРЕНЕ в ДМОС или непряко чрез Комисията за защита на личните данни.

При съмнение за злоупотреба със самоличност

Фалшиви документи за самоличност или документи за самоличност на друго лице могат да се използват при извършване на престъпления или при опит за влизане или престой в Шенгенското информационно пространство.

След надлежно установяване от компетентните органи със съответния акт за извършено нарушение „кражба на самоличност“, данните за лицето, с чиято самоличност е злоупотребено и с изрично негово съгласие, могат да бъдат добавени към сигнал в ШИС II, само за тази конкретна цел.

Средства за правна защита

Когато искането на физическото лице не е било удовлетворено или то счита, че правата му са нарушени, същото има право да подаде жалба до националния надзорен орган по защита на данните – Комисията за защита на личните данни, или да се обърне към съответния компетентен съд.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



European Data Protection Board



През ноември и декември 2021 г. се състояха две заседания на Европейския комитет по защита на данните (ЕКЗД).

На 19 ноември 2021 г. ЕКЗД прие **Насоки относно взаимодействието между член 3 и глава V от ОРЗД**. В тях се пояснява взаимодействието между териториалния обхват на ОРЗД (член 3) и съдържащите се в глава V разпоредби относно международното предаване на данни, като целта е да се подпомогнат администраторите и обработващите лични данни в ЕС при определянето дали дадена операция по обработване на данни представлява международен трансфер на данни, както и да се осигури общо разбиране на понятието. В насоките се определят три съвкупни критерия, въз основа на които обработването се класифицира като предаване на данни: 1) износителят на данни (администратор или обработващ лични данни) подлежи на разпоредбите на ОРЗД за въпросното обработване на данни; 2) износителят на данни предава или предоставя личните данни на вносителя на данни (друг администратор, съвместен администратор или обработващ лични данни); 3) вносителят на данни се намира в трета страна или е международна организация.

Обработването на данни ще се счита за предаване, независимо дали вносителят, установен в трета държава, вече подлежи на разпоредбите на ОРЗД съгласно член 3 от Регламента. Същевременно, ЕКЗД счита, че събирането на данни директно от субектите на данни в ЕС по собствената им инициатива не представлява предаване на данни.

Във връзка с приемането на насоките, председателят на ЕКЗД Андреа Йелинек поясни: „Тези насоки осигуряват последователно тълкуване на понятието „международно предаване на данни“ и поясняват, че когато даден вносител на данни подлежи на разпоредбите на ОРЗД, задълженията съгласно глава V от ОРЗД се прилагат както за предоставянето на данните от ЕС към вносителя, така и за всеки по-нататъшен трансфер, който се извършва от вносителя“.

Насоките са обект на обществена консултация, която ще продължи до 31 януари 2022 г.

ЕКЗД прие **Изявление относно пакета за цифровите услуги и стратегията за данните, представени от Европейската комисия**. В изявлението се изтъкват три вида общи опасения във връзка с представените дотук предложения на Комисията - Законодателния акт за управление на данните, Законодателния акт за цифровите услуги, Законодателния акт за цифровите пазари и Регламента относно изкуствения интелект:

1. липса на защита на основните права и свободи на лицата;
2. разпокъсан надзор;
3. рискове от несъответствия.

ЕКЗД и ЕНОЗД вече публикуваха **съвместни становища относно Законодателния акт за управление на данните и Регламента относно изкуствения интелект**, а ЕНОЗД публикува **становища относно Европейската стратегия за данните, Законодателния акт за цифровите пазари и Законодателния акт за цифровите услуги**. В изявлението си ЕКЗД отново призовава за пълна забрана на използването на изкуствен интелект за автоматично разпознаване на човешки черти на обществено достъпни места и настоятелно призовава съзаконодателя да обмисли постепенно премахване, водещо до забрана на целевото рекламиране въз основа на повсеместно проследяване, като профилирането на деца следва изобщо да бъде забранено. ЕКЗД подчертава рисковете, свързани с паралелните структури за надзор, и настоятелно препоръчва във всяко предложение да се предвиди изрично правно основание за ефективното сътрудничество и обмяна на информация между съответните компетентни надзорни органи и органите за защита на данните. Комитетът призовава Европейската комисия и съзаконодателя да гарантират, че в предложенията ясно се посочва, че те не засягат и не

подкопават прилагането на съществуващите правила за защита на данните, както и че тези правила имат предимство при обработването на лични данни, включително по отношение на предстоящото предложение за законодателен акт за данните.

На състоялото се през **декември 2021 г.** заседание Комитетът прие **Принос към извършените от Европейската комисия преглед и оценка на Директивата за защита на данните в правоприлагането**. Целта на Директивата е постигане на хармонизирано ниво на защита на данните за лицата в областта на правоприлагането в целия ЕС. Последните четири години се характеризираха предимно с национални процеси за транспониране на директивата. ЕКЗД е на мнение, че е твърде рано да се правят заключения относно нейната ефективност или да се обмисля преразглеждането ѝ, тъй като поради нейното скорошно внедряване е налице ограничен опит и емпирични данни относно някои нейни части. Едновременно с това се призовават държавите-членки, които все още са във фазата на реализиране, да инвестират всички възможни средства, за да гарантират, че транспонирането е напълно в съответствие с Директивата. В своя принос Комитетът потвърждава ангажимента си да продължи да предоставя насоки относно тълкуването на Директивата, както и остава ангажиран с предоставянето на независими оценки на бъдещи проекти на решения за адекватност, изготвени от Европейската комисия, по отношение на изискванията на Директивата, по-специално, свързаните с приложимите права, ефективните средства за правна защита и гаранциите относно последващото предаване на данни. ЕКЗД подчертава, че ефективното изпълнение на задачите в съответствие с Директивата изисква наличието на необходимите ресурси, както човешки, така и технически, и призовава държавите-членки да гарантират, че ресурсите на надзорните органи се увеличават пропорционално на работното им натоварване.

Като част от изпълнението на **Стратегия на ЕКЗД 2021-2023** и след създаването на Експертна група за подкрепа, бе постигнато съгласие по плана на проекта за групата. Нейната цел е да предоставя помощ на членовете на Комитета под формата на експертен опит, необходим за разследванията и дейностите по правоприлагане, както и да засили сътрудничеството и солидарността между членовете на ЕКЗД чрез споделяне, укрепване и допълване на силни страни и посрещане на оперативните нужди.

ЕКЗД прие окончателна версия на **Насоки с примери относно уведомленията за нарушаване на сигурността на данните**. Тези насоки допълват **Насоките на работната група по член 29 относно уведомяването за нарушение на данните**, като въвеждат по-ориентирани към практиката насоки и препоръки. Те имат за цел да помогнат на администраторите на лични данни да решат как да се справят с нарушенията на данните и какви фактори да вземат предвид при оценката на риска. След проведена обществена консултация Насоките бяха актуализирани с оглед отразяване на получените коментари.

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ ПОСТИГНАХА ПРЕДВАРИТЕЛНО СПОРАЗУМЕНИЕ ОТНОСНО АКТА ЗА УПРАВЛЕНИЕ НА ДАННИТЕ

На 30 ноември 2021 г. бе обявено постигането на предварително споразумение на преговарящите от Съвета на ЕС и Европейския парламент относно Акта за управление на данните (АУД). На 25 ноември 2020 г. Европейската комисия предложи нови правила за управление на данните - Регламент относно европейска рамка за управление на данните (Акт за управление на данните). Целта е да се оползотворява пълноценно потенциалът на постоянно нарастващите масиви от данни в основана на доверие европейска рамка, да се улесни споделянето на данни в целия ЕС. Това ще се постигне като се повиши контрола и доверието от страна на гражданите и предприятията по отношение на техните данни чрез изграждане на надеждна среда, за да се улесни използването на наличните данни за научни изследвания и създаването на иновативни нови услуги и продукти.

С Акта за управление на данните ще бъдат създадени стабилни механизми за улесняване на повторното използване на определени категории от защитени данни от публичния сектор, ще

се повиши доверието в посредническите услуги за данни и ще се насърчи алтруизмът на данните в целия ЕС. Той е важен елемент от европейската стратегия за данните, която има за цел да укрепи икономиката, основана на данни, да увеличи богатството и благосъстоянието и да предостави на Европа конкурентно предимство в полза на нейните граждани и предприятия.

Актът за управление на данните ще даде възможност за **по-широка повторната употреба на защитени данни от общественния сектор**. Ще се създаде механизъм, който ще позволи безопасното повторно използване на определени категории данни от общественния сектор, които са обект на правата на други лица. Органите от общественния сектор, позволяващи този вид повторно използване, ще трябва да бъдат подходящо оборудвани от техническа гледна точка, за да гарантират, че неприкосновеността на личния живот и поверителността са напълно запазени. Изключителни договорености за повторно използване на данни от общественния сектор ще бъдат възможни, когато това е обосновано и необходимо за предоставянето на услуга от общ интерес. Според постигнатото предварително споразумение, максималната продължителност за съществуващите договори ще бъде 2,5 години, а за новите договори - 12 месеца. Европейската комисия ще създаде единна европейска точка за достъп с електронен **регистър** на данни от публичния сектор с възможност за търсене. Този регистър ще бъде достъпен чрез единни национални информационни точки.

С АУД се създава рамка за насърчаване на **посреднически услуги за данни**, с която ще се гарантира сигурна среда, където дружествата или физическите лица могат да обменят данни. За дружествата тези услуги могат да бъдат под формата на цифрови платформи, които да подкрепят доброволното споделяне на данни между дружествата или да улесняват спазването на законно установените задължения за обмен на данни. **По отношение на личните данни** тези услуги и техните доставчици ще помогнат на физическите лица да упражняват правата си съгласно Общия регламент за защита на данните (ОРЗД). Това ще даде възможност на хората да упражняват пълен контрол върху данните си и ще им позволи да ги споделят с дружества, на които имат доверие. Доставчиците на посреднически услуги за данни ще трябва да бъдат вписани в **регистър**, така че клиентите им да знаят, че могат да разчитат на тях.

Чрез АУД също така се улесняват физическите лица и дружествата да **предоставят доброволно данни в името на общественния интерес**, като например за целите на научноизследователски проекти в областта на медицината. В Акта са предвидени мерки за създаване на необходимото доверие и насърчаване на физическите лица и дружествата да „даряват“ данни на организации за алтруизъм по отношение на данните, така че данните да могат да се използват за по-широко обществено благо.

Предвидено е доброволно сертифициране, което ще улесни идентифицирането на отговарящи на изискванията **доставчици на посреднически услуги за данни и организации за алтруизъм по отношение на данните**.

С АУД се създават **гаранции** за данните от общественния сектор, посредническите услуги за данни и организациите за алтруистично споделяне на данни срещу незаконно международно прехвърляне или правителствен достъп до нелични данни. **По отношение на личните данни** ЕС вече разполага с подобни гаранции съгласно ОРЗД. **По отношение на неличните данни** чрез вторично законодателство Европейската комисия може да приема решения относно адекватното ниво на защита, в които се посочва, че конкретни държави извън ЕС предоставят подходящи гаранции за използването на нелични данни, предавани от ЕС. Тези решения ще бъдат подобни на решенията относно адекватното ниво на защита, свързани с личните данни съгласно ОРЗД. Комисията може също така да приема образци на договорни клаузи в подкрепа на органите от публичния сектор и повторните ползватели в случай на прехвърляне на данни от публичния сектор на трети държави.

Според предварителното споразумение, новите правила ще станат приложими 15 месеца след влизането в сила на регламента.

Приетото на 30 ноември 2021 г. предварително споразумение **подлежи на одобрение от Съвета на ЕС**.

ЕВРОПЕЙСКАТА КОМИСИЯ ПРИЕМА МЕРКИ В ПОЛЗА НА КИБЕРСИГУРНОСТТА НА БЕЗЖИЧНИТЕ УСТРОЙСТВА И ПРОДУКТИ



Безжичните устройства присъстват трайно в ежедневието на хората. Пандемията от COVID-19 допринесе за все по-честото им използване за професионални или лични цели, а ежедневно използване на мобилни устройства с безжична връзка към интернет създава реални киберзаплахи за потребителите. Тези устройства имат достъп до лична информация и функционират в комуникационните мрежи. Във връзка с това, в края на октомври 2021 г. Европейската комисия прие делегиран акт въз основа на [Директивата за радиосъоръженията](#), който има за цел всички устройства с безжичен достъп до интернет да се утвърждават като безопасни преди да бъдат предлагани на пазара на ЕС.

С този акт се установяват нови правни изисквания за мерките в областта на киберсигурността, с които производителите ще трябва да се съобразяват при проектирането и производството на съответните продукти.

Според Тиери Бретон, комисар по въпросите на вътрешния пазар „Киберзаплахите стават все по-разнообразни, сложни и изменчиви. С изискванията, които въвеждаме днес, ще подобрим значително сигурността на широк набор от продукти и ще подсилим своята устойчивост на киберзаплахи. Мерките са в хармония и с амбициозните цели, които си поставя Европа в областта на цифровите технологии. Става дума за важна крачка към създаването на всеобхватен набор от общи европейски стандарти за киберсигурност за продуктите (включително свързаните с интернет продукти) и услугите, предлагани на нашия пазар.“

В прессъобщение във връзка с приетия акт се заявява, че новите мерки ще спомогнат за:

- **подобряване устойчивостта на мрежата:** безжичните устройства и продукти ще трябва да разполагат с характеристики, които им позволяват да избягват опасните комуникационни мрежи и да възпрепятстват използването на устройствата за нарушаване работата на уебсайтове или на други услуги.

- **подобрена поверителност за потребителите:** безжичните устройства и продукти ще трябва да разполагат с характеристики, които гарантират защитата на личните данни. Например производителите ще трябва да въведат допълнителни мерки за предотвратяване на неразрешения достъп или предаването на лични данни. Съществен елемент от акта е защитата на правата на децата.

- **намаляване на риска от парични измами:** безжичните устройства и продукти ще трябва да разполагат с характеристики, които да спомагат за свеждане до минимум на риска от измами при електронните разплащания. Например те ще трябва да гарантират по-строг контрол при идентификацията на потребителя, за да се избегнат мошенически плащания.

Ако Съветът и Парламентът не представят възражения, делегираният акт ще влезе в сила след двумесечен период за контрол.

След неговото влизане в сила производителите ще разполагат с преходен период от 30 месеца, преди да започнат да спазват новите правни изисквания. Това ще осигури достатъчно време на отрасъла, за да адаптира съответните продукти, преди новите изисквания да започнат да се прилагат, което се очаква да стане в средата на 2024. Европейската комисия ще поиска от европейските организации за стандартизация да разработят адекватни стандарти. Като алтернатива производителите ще могат също така да доказват съответствието на своите продукти, като ги подлагат на оценка от компетентни нотифицирани органи.

СЪСТОЯ СЕ 43-ТОТО ИЗДАНИЕ НА ГЛОБАЛНАТА АСАМБЛЕЯ ПО ВЪПРОСИТЕ НА НЕПРИКОСНОВЕНОСТТА



GPA

Global Privacy Assembly

В края на октомври 2021 г. Мексиканският национален институт по прозрачност, достъп до информация и защита на личните данни (INAI) бе домакин на 43-тото издание на Глобалната асамблея по въпросите за неприкосновеността - най-значимият световен форум за обмяна на знания, опит и идеи в сферата на защитата на личните данни и неприкосновеността на личния живот.

Форумът се състои за първи път през 1979 г. под името Международна конференция на комисарите по защита на данните и поверителността. Повече от четири десетилетия тя функционира като платформа за среща на лидерите в областта на защитата на личните данни. Това се постига посредством обединените усилия на организации от 6 континента – общо сто и десет акредитирани членове и шестнадесет наблюдатели.

Глобалната асамблея по въпросите за неприкосновеността е световен форум, на който независими регулатори за поверителност, защита на данните и свобода на информацията приемат резолюции и препоръки на високо ниво, адресирани до правителства и международни организации. Асамблеята е ежегодно събитие, включващо закрыта сесия за акредитирани членове и наблюдатели, и отворена сесия за всички регистрирани участници. В работа на Конференцията вземат участие делегати от цял свят – органи за защита на личните данни, правителствени и неправителствени организации, представители на академичните среди и бизнеса.

Тази година, предвид неприсъственото осъществяване на събитието, беше организирано предварително гласуване за приемане на отчетните документи на 11-те работни групи към Глобалната асамблея по въпросите на неприкосновеността.

На 43-тото издание на Глобалната асамблея по въпросите за неприкосновеността бяха приети:

- Резолюция за стратегическото развитие на Асамблеята за периода 2021 – 2023 г.;
- Резолюция относно споделянето на данни за обществени цели;
- Резолюция за цифровите права на децата;
- Резолюция относно достъпа на държавни органи до данни, неприкосновеността на личния живот и върховенството на закона
- Резолюция за бъдещето развитие на Асамблеята и нейния Секретариат.

С приетата **Резолюция за стратегическото развитие на Асамблеята за периода 2021 г. – 2023 г.** бе одобрен Стратегическият план на Асамблеята за този период, чието изпълнение започва незабавно. Чрез резолюцията се възлага на Изпълнителния комитет на форума да оцени досегашните стратегически цели на Асамблеята и да подготви изменения в тяхното съдържание, заедно с план за постигането им. Стратегическият план за 2021г. - 2023г. продължава да се фокусира върху трите стълба на съвместната работа, подчертани в предходния план, които представляват основополагащи предизвикателства пред всички членове на Асамблеята. Трите стълба са:

- Глобална рамка и стандарти;
- Сътрудничество по правоприлагането;
- Области на фокусирани политики.

На база на трите стълба са изведени следните 3 стратегически приоритета:

- Подобряване на неприкосновеността на световно ниво в ерата на ускорената дигитализация.
- Засилване на „гласа“ и влиянието на Глобалната асамблея.
- Изграждане на капацитет за GPA и неговите членове.

В Резолюцията се изразява стремеж за постигане на стратегическите цели чрез фокусиране върху основополагащи въпроси, които допълват и укрепват регулаторното сътрудничество между членовете на Глобалната асамблея по въпросите на неприкосновеността.

С приетата **Резолюция относно споделянето на данни за обществени цели** се признава необходимостта от продължаване и разширяване на дейността на досегашната Работна група за COVID-19 и се разширява мандата ѝ във връзка със защитата на личните данни и неприкосновеността, в контекста на опасенията, свързани със споделянето на данни. Документът отчита съвременното развитие за изместване на фокуса от реакцията на глобалната пандемия към икономическо възстановяване. С оглед институционализиране на усилията за споделяне на данни за обществени цели се създава нарочна работна група, която ще продължи работата, като:

- Съсредоточава усилия върху идентифицирането на практически и прагматични подходи за това как личните данни могат да бъдат споделяни и използвани, за да се даде възможност за иновации и растеж. Същевременно се защитават индивидуалните права и се насърчава общественото доверие чрез прилагането на принципи и най-добри практики относно ключови компоненти на споделянето на данни за обществени цели;

- Засилено си сътрудничи със съответните заинтересовани страни, международни мрежи, организации на гражданското общество и защитници на неприкосновеността на личния живот. Нейните усилия са насочени към укрепване на капацитета на членовете и наблюдателите на Глобалната асамблея за справяне с възникващи предизвикателства, свързани със споделянето на данни;

- Разработва проактивни отговори на възникващите предизвикателства пред защитата на данните и неприкосновеността на личния живот, свързани със споделянето на лични данни, например за здравни паспорти, наблюдение на здравето на пристигащи пътници и завръщащи се граждани, мерки за проследяване на контакти, обработване на данни на деца или ученици в контекста на технологиите за електронно обучение;

- Осъществява консултации с референтния панел относно нововъзникващите политически идеи на Асамблеята (GPA Reference Panel on emerging policy ideas), с оглед обмислянето на бъдещи подходи за споделяне на данни;

- Докладва за напредъка в дейността на работната група в закритата сесия на Глобалната асамблея през 2022 г.

С приетата **Резолюция за цифровите права на децата** се препоръчва на всички заинтересовани страни в областта на защитата на правата на децата в цифровата среда да вземат предвид:

- Упражняването на права и информираност на децата в дигиталната среда;
- Защитата на основните свободи на децата по отношение на обработването на личните им данни;
- Защитата на децата срещу търговската експлоатация на техните данни;
- Правата на децата в разработването на регулации и дизайн на услугите, които ги засягат;
- Участието на носителите на родителски права и дигиталното образование.

С приетата **Резолюция относно достъпа на държавни органи до данни, неприкосновеността на личния живот и върховенството на закона** се застъпва прилагането на конкретни принципи за достъп на държавните органи за целите на националната сигурност и обществената безопасност до лични данни, съхранявани от частния сектор. Чрез посочените по-долу принципи се установяват условия, гарантиращи, че всякакъв вид легитимен достъп на публичните органи за цели, свързани с националната сигурност или обществената безопасност, се осъществяват при зачитането на неприкосновеността на личния живот и върховенството на закона:

- **Наличие на правно основание:** правителственият достъп до лични данни трябва да бъде надлежно уреден в законодателството, прието след публичен дебат и контрол от страна на законодателите. Законодателството трябва да зачита правата на защита на личните данни и на неприкосновеността на личния живот, другите човешки права и да бъде не дискриминационно.

- **Ясно и точно законодателство, приложимо за правителствен достъп:** всяка норма, разрешаваща достъп до лична информация, трябва да бъде: а) публично достъпна, б) написани на ясен, лесно разбираем език, и, в) точна и конкретна по отношение на обхвата на личната информация, за която законът предоставя правителствен достъп, както и условията за такъв достъп.

- **Общ принцип на необходимост и пропорционалност:** за да бъде оправдан достъпът до лични данни, включително специални категории данни от държавни органи. Специфичното използване на лична информация трябва да бъде свързано с очевидно необходима функция или дейност на правителството, а натрапчивостта трябва да е пропорционална на въпросната цел.

- **Прозрачност:** правителственият достъп, произтичащ от законова норма, трябва да изисква проактивно, публично отчитане и публично достъпни изисквания за процеса на отчетност за участващите правителствени агенции и да позволява предоставянето на информация на засегнатите лица, освен ако не съществуват ограничения за прозрачността спрямо хората представлява необходима и пропорционална мярка в едно демократично общество.

- **Права на субектите на данни:** като се вземат предвид изискванията на националната сигурност и обществена безопасност, достъпът на правителството до лични данни следва да интегрира специфична рамка за упражняването на правата на субектите на данни, включително чрез директно отправяне на исканията им до публичните органи. По-специално, лицата трябва да имат право на достъп, да коригират или изтриват своите лични данни, освен ако ограниченията на правата на субекта на данни представляват необходима и пропорционална мярка в едно демократично общество.

- **Независим надзор:** законите, разрешаващи достъп, трябва да предоставят, както независим предварителен надзор (напр. предварително съдебно разрешение), така и на ретроспективен преглед (напр. одит на обработването от независим регулаторен орган), като се вземат предвид тежестта и сериозността на въздействието върху основните права и свободи на физическите лица при осъществяване на правителствен достъп.

- **Законови ограничения за използването на придобитите данни от страна на правителството:** законът, разрешаващ достъп на правителството до лични данни за една конкретна цел, трябва да регулира и ограничава всяко повторно използване или по-нататъшно предаване на данни за други цели.

- **Ефективни средства за правна защита и обезщетение за засегнатите лица:** всеки правителствен достъп до лични данни следва да бъде предмет на специфични разпоредби, за да могат всички засегнати лица да търсят ефективно обезщетение и средства за защита

В допълнение към принципите по-горе, Глобалната асамблея по въпросите на неприкосновеността разглежда следните примери и най-добри практики като уместни илюстрации на по-нататъшна отчетност при достъпа на правителството до лични данни и реализирането на ключови предпазни мерки, гарантиращи защитата на неприкосновеността на личния живот и личните данни на физическите лица:

- Гарантиране, че криптографските системи не са компрометирани чрез правителствени изисквания за достъп, които биха могли да доведат до изключителен достъп чрез съзнателно въвеждане на уязвимости в киберсигурността (например mandated 'backdoors');

- Прозрачност от страна на търговските дружества чрез отчитане/документиране на правителствените искания за достъп;

- Допълнителни средства за правна защита и обезщетение от частния сектор във връзка с достъпа на правителството до лични данни, за да се подкрепи и улесни прилагането на принципа на ефективни средства за правна защита и обезщетение;

- Международно регулаторно сътрудничество относно достъпа на правителствата до лични данни.

Глобалната асамблея за поверителност призовава правителствата и международните организации да работят за разработването на многостранни инструменти, гарантиращи спазването на ключовите принципи за защита на данните и неприкосновеност на личния живот във връзка с правителствения достъп до лични данни. В допълнение, Асамблеята приканва правителствата и международните организации да участват в дискусии, насочени към регулиране на продажбата и използването на технологии, позволяващи особено натрапчив и непропорционален достъп до лични данни, по-специално по отношение на електронно комуникационно съдържание и данни.

Приета бе и **Резолюция за бъдещето развитие на Асамблеята и нейния Секретариат.**

ЗАСЕДАНИЕ НА КОНСУЛТАТИВНИЯ КОМИТЕТ НА КОНВЕНЦИЯ 108 НА СЪВЕТА НА ЕВРОПА

През ноември 2021 г. дистанционно се проведе 42-то пленарно заседание на Консултативния комитет на Конвенция 108 на Съвета на Европа за защита на лицата при автоматизираната обработка на личните данни

Конвенцията за защита на лицата при автоматизираната обработка на лични данни, известна като Конвенция 108 е приета през 1981 от Съвета на Европа. Тя е първият правно обвързващ международен акт, приет в областта на защитата на личните данни. България е ратифицирала Конвенцията на 18 септември 2002 г.

След 7 години интензивна работа и преговори, на 18 май 2018 г., на 128-ото Заседание на Комитета на министрите на Съвета на Европа в Елсинор, Дания, бе приет Протокола (CETS № 223) за изменение на Конвенция 108 (ETS № 108). Модернизирането на Конвенция 108 отговаря на предизвикателствата пред неприкосновеността, които са резултат от развитието на новите информационни и комуникационни технологии и изграждането на цифровото общество. Модернизираната конвенция осигурява силна правна рамка против злоупотребите, които са един от основните проблеми на съвременното общество. Засилва се механизмът за гарантиране на ефективното прилагане на Конвенцията. Протоколът за изменение на Конвенция 108 е израз на постигнатия широк консенсус за изменение на Конвенцията в следните аспекти: запазване на общия и технологически неутралния характер на разпоредбите на Конвенцията; запазване на единството и съвместимостта на Конвенцията с други правни инструменти; препотвърждаване на отворения характер на Конвенцията, чрез който тя има уникален потенциал да бъде универсален стандарт за защита. С разпоредбите на Протокола се въвежда принципът на пропорционалност на намесата, а именно преследването на правомерна цел и постигането на справедлив баланс на интересите - публични и частни, а също така и на засегнатите права и свободи.

При приемането на Протокола за изменение на Конвенция 108 бе подчертано значението на бързото присъединяване на максимален брой страни, за да се улесни формирането на всеобхватен правен режим за защита на данните в рамките на модернизираната Конвенция.

Държавите-членки и другите страни по Конвенцията бяха призовани за незабавно започване на процеса съгласно националното им законодателство, водещо до неговото ратифициране, одобряване или приемане. Протоколът е открит за подписване на 10 октомври 2018 г., когато на специална церемония в сградата на Съвета на Европа в Страсбург протоколът е подписан от 20 страни членки на Съвета на Европа (Австрия, Белгия, България, Чешката република, Естония, Финландия, Франция, Германия, Ирландия, Латвия, Литва, Люксембург, Монако, Нидерландия, Норвегия, Португалия, Русия, Испания, Швеция и Обединеното кралство), както и от Уругвай. При условие за последваща ратификация, с декларация за временното му прилагане до влизането му в сила, от името на България Протоколът е подписан от българският постоянен представител към Съвета на Европа посланик Катя Тодорова. **На 11 септември 2019 г. Народното събрание ратифицира** със закон Протокола за изменение на Конвенцията за защита на лицата при автоматизирана обработка на лични данни. Разпоредбите на Протокола са в съответствие с Конституцията, с българското законодателство, с международните задължения на Република България и с правото на Европейския съюз и не изискват мерки от законодателен характер с оглед на тяхното прилагане.

Протоколът укрепва ролята на Комитета по Конвенцията, който изработва и приема документи, свързани с неговото приложно поле. **В рамките на проведеното през ноември 2021 г. заседание** на Комитета бе предоставена информация относно процеса по подписване и ратифициране на Протокола за изменение на Конвенция 108. Към момента общо 43 страни са подписали протокола и 15 страни са го ратифицирали. Италия и Уругвай са ратифицирали протокола съответно през м. юли и август 2021 г., а Германия и Северна Македония през октомври 2021 г.

Финализирани бяха документите, свързани с:

- Насоките за обработване на лични данни за целите на политическите кампании. Бяха приети направените предложения по документа от страна на Комисията за защита на личните данни;
- Механизма за оценка и последващи действия съгласно Конвенция 108+. Същите ще бъдат публикувани на институционалната страница на Съвета на Европа.

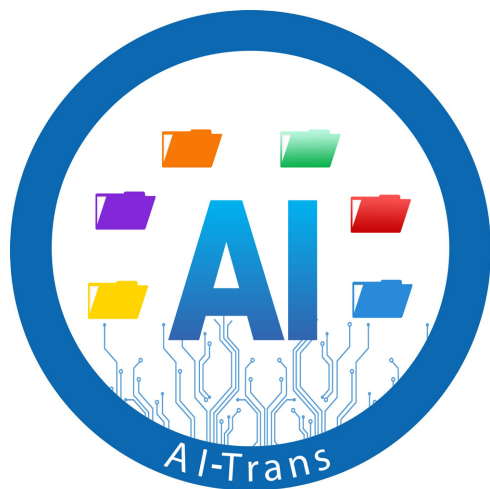
Продължава работата по следните документи, за които се приемат предложения до началото на декември 2021:

- Насоки, свързани с цифровата идентичност и защитата на данните;
- Доклад относно последиците за защитата на данните на механизмите за междудържавен обмен на данни за борба с изпирането на пари/ противодействие на финансирането на тероризма и данъчни цели;
- Доклад за необходимостта от насоки по член 11 от модернизираната Конвенция 108.

Обобщено бе сътрудничеството с Комитета по Конвенцията относно манипулирането на спортни състезания по отношение на въпроси, които не са свързани с материалното наказателно право и съдебното сътрудничество по наказателноправни въпроси (Конвенция „Маколин“); Управителния комитет за правата на детето (CDENF); Специалната комисия по изкуствен интелект (CAHAИ); Комисията по биоетика (DH-BIO); Управителния комитет по медии и информационно общество (CDMSI).

Протоколът за изменение на Конвенция 108 ще влезе в сила след като бъде ратифициран от всички държави страни по Конвенцията. Модернизираната конвенция ще продължи да бъде отворена за присъединяване за всяка държава в света като единствен по рода си световен стандарт в защитата на личните данни.

УСПЕШНО ЗАВЪРШИ ИЗПЪЛНЕНИЕТО НА ПРОЕКТ AI-TRANS, ФИНАНСИРАН ОТ ЕС



На 30 ноември 2021 г. приключи изпълнението на Европейския проект с название „AI-Trans: Increasing AI Transparency Through Digital Alternative Learning of Privacy Training”, финансиран чрез програмата „Еразъм+“. Той бе наднационално усилие, обединяващо експертни екипи от България, Италия, Полша и Молдова. В проектния консорциум бяха включени университети и неправителствени организации.

Проектът се явява продължение на успешно реализирания „e-OpenSpace – Европейска иновативна отворена платформа за електронен обмен на информация и устойчиво предоставяне на образование за възрастни в сферата на защитата на неприкосновеността и личните данни“. Проектната инициатива е поредният проект на Комисията за защита на личните данни, който тя се нагърбва с нелеката задача на координатор – водещ

партньор, обединяващ усилията на всички членове на проектния консорциум. Чрез тези последователни действия, Комисията не само изпълнява Политиката на партньорство от Стратегията на Комисия за защита на личните данни за развитие в областта на защитата на личните данни (Хоризонт 2022), но се нарежда сред българските държавни институции, които координират дейностите по наднационални проекти, чрез разгръщане на широка мрежа от партньорства на КЗЛД сред чуждестранни организации. Продължава изграждането на административен капацитет в институцията, което способства за последващите резултати в управлението на международни проекти.

В края на март 2019 г. КЗЛД кандидатства с проектно предложение по програмата „Еразъм+“. Предложението е одобрено и предложено за финансиране. Договорът за безвъзмездна помощ е подписан в края на месец септември 2019 г. Проектът обединява усилията на Комисията за защита на личните данни, като координатор, с тези на Софийския университет, Фондация ЛИБРе и италианската неправителствена организация GVMAS, Университета в Лодз, Полша, както и молдовската асоциация за изследване на неприкосновеността.

Целта на проектния консорциум бе да създаде иновативно обучително съдържание въз основа на вече създадено устойчиво и дългосрочно стратегическо партньорство между национални надзорни органи, академични среди и организации на гражданското общество. Проектът осигурява знания и развитие на уменията, свързани с поверителността и защитата на личните данни във връзка с новите технологии, и по-специално, с изкуствения интелект (AI) и интернет на свързаните устройства (IoT).

AI-Trans е междусекторен проект, насочен към хоризонтална политика на защитата на личните данни. Изкуственият интелект, интернет на свързаните устройства, „умните“ домашните приспособления не са научна фантастика, те присъстват в ежедневието не само у дома, но и на работното място. За тяхното управление и използване се изискват нови умения, способности и знания. Обща цел на AI-Trans е насърчаване на иновативното образование и информираност в областта на съвременните високотехнологични предизвикателства чрез обучение за защита на личните данни и неприкосновеността на личния живот. Конкретните цели на проекта са:

- Подпомагане на устойчивото стратегическо партньорство между органите за защита на данните, академичните среди и неправителствения сектор в ЕС в областта на AI и IoT чрез обучение за защита на данните и разяснения за защитата на неприкосновеността на личния живот;

- Разработване на удобно за потребителите иновативно съдържание за обучение в областта на AI и IoT чрез обучение за защита на данните и разяснения за защитата на неприкосновеността на личния живот.

По време на изпълнението на проекта бяха проведени 2 международни координационни срещи на проектния консорциум.



Домакин на първата среща беше Комисията на защита на личните данни през ноември 2019 г.

Следвайки въведените противоепидемични мерки, втората международна среща бе организирана дистанционно на 29 ноември 2021 г.

При същите условия, седмица по-рано – в периода 22-26 ноември 2021 г. се проведе краткосрочното обучение за персонал на партньорите по проект „AI-Trans”. По покана на водещия партньор по проекта – Комисията за защита на личните данни, взеха участие представители на всички партньори на проектното начинание.

В самия края на проектното изпълнение бяха реализирани 5 национални събития за разпространение на резултатите по проект „AI-Trans“. В тях взеха участие повече от 200 души. Гостите на тези събития бяха запознати с разработените по проекта интелектуални продукти. Всички те са достъпни чрез обучителната платформа e-OpenSpace. Нейните функционалност и съдържание създават непосредствена възможност за организиране на неформални цифрови обучения в областта на защита на личните данни, като платформата е достъпна на интернет адрес <http://eopen.cdpd.bg/>.

Проект „AI-Trans: Increasing AI Transparency Through Digital Alternative Learning of Privacy Training” по Ключова дейност 2: „Стратегически партньорства по програма „Еразъм+” и номер на договора 2019-1-BG01-KA204-062588 се изпълнява с общите усилия на Комисията за защита на личните данни (координатор на проекта), Софийския университет и Университета в Лодз, Полша, както и неправителствените организации GVMAS - Италия, ЛИБРе - България и Асоциация за изследване на неприкосновеността – Молдова. Проектен ръководител бе Венцислав Караджов, председател на КЗЛД и заместник-председател на Европейския комитет по защита на данните. Проектът AI-Trans бе с продължителност 26 месеца и стойността му е 226 197,61 лв. (115 653 евро).

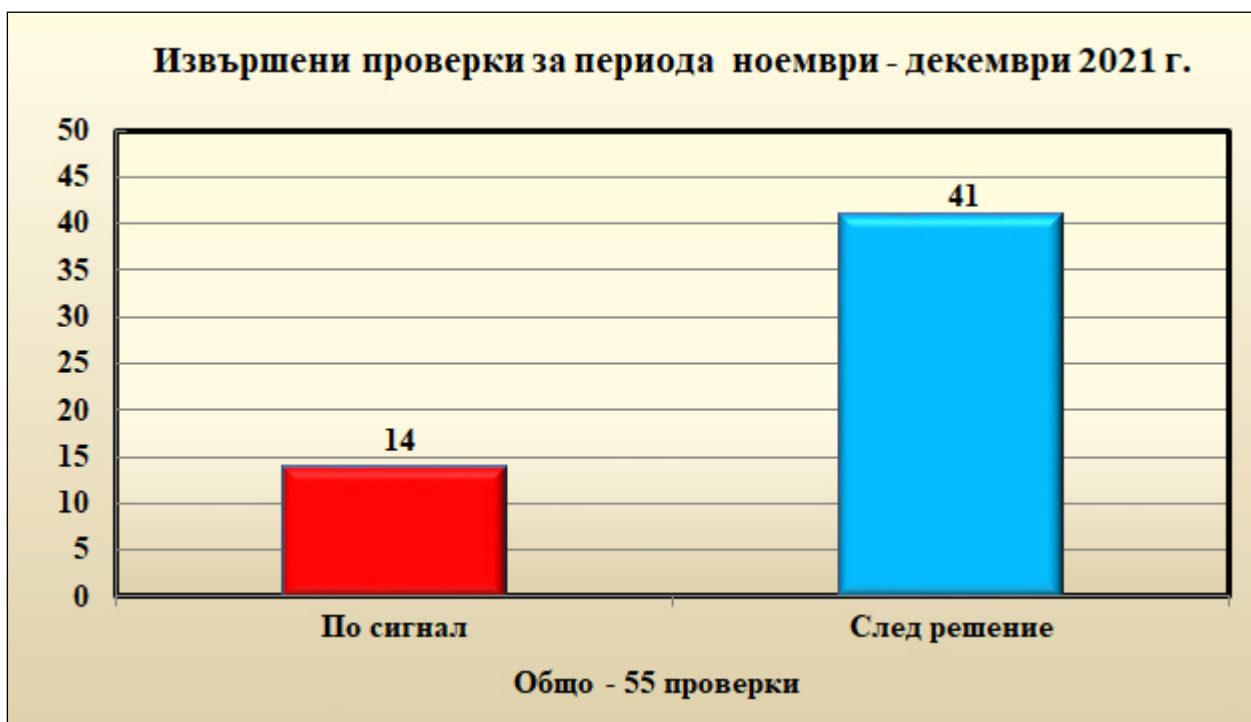


Съфинансиран от програма
„Еразъм+”
на Европейския съюз

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА НОЕМВРИ - ДЕКЕМВРИ 2021 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета през месеците ноември и декември 2021 г. са извършени общо 55 проверки – 14 след постъпили в КЗЛД сигнали и 41 след решение на КЗЛД.



Разгледани са 66 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

Във връзка с констатации, че с определени операции по обработване на лични данни са нарушени разпоредби на регламента, за отчетния период КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са съставени 2 Акта за установяване на административно нарушение, издадени са 8 Разпореждания и е отправено 1 Официално предупреждение.

РЕШЕНИЯ ПО ЖАЛБИ

КЗЛД публикува в своя бюлетин и на институционалния си сайт решения по жалби, с цел да се осигури прозрачност за обществеността относно практиката на Комисията при разглеждането на жалби на граждани. За постигането на тази цел не е необходимо публикуване на всички решения на КЗЛД по жалби, а отразяване произнасянето на Комисията по различни казуси. Всички публикувани решения на КЗЛД са с анонимизирани лични данни на физическите лица и голяма част от имената на юридическите лица.

РЕШЕНИЕ № ППН-01-342/2020 г. София, 21.12.2021 г.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав, председател, Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на редовно заседание, проведено на 13.10.2021 г. и обективизирано в протокол № 42/13.10.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни (ЗЗЛД) във вр. с чл. 57, § 1, б. „е“ от Регламент (ЕС) 2016/679, разгледа по същество жалба с рег. № ППН-01-342/20.04.2021 г., подадена от Й.М. срещу Столична община.

В жалбата Й.М. е посочила, че е подала сигнал в Столична община, през Контактния център за гражданите, като сигналът, който подала е препратен от Столична община на трето лице, без нейно съгласие, в нарушение на правата ѝ по ЗЗЛД.

В условията на залегалото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомена Столична община. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становища с относими доказателства по предявените в жалбата твърдения.

От общината е постъпило становище с рег. № ППН-01-290#4/21.06.2021 г., в което е описано, че сигналът, подаден от г-жа Й.М. с № СОА21-КЦ01-10146/24.02.2021 г. е насочен съгласно „Вътрешните правила за организацията на работа и задълженията на служителите в отдел „Контактен център на Столична община“ на дирекция ”Административно обслужване“ към направление „Обществено строителство“ за процедиране по компетентност. След разглеждане на сигнала и във връзка със сключен договор между Столична община и ДЗЗД с рег.№ *** с предмет „Осъществяване на инвеститорски контрол по изпълнението на обет СМР за отводняване на пътното платно по ул.“Шумако” от ул.“Св. Мария Магдалина“ до ЧОУ „Дрита”, кв.“Симеоново”, направление „Обществено строителство”, като сигнала е изпратен до ДЗЗД, тъй като в рамките на гаранционния срок на обекта консултантът има задължение за извършване на периодичен оглед на обекта след неговото приемане, с цел своевременно документиране и отстраняване на евентуално появили се дефекти в гаранционния срок. Сигналът на г-жа Й.М. е следвало да бъде изпратен до дружеството със заличени лични данни, но служителят, към който е разпределена преписката за процедиране поради натовареността на администрацията и по невнимание допуска грешка и същият е изпратен без да са обезличени личните данни. В случая данните са изпратени на лице, с което Столична община има сключен договор да осъществява контрол върху строителната дейност, по повод на която е сигналът.

За да упражни правомощията си, Комисията следва да бъде валидно сезирана.

Разглежданата жалба съдържа задължително изискуемите реквизити, посочени в разпоредбата на чл. 30, ал. 1 от Правилника за дейността на Комисията за защита на личните данни и на нейната

администрация (ПДКЗЛДНА), а именно: налице са данни за жалбоподателя, естеството на искането, дата и подпис, с оглед което същата е редовна.

Съгласно чл. 38, ал. 1 от Закона за защита на личните данни (ЗЗЛД) при нарушаване на правата му по Регламент 2016/679 и ЗЗЛД всеки субект на данни има право да сезира Комисията за защита на личните данни в срок 6 месеца от узнаване на нарушението, но не по-късно от две години от извършването му.

В чл. 27, ал. 2 от АПК законодателят обвързва преценката за допустимостта на искането с наличие на посочените в текста изисквания. т. 6 на посочената разпоредба препраща към процесуални предпоставки, посочени в други нормативни актове. Съгласно чл. 57, пар. 1, 6. „е“ от Регламент 2016/679 във връзка с уточнението, направено в съображение 122 към Регламента, при сезирането и, Комисията разглежда жалби, подадени от субекти на данни срещу администратор или обработващ лични данни, публичен орган или частна структура, действаща в обществен интерес.

На заседание на Комисията, проведено на 14.07.2021 г., жалбата е обявена за процесуално допустима, а като страни в производството са конституирани: жалбоподател Й.М. и ответна страна Столична община, посочено като пасивно легитимирана страна от жалбоподателя. На страните е указано разпределянето на доказателствената тежест. Уведомени са за разглеждането на жалбата по същество.

Комисията за защита на личните данни е независим държавен орган, който осъществява защита на лицата при обработването на личните им данни и при осъществяване на достъпа до тези данни, както и контрол по спазването на Регламент 2016/679 и Закона за защита на личните данни.

Предмет на жалбата е неправомерно предоставяне на лични данни в обем три имена, телефонен номер, имейл адрес и адрес на жалбоподателката от Столична община на трето лице.

По административната преписка не е спорно, че г-жа Й.М. е подала сигнал за некачествен ремонт на ул. „Шумако“, ж.к. Симеоново до Столична община чрез контактен център, заведен с рег. № СОА21-КЦ01-10146/24.02.2021 г. Не е спорно, че Столична община е изпратила сигнала на ДЗЗД с писмо изх. № СОА21-ТД26-3004 на 11.03.2021 г.

Разгледана по същество жалбата е основателна.

Понятието „лични данни“, което фигурира в тези разпоредби, включва, съгласно определението в член 4, § 1 от Регламент (ЕС) 679/2016 „всяка информация, свързана с идентифицирано или подлежащо на идентификация лице“. За подлежащо на идентифициране лице се смята „лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор, идентификационен номер или чрез един или повече специфични признаци, отнасящи се до неговата физическа, физиологична идентичност“.

По административната преписка не е спорно, че личните данни на жалбоподателката, в обем: три имена, електронен адрес, телефонен номер и постоянен адрес, са изпратени с писмо от Столична община на ДЗЗД, без да е направено необходимото заличаване на данните на жалбоподателката. Не е спорно, че от общината е сключен договор № СОРД55-709 от 05.11.2014 г., с предмет „Осъществяване на инвеститорски контрол по изпълнението на обект СМП за отводняване на пътното платно по ул. „Шумако“ от ул. „Св. Мария Магдалена“ до ЧОУ „Дрита“, кв. „Симеоново“. Не е спорно, че от Столична община е изработена „Инструкция за работа на служителите на Столична община при обработка на документи, получени чрез Контактния център“. Столична община не отрича допуснатата техническа грешка, предвид натовареност на служителите от общината. Въпреки сключени между общината и ДЗЗД договор, не е налице основание за предоставяне на данните на жалбоподателката на последното. Безспорно е, че от Столична община при установяване на нарушението са сигнализирали ДЗЗД, следствие на което е налице декларация за унищожаване на данните на жалбоподателката, която съдържа в себе си и изявление, че данните не са предоставени на трети лица.

С оглед разпределяне на доказателствената тежест в процеса и събраните по преписка доказателства се налага изводът, че личните данни на г-жа Й.М. са обработени в нарушение на принципа за свеждане на данните до минимум, разписан в разпоредбата на чл. 5, §1, б. „в“ от Регламент (ЕС) 2016/679.

Предвид характера и вида на нарушението, обстоятелството, че от Столична община са предприели последващи действия и факта, че са налице правила за обработване лични данни при постъпване по електронен път, Комисията счита, че е целесъобразно да бъде отправено официално предупреждение до администратора по смисъла на чл. 58 §2, б. „б“ от Регламента.

Комисията действа в условията на оперативна самостоятелност като преценява кое от своите правомощия да реализира. Преценката се основава на съображенията за целенасоченост, целесъобразност и ефективност на решението, като следва да се постанови акт, който в най-пълна степен да защитава обществен интерес. Правомощието относно прилагане на подходяща корективна мярка по отношение на администратора на лични данни касае ситуации, в които администраторът не е изпълнил свое задължение, който пропуск може да санира, като в предоставения му срок извърши пропуснатите действия и обективира изискваното от закона поведение. Относно прилагането на подходящата корективна мярка по член 58, параграф 2 от Регламента следва да се има предвид естеството, тежестта и последиците от нарушението, като се оценят всички факти по случая. Оценката за това, какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай ще трябва да отразява целта, преследвана с избраната корективна мярка, т.е. възстановяване на спазването на правилата или санкциониране на неправомерно поведение (или и двете). В конкретния случай корективните мерки по букви „а“ – „з“ и буква „й“ на чл. 58, параграф 2 от Регламента са приложими предвид факта, че се касае за липса на „свеждане на данните до минимум“, което е нарушение на настоящия регламент (буква чл. 5, §1, буква „в“). Комисията съобразява обстоятелството, че от Столична община са извършени всички необходими действия за отстраняване на нарушението, в момента, в който е установено то, включително, предприели са последващи действия, предоставени са правила за обработване лични данни при постъпване по електронен път. Предвид изложеното и на основание чл. 57, § 1, б. „е“ от Регламента, съответно чл. 10, ал. 1, във връзка с чл. 38, ал. 3 от Закона за защита на личните данни, Комисията

РЕШИ:

1. Обявява жалба с рег. № ППН-01-342/20.04.2021 г., подадена от Й.М. срещу Столична община за основателна, за нарушение на чл. 5 §1, б. „в“ от Регламент (ЕС) 2016/679.

2. Във връзка с т. 1 и на основание чл. 58 §2, б. „б“ от Регламента, КЗЛД отправя официално предупреждение до Столична община за съобразяване на операциите по обработване на данни с разпоредбите на Регламента.

Решението подлежи на обжалване в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Административен съд – София-град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ
№ ППН-01-739/2020 г.
София, 21.12. 2021 г.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав, председател, Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на редовно заседание, проведено на 20.10.2021 г. и обективизирано в протокол № 43/20.10.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни (ЗЗЛД) във вр. с чл. 57, § 1, б. „е“ от Регламент (ЕС) 2016/679, разглежда жалба с рег. № ППН-01-739/22.10.2020 г., подадена от В.Г. срещу Института по Минералогия и Кристалография (ИМК) – БАН.

Жалбоподателят информира Комисията, че до 01.07.2018 г. е бил служител на Института по Минералогия и Кристалография – БАН, заемащ длъжност доцент. След напускане установил, че акаунта в системата за отчитане на наукометрични резултати и експертна дейност SONIX, която е основно средство за институтите на БАН за годишно отчитане на наукометричните показатели, продължава да съществува, но е с блокиран достъп за г-н В.Г. В жалбата е посочено, че посредством системата SONIX се събират лични данни за научната дейност (публикации, цитирания, патенти и др.) на изследователите от БАН, на основание трудов договор. В.Г. сочи, че директорите и научните секретари на всеки институт на БАН са инструктирани относно правилата за отчитане в SONIX, като правилата не допускат използването и отчитането на лични данни за наукометрични цели.

Посочено е още, че в началото на 2020 г. г-н В.Г. установил, че през акаунта му в SONIX в годишните отчети на ИМК – БАН за 2018 и за 2019 г. се отчитат цитирания на негови публикации, в които е единствен автор от страна на ИМК – БАН.

Г-н В.Г. допълва в жалбата си, че неправомерно е отчетена една негова публикация, излязла през 2018 г., като цялата наукометрична информация не е представена в подписан и предаден от него годишен отчет към ИМК, както изисква правилника на БАН и е използвана без негово съгласие след напускането му, като служител на БАН.

Жалбоподателят твърди, че изложените от него факти и обстоятелства могат лесно да бъдат проверени в годишните отчети на ИМК – БАН за 2018 и 2019 г. (публично достъпна информация).

Отправено е искане да бъде заличен персоналният акаунт на г-н В.Г. в системата на Sonix или ако това е технически невъзможно да му бъде възстановен електронният достъп до акаунта в системата Sonix.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството на Института по минералогия и кристалография „Акад. Иван Костов“, е предоставена възможност по чл. 34, ал. 3 АПК за изразяване на становище и предоставяне на относими доказателства по предявените в жалбата твърдения.

В депозираното от ИМК – БАН становище с рег. № ППН-01-739#3(20)/18.01.2021 г. е посочено, че жалбоподателят В.Г. е бивш служител на ИМК – БАН, защитил докторска дисертация и хабилитиран в същия институт, напуснал на 01.07.2018 г., а информацията за научни степени, заемани академични длъжности, наукометрични научни резултати на всеки учен е публично достъпна чрез регистъра на научната дейност в Република България, който представлява електронна база данни с публичен достъп, която се поддържа от Министерство на образованието и науката чрез Националния център за информация и документация в съответствие с чл. 2 а от Закона за развитие на академичния състав на Република България и Правилника за прилагането му. Имената, научните степени, публикациите, местоработата, дипломите и др. на д-р В.Г. са под номер *** в регистъра на научната дейност на Република България и са публично достъпни.

Информират, че системата SONIX е електронна платформа, създадена във връзка с отчитане на научната дейност на БАН, като системата е вътрешна за БАН и „активни потребители на системата“

са само служители с трудов договор в звено (институт) от БАН, а всеки ползвател на системата SONIX, съставя сам своя уникална парола, поради която причина не би могло друг да се възползва от акаунта. Посочено е още, че наукометричните данни на служителите, събирани в системата са идентични с данните събирани в публично достъпната електронна среда на Националния център за информация и документация, а в системата SONIX не се „събират и съхраняват“ лични данни като ЕГН, номер на лична карат, банкови сметки, адреси и други.

Считат жалбата на В.Г. за неоснователна.

Разглежданите жалби съдържат задължително изискуемите реквизити, посочени в чл. 28, ал. 1 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, а именно: налице са данни за жалбоподателя, естество на искането, дата и подпис, с оглед на което са редовни.

Жалбата е процесуално допустим – подадени в срока по 38, ал. 1 от ЗЗЛД от физическо лице с правен интерес. Същата има за предмет твърдения за неправомерно обработване на лични данни на жалбоподателя и е насочена срещу администратор на лични данни. С жалбите е сезиран компетентен да се произнесе орган – Комисия за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 разглежда жалби, подадени от субекти на данни.

Комисията за защита на личните данни е независим надзорен орган, който осъществява защита на лицата при обработване на техните лични данни и при осъществяване на достъпа до тези данни, както и контрола по спазване на 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 (накратко „Регламента“ или Регламент 2016/679) и Закона за защита на личните данни (ЗЗЛД). Една от задачите на КЗЛД по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 е да разглежда жалби, подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждане на жалбите е процесуално развита в чл. 38, ал. 4 ЗЗЛД – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията жалбата може да бъде оставена без разглеждане.

С Регламент 2016/679 и Закона за защита на личните данни (ЗЗЛД) се определят правилата по отношение на защитата на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение на свободното движение на лични данни. Целта е да се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

По административната преписка не е спорно, че г-н В.Г. е бивш служител на ИМК – БАН и като такъв е ползвал системата SONIX.

Обработването на лични данни от администратори на лични данни, както в публичната, така и в частната сфера, е законосъобразно и допустимо, ако е налице някое от правните основания, изчерпателно изброени в чл. 6, параграф 1 от Регламент (ЕС) 2016/679:

- а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;
- б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
- г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

В случаите, когато администратор на лични данни прави преценка дали да обработва личните данни на базата на съгласие, той трябва да изследва обстоятелството дали не е налице друго правно основание за тяхното обработване. В случай че друго основание е налице, не е необходимо изискването и на съгласие от субекта на данни.

Посочената разпоредба обаче не се прилага, когато обработването на данни е за целите по чл. 25 з, ал 1 от ЗЗЛД, а именно обработването на лични данни за академично изразяване е законосъобразно, когато се извършва за осъществяване на свободата на изразяване и правото на информация при зачитане на неприкосновеността на личния живот. Настоящия случай е точно такъв. Като служител по трудово правоотношение с ИМК – БАН, за г-н В.Г. е налице задължение за създаване на акаунт в системата SONIX, която е електронна платформа, във връзка с отчитане на научната дейност на БАН. Системата е вътрешна за БАН и активни потребители са само служителите с трудов договор в звено институт на БАН. Всеки ползвател на системата създава сам своя уникална парола, поради което никой не може да се „възползва“ от неговия акаунт. В системата се съхранява информация – статии, съавтори, афилиации на авторите, линкове към публикации, наукометрични показатели, проекти.

Наукометричните данни за служителите, събрани в системата SONIX са идентични с данните, събрани в публично достъпната електронна среда на Националния център за информация и документация. След напускане на служител от първично звено Институт), статутът в системата SONIX се променя в „неактивен“ и научният служител няма достъп до системата.

В допълнение следва да се посочи, че жалбоподателят В.Г. е защитил докторска дисертация в ИНК – БАН. Информацията за научните степени, заеманите академични длъжности, наукометрични научни резултати на всеки учен е публично достъпна чрез регистъра на научна дейност на в Република България, който представлява електронна база данни с публичен достъп, която се поддържа от Министерство на образованието и науката чрез Националния център за информация и документация, в съответствие с чл. 2а от Закона за академичния състав в Република България и Правилника за прилагането му.

В този смисъл твърденията на жалбоподателя за използвани негово лични данни се явяват неоснователни, а по отношение на искането за възстановяване/заличаване на акаунта на г-н В.Г. следва да се посочи, че вече са налице доказателства, че по този въпрос е отговорено от института на жалбоподателя, че няма възможност за възстановяване на акаунта, предвид липсата на трудово правоотношение, поради, която причина и акаунтът не е активен.

По отношение на твърденията на жалбоподателя за неправомерно отчетена една публикация, излязла през 2018 г., като цялата наукометрична информация не е представена в подписан и предаден от него годишен отчет към НМК, както изисква правилника на БАН и е използвана без негово съгласие след напускането му, като служител на БАН, следва да се посочи, че това твърдение е извън компетентността на КЗЛД.

Публикациите на г-н В.Г. след оповестяването им в съответните платформи стават общодостъпни за всички, а най-вече са интересни за хората, които работят в съответната предметна област и имат професионален интерес.

Съмненията на жалбоподателя, че някой е достъпвал неговия вече закрит профил, до който той няма достъп, няма как да бъдат кредитирани като незаконосъобразно обработване на негови лични

данни. Напротив, личните му данни, имената му като автор, са явно обработени, тъй като неговите публикации са общоизвестни и жалбоподателят е цитиран като автор.

Въз основа на изложеното, на основание 57, § 1, б. „е” от Регламент 2016/679 и чл. 38, ал. 4 от ЗЗЛД, Комисията се произнесе със следното

РЕШЕНИЕ:

Обявява жалба с рег. № ППН-01-739/22.10.2020 г., подадена от В.Г. срещу Института по Минералогия и Кристалография към БАН, за очевидно неоснователна, и я оставя без разглеждане.

Решението подлежи на обжалване в 14-дневен срок от връчването му, чрез Комисията за защита на личните данни пред Административен съд – София – град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/



СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ Рег. № ПНМД-01-89/2021 г. гр. София, 21.10.2021 г.

ОТНОСНО: *Запитване за законосъобразност на нормативни актове, изискващи предоставяне на лични данни*

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 13.10.2021 г., разгледа преписка с рег. № ПНМД-01-89/2021 г. от главния секретар на Патентно ведомство на Република България, във връзка с постановление на Министерски съвет № 130 от 02.04.2021 г., с което е приета Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означения, обнародвана в брой 28 от 06.04.2021 г. на Държавен вестник, с която се урежда начинът на оформяне, реда за подаване и експертиза в Патентно ведомство на заявките за регистрация на марки и географски означения.

Съгласно чл. 3, ал. 1 от Наредбата, когато заявителят е физическо лице, в заявката се посочват името, презимето и фамилията; гражданството; ЕГН или личен номер, ако има такъв; постоянен и настоящ адрес или адрес на пребиваване, както и електронен адрес или адрес за кореспонденция на територията на Република България.

Посочването на ЕГН е регламентирано като задължителен реквизит в нормата на чл. 3, ал. 1 от Наредбата, при подаване на заявки за регистрации на марки от физически лица, тъй като в практиката си Патентно ведомство на Република България многократно се е сблъсквало със затруднения при получаването на кореспонденция от заявителите. В повечето случаи затрудненията са били свързани с неполучена кореспонденция от страна на заявителите, тъй като посочените от тях адреси са били неактуални. В резултат на това множество производства по заявки за регистрации на марки са оставали без разглеждане, което е било в ущърб на заявителите и в разрез с духа и целите на Закона за марките и географските означения (ЗМГО).

Главният секретар на Патентно ведомство твърди, че при изготвяне на Наредбата, съставителите и са счели за нужно да регламентират задължително посочване на ЕГН от страна на физическите лица при подаване на заявка за регистрация на марка, тъй като чрез него може да бъде направена справка за настоящ адрес в Единната система за гражданска регистрация и административно обслужване на населението (ЕСГРАОН). Това съображение е аргументирано именно с цел надлежното получаване на кореспонденция, изпратена от Патентно ведомство и е във връзка с подобряване качеството на обслужване на заявителите на регистрации за марки.

От друга страна обаче, притесненията на главния секретар на Патентно ведомство са, в това, че ЕГН безспорно представлява лични данни и задължението за предоставянето му от страна на заявители за регистрация на търговски марки може да противоречи на действащото законодателство на Република България. Предоставянето на ЕГН не е необходимо за целите на извършване на услугите, а единствено за целите на изпращане на кореспонденцията и нейното получаване.

В тази връзка главният секретар на Патентно ведомство, моли за официалното становище Комисията за защита на личните данни, дали разпоредбата на чл. 3, ал. 1 от Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означение, противоречи на Закона за защита на личните данни, Регламент (ЕС) 2016/679 и въведените с него принципи, или друг нормативен документ, уреждащ обработването на лични данни на физически лица и осъществяването на достъпа до тези данни.

Правен анализ:

Съгласно чл. 4, т. 7) от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) „администратор на лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. Следователно Патентното ведомство на Република България има качеството на „администратор“ на лични данни по отношение на личните данни, обработвани за **изпълнение на дейностите по Закона за марките и географските означения (ЗМГО)**.

Действията по отношение обработването на лични данни за целите на заявяване на регистрация на марка или географско означение, представляват „обработване на лични данни“ съгласно легалната дефиниция, посочена в чл. 4, пар. 2 от ОРЗД. Това означава всяка операция или съвкупност от операции, включващи лични данни или набор от лични данни чрез автоматични или други средства като събития, записване, организиране, структуриране, съхранение, адаптиране или промяна, изключване, консултиране, използване, разкриване чрез предаване, разпространение или друг начин, според който стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване.

С разпоредбата на чл. 6, пар. 1 от ОРЗД, включително съображение (41) от същия, се въвеждат основанията за законосъобразното обработване на лични данни, за което е необходимо наличието на поне едно от изброените условия:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнение на договор, съгласно който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди изключване на договор;

в) обработването е необходимо за спазване на законовото задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данни или върху друго физическо лице;

д) обработването е необходимо за изпълнение на задача от обществен интерес или при упражняване на официални правомощия, които са предоставени на администратора;

д) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

От друга страна, в ОРЗД, са определени принципите, които администраторът на лични данни (Патентното ведомство на Република България) следва да спазва при обработване на данните. Всеки администратор е длъжен да обработва личните данни законосъобразно, при спазване разпоредбите на ОРЗД, а именно:

- да ги обработва законосъобразно и добросъвестно и прозрачно;
- да ги събира за конкретни, точно определени и законни цели и да не ги обработва допълнително по начин, несъвместим с тези цели;
- да свежда събирането и обработването на данни до минимум;
- да събира и да бъдат поддържани в актуален вид;

– да ги поддържа във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означения урежда начина на оформяне, реда за подаване и експертиза в Патентното ведомство на заявките за регистрация на марки и географски означения. Същата е издадена на основание чл. 42, ал. 5 от ЗМГО.

Заявката за регистрация на марка или на географско означение се подава на място в Патентното ведомство, по пощата, по факс или по електронен път чрез електронната поща на ведомството или чрез Портала за електронни услуги на Патентното ведомство. Когато заявителят е физическо лице, в заявката се посочват името, презимето и фамилията; гражданството; **ЕГН или личен номер**, ако има такъв; постоянен и настоящ адрес или адрес на пребиваване, както и електронен адрес или адрес за кореспонденция на територията на Република България (чл. 3, ал. 1 от Наредбата). Единният граждански номер, е част от реквизитите, които са изчерпателно изброени и необходими при подаване на заявка за регистрация на марка или на географско означение, когато заявителят е физическо лице.

Следва да се отбележи, че по силата на чл. 9, ал. 1 от ЗМГО марката е знак, който е способен **да отличава стоките или услугите на едно лице от тези на други лица** и може да бъде представен в **Държавния регистър на марките по начин, който позволява ясно и точно да се определи предметът на закрилата**, предоставена с регистрацията. Съгласно чл. 10 от ЗМГО правото върху марка се придобива чрез регистрация, считано от датата на подаване на заявката. Правото на регистрация принадлежи на първия заявител, а правото върху марка е изключително право, което може да бъде противопоставено на трети добросъвестни лица от датата на публикация на регистрацията в Официалния бюлетин на Патентното ведомство. По аналогичен начин са уредени въпросите относно регистрацията и произтичащите от нея права във връзка с географското означение (арг. 89 и сл. от ЗМГО).

Видно от законовите разпоредби, важен елемент от придобиването на правата по ЗМГО, както и за тяхната защита, е еднозначното идентифициране на заявителя на тези права, въпреки че ЗМГО не го посочва изрично. Когато заявителят е физическо лице, неговата еднозначна идентификация може да се извърши по Единния граждански номер (ЕГН). Съгласно разпоредбите на чл. 11, ал. 1 от Закона за гражданската регистрация (ЗГР) ЕГН е административен идентификатор на подлежащите на регистрация физически лица съгласно чл. 3, ал. 2 от ЗГР. **Това е уникален номер, чрез който физическите лица се определят еднозначно.**

В същото време, Патентното ведомство води и поддържа държавните регистри на марките (чл. 5 ЗМГО) и географските означения (чл. 6 ЗМГО). Съгласно чл. 7 от ЗМГО въпросните регистри са електронни и публични. Публичният характер на регистрите обаче, не означава, че ЕГН трябва да е видим.

По отношение произтичащите от чл. 2, ал. 1 Закона за електронното управление (ЗЕУ) задължения, Патентното ведомство, като административен орган, предоставящ обществени услуги, не може да изисква от гражданите и организациите представянето или доказването на вече събрани или създадени данни, а е длъжно да ги събира служебно от първичния администратор на данните. В този смисъл, данни могат да се събират и/или проверяват, чрез достъп до тях от регистрите на първичните администратори, а за достоверността на тези проверки е необходимо еднозначното идентифициране на лицата, участващи в административния оборот, а именно чрез ЕГН.

По тези съображения и на основание чл. 58, пар. 3, б. „б” от Регламент (ЕС) 2016/679 вр. с чл. 10 а, ал. 1 от Закона за защита на личните данни, Комисията за защита на лични данни изрази следното

СТАНОВИЩЕ:

Разпоредбата на чл. 3, ал. 1 от Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означения представлява условие за законосъобразност на обработването на лични данни по чл. 6, пар. 1, б. в) от Регламент (ЕС) 2016/679, а именно обработването е необходимо за спазване на законовото задължение, което се прилага спрямо администратора въз основа на Закона за марките и географските означения.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

**СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ППН-02-463/2021 г.
гр. София, 18.11.2021 г.**

ОТНОСНО: *Фигурата на длъжностно лице по защита на данните в контекста на служебното правоотношение*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 10.11.2021 г., разглежда писмо вх. № ППН-02-463/04.10.2021 г. от адвокат от САК, с което моли комисията да установи дали и в каква степен *Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация* противоречи на императивни правила и законни цели установени с Общия регламент относно защитата на данните, и пряко нарушава законоустановената независимост на длъжностно лице по защита на личните данни при изпълнение на неговите задачи.

Във връзка с искането си, адвокатът посочва мотиви и бележки по приложимите правни актове, като изразява притеснение за колизия между тях, както следва:

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета въведе фигурата на длъжностното лице по защита на данните (ДЛЗД). Нейните основни функции са предоставяне на съвети и консултации в областта на защитата на личните данни, както и осъществяване на надзор по спазването на Регламента в организацията на администратора. Член 39, параграф 1 от Регламента посочва изчерпателно задължителен минимум от задачи, които ДЛЗД трябва да изпълнява:

- **да информира и съветва** администратора или обработващия лични данни и служителите, които извършват обработване;
- **да наблюдава спазването** на регламента;
- **при поискване да предоставя съвети** по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 35;
- **да си сътрудничи с надзорния орган;**
- **да действа като точка за контакт за надзорния орган.**

За да гарантира безпрепятственото и независимо упражняване на тези специфични и законоустановени надзорни функции, Общият регламент съдържа следните императивни правила установени в чл. 38, пар. 3:

Администраторът и обработващият лични данни правят необходимото длъжностното лице по защита на данните **да не получава никакви указания за тези задачи; и**

Длъжностното лице по защита на данните **не може да бъде освобождавано от длъжност, нито санкционирано** от администратора или обработващия лични данни за изпълнението на своите задачи.

Когато обработването се извършва от публичен орган, ОРЗД го задължава безусловно да определи длъжностно лице по защита на данните, независимо от това дали основните му дейности предполагат редовно и/или мащабно обработване на лични данни – чл. 37, пар. 1, б. „а”. Вероятно, една от причините за това е, че за разлика от търговското дружество, при публичния орган предвидените в Регламента имуществени санкции не биха имали същия възпиращ и дисциплиниращ ефект. Ето защо, Регламентът изисква публичният орган винаги да бъде подпомаган при наблюдението на вътрешното спазване от лице с експертни познания. В изпълнение на това изискване, с постановление на Министерски съвет, е изменен и допълнен *Класификатора на длъжностите в администрацията*, като е добавена длъжността – *длъжностно лице по защита на личните данни* за всеки един вид администрация.

Към настоящия момент, всяка българска администрация, в изпълнение на задължението си по чл. 37, пар. 1, б. „а”, е назначила длъжностно лице по защита на личните данни. В голямата си част, тези лица са назначени на държавна служба и имат статут на държавни служители. По този начин, върху служебното правоотношение възникнало по силата на акта за назначаване и уредено от Закона за държавния служител, се наслагва друго специфично правоотношение, възникващо по силата на Общия регламент - правоотношение между Администратор (Обработващ) лични данни и неговото ДЛЗД. Тоест, и за двете страни възникват поредица от права и задължения, произтичащи от два различни източника - Закона за държавния служител и свързаните с него подзаконови нормативни актове и Регламент (ЕС) 2016/679, Закона защита на личните данни, и други нормативни актове в областта на защитата на данните.

Такъв подзаконов нормативен акт е *Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация*. По тази наредба, ежегодно, се извършва оценяването на изпълнението на длъжността на всеки един държавен служител в съответната администрация, включително и на длъжностното лице по защита на данните, ако същото е назначено на служебно правоотношение. Оценяването съдържа две компоненти: постигането на предварително определените цели и показаните компетентности. Въз основа на степента на постигане на целите и на показаните компетентности, оценяващият ръководител определя годишната оценка на изпълнението на длъжността, като тази оценка по-нататък служи за определяне на възнагражденията на служителите, за повишаването им в ранг, а при оценка „неприемливо изпълнение” може да бъде законно основание за прекратяване на служебното правоотношение, тоест за уволнението на служителя. Също така, въпросната наредба предвижда провеждането на междинни срещи между оценяващият ръководител и оценяваният, на които се прави преглед на изпълнението на длъжността, **показаните компетентности от служителя**, както и може да се набележат конкретни действия за подобряване на изпълнението.

При така изложените аргументи, адвокатът се обръща към КЗЛД, като счита, че извършването на „оценяване на изпълнението на длъжността” заема от ДЛЗД и „набелязването на конкретни действия за подобряване на изпълнението” на задачите на ДЛЗД от страна на Администратора (Обработващия), представлява нормативно установен способ за санкциониране и освобождаване от длъжност, както и възможност за даване на указания на длъжностното лице как да изпълнява своите задачи. На практика, поднадзорното лице дава оценка на експертизата на извършващото надзора лице, а при незадоволителна оценка му налага санкции.

С оглед всичко гореизложено, адвокатът моли КЗЛД да установи дали и в каква степен **Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация противоречи на императивни правила и законни цели установени с Общия регламент, и пряко нарушава законоустановената независимост на длъжностно лице по защита на личните данни при изпълнение на неговите задачи.**

В допълнение адвокатът отбелязва, че компрометираната самостоятелност на длъжностното лице означава невъзможност за осъществяване на независим надзор върху съответния публичен орган, което пък от своя страна се явява сериозен източник на риск за правата и свободите на субектите данни. Този риск нараства многократно в условията на пандемия, когато множество български публични органи извършват редовно мащабно обработване на специални категории данни – такива относно здравето, както на българските граждани, така и на граждани на държави-членки на ЕС.

Адвокатът също така моли настоящето писмо да се счита за сигнал по реда на Глава осма, Раздел I от АПК, както и моли да бъде уведомена своевременно за решението на КЗЛД по него.

Правен анализ:

Настоящото искане съдържа принципи въпроси по прилагането на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) в частта му, касаеща правното положение на длъжностното лице по защита на данните (ДЛЗД), които следва да бъдат разгледани в съответствие с чл. 57, пар. 1, б. „в” във връзка с чл. 58, пар. 3, б. „б” от Регламент (ЕС) 2016/679. Тъй като в искането не е посочена информацията по смисъла на чл. 28, ал. 1, т. 4 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация (ПДКЗЛДНА), т.е. не е посочено лице, срещу което е подадено искането, респ. по същото не може да бъде образувано производство по Раздел II от ПДКЗЛДНА.

Съгласно съображение (97) и разпоредбата на чл. 37, пар. 5 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на ОРЗД от лице с „експертни познания и професионални качества” в областта на правото и практиките за защита на данните.

Правната уредба, разписана в съображение (97) и разпоредбата на чл. 37, пар. 6 от Регламент (ЕС) 2016/679 определя длъжностното лице по защита на данните, като „служител” или „член на персонала”. Граматическото тълкуване на тези понятия показва, че законодателят е имал предвид конкретни физически лица, независимо дали са служители на администратора или обработващия или служители на външна организация, предоставяща услуги в областта на защитата на личните данни.

Разпоредбата на чл. 37, пар. 6 от Регламент (ЕС) 2016/679 допуска възможността ДЛЗД „да изпълнява задачите въз основа на договор за услуги”. Логическото тълкуване показва, че ДЛЗД не е задължително да бъде страна по договора за представянето на услугата. Напротив, то винаги следва да е конкретен служител, изпълняващ задачите, произтичащи от договора.

Съгласно разпоредбите на чл. 37, пар. 7, чл. 38, пар. 4, чл. 39, пар. 1, б. д) от Регламент (ЕС) 2016/679 длъжностното лице по защита на данните е точка за контакт за субектите на данни, за служителите на администратора и за надзорния орган. Според Насоките за длъжностните лица по защита на данните („ДЛЗД”) на Европейския комитет за защита на данните „целта на тези изисквания е да се гарантира, че субектите на данни (както в рамките на организацията, така и извън нея) и надзорните органи ще могат лесно и пряко да се свързват с ДЛЗД, без да се налага да осъществява контакт с друга част на организацията”. Непосредственият контакт с ДЛЗД е особено важен в процедурата по уведомяване на надзорния орган за нарушение на сигурността на личните данни по смисъла на чл. 33 от Регламент (ЕС) 2016/679, предвид краткия 72-часов срок, отреден за предприемане на действия и комуникация. Това е съществена гаранция за правата на субектите на данни от една страна, а от друга е проявление на спазването на принципа за отчетност, заложен в ОРД.

Съгласно разпоредбата на чл. 38, пар. 3 от Регламент (ЕС) 2016/679 ДЛЗД **„не може да бъде освобождавано от длъжност”**, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Също така администраторите/обработващите лични данни са длъжни да гарантират, че ДЛЗД **„не получава никакви указания във връзка с изпълнението на тези задачи”** и **„се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни”**.

„Според ОРЗД санкционирането е забранено само ако се налага в резултат на изпълнението на задълженията на ДЛЗД в качеството му на ДЛЗД. Например ДЛЗД може да прецени, че дадено обработване би могло да доведе до голям риск и да посъветва администратора или обработващия лични данни да направи оценка на въздействието върху защитата на данните, но администраторът или обработващият лични данни да не е съгласен с оценката на ДЛЗД. В такъв случай ДЛЗД не може да бъде освободено от длъжност поради факта, че е дало този съвет.”

С нормите на съображение (97) и чл. 38, пар. 6 от Регламент (ЕС) 2016/679 се очертават характерните особености на длъжността на ДЛЗД – **„да изпълнява своите задължения и задачи независимо”** и функциите му **„да не водят до конфликт на интереси”**, независимо дали ДЛЗД е член на персонала на администратора/обработващия, дали съвместява длъжността или изпълнява задачи по договор за услуги. Направените уточнения налагат ДЛЗД да е лице различно от администратора/обработващия, както и от лицата, които определят целите и средствата за обработването на лични данни при съответния администратор/обработващ (като например управител, главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на маркетингов отдел, ръководител на отдел „Човешки ресурси” или ръководител на ИТ отдел, но също така и други функции по-надолу в организационната структура, ако въпросните длъжности или функции са свързани с определяне на целите и средствата за обработване на данните).

Съществен елемент от независимостта на ДЛЗД е, че същото **„се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни”** (чл. 38, пар. 3 от ОРЗД). Тази разпоредба дава ясен сигнал, че когато ДЛЗД е служител на администратора/обработващия, включително когато той е публичен орган, неговата позиция следва да бъде организационно и функционално обособена от другите структурни звена на организацията. Аналогични примери за длъжности в администрацията, които пряко отчитат своята дейност пред най-висшето ръководно ниво са длъжностите на служител по сигурността на информацията и финансовия контролор. По правило тези длъжности са на пряко подчинение на ръководителя на съответната организация, т.е. функционално ръководството на тяхната дейност не може да бъде опосредено, чрез структурното им позициониране в рамките на административните звена (дирекции, отдели, сектори). Дори когато ДЛЗД изпълнява тази функция по съвместяване или чрез възлагане към друга заемана длъжност, ДЛЗД подлежи на оценка, извършена от съответния пряк ръководител, който в случая, за да бъде изпълнено условието на ОРЗД, е ръководителят на организацията. Това разбиране напълно съответства на изискванията на чл. 4, ал. 1 от Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация, в който се посочва, че оценяващ е ръководителят, на когото съответният служител е непосредствено подчинен – в случая ДЛЗД трябва да бъде оценявано, като държавен служител, заемащ длъжността ДЛЗД съгласно Класификатора на длъжностите в администрацията пряко от органа по назначаването.

В заключение, може да се обобщи, че ОРЗД осигурява няколко гаранции, с които се дава възможност на ДЛЗД да действа независимо:

- не се дават указания от страна на администраторите или обработващите лични данни по отношение на изпълнението на задачите на ДЛЗД;
- не се допуска освобождаване от длъжност от страна на администратора във връзка с изпълнението на задачите на ДЛЗД;
- не се допуска конфликт на интереси с евентуални други задачи и задължения.

Това обаче не означава, че ДЛЗД е безотчетно, безконтролно и безотговорно пред администратора/обработващия, включително когато е публичен орган. В този смисъл предвиденият в Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация механизъм за оценка на дейността на държавния служител, заемащ длъжността ДЛЗД, не противоречи на изискването за отчетност и независимост по Регламент (ЕС) 2016/679 на ДЛЗД пряко пред най-висшето ръководство на публичния орган. Нещо повече, ОРЗД изисква ДЛЗД да е независимо при изпълнението на възложените му задачи по смисъла чл. 39, като то не носи лична отговорност по ОРЗД, в случай на неспазване на изискванията за защита на данните. Администраторът или обработващият лични данни е този, който е длъжен да гарантира и да бъде в състояние да докаже, че обработването се извършва в съответствие с ОРЗД. Спазването на разпоредбите за защита на данните е отговорност на администратора или обработващия лични данни. В същото време, ДЛЗД може да носи дисциплинарна отговорност по общия ред, например нарушение на трудовата дисциплина, в случай на кражба, физически, психологически или сексуален тормоз или подобни груби прояви на поведение, несъвместимо с трудовата дисциплина и т.н.

По тези съображения и на основание чл. 58, пар. 3, б. б) от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

Предвиденият в Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация механизъм за оценка на дейността на държавния служител, заемащ длъжността ДЛЗД, не противоречи на изискването за независимост на ДЛЗД по чл. 38, пар. 3 от Регламент (ЕС) 2016/679.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ Рег. № ПНМД-17-206/2021 г. гр. София, 29.11.2021 г.

ОТНОСНО: *Заличаване на лични данни от базата данни на съда*

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 24.11.2021 г., разгледа преписка с рег. ПНМД-17-200/2021 от г-н М. по въпрос, свързан с правната възможност за заличаване на личните му данни от базата данни на съда. Г-н М. твърди, че като непълнолетен е бил осъден на лишаване от свобода, след което е завършил право, като не е знаел, че присъдата ще му пречи за някои професии, за което се изисква образование право.

Посочва се, че по-специално в Закона за нотариусите и нотариалната дейност е разписано, че не могат да бъдат нотариуси лица, които са осъждани на лишаване от свобода, независимо от

реабилитацията. Същото е разписано и в Закона за частните съдебни изпълнители.

Въпросът, който поставя г-н М. е следният: след като са минали 16 години от датата на реабилитацията, не следва ли осъждането и последиците да се заличат независимо какво е предвидено в друг закон или указ по чл. 88 а от Наказателния кодекс (НК), така наречената „абсолютна реабилитация” и когато лице си вад свидетелство за съдимост за конкурс за нотариус или частен съдебен изпълнител, то да е неосъждано, въпреки че в момента същото е осъждан/реабилитиран.

Г-н М. твърди, че може да се яви на изпита за адвокат, за синдик, но на изпит за нотариус и частен съдебен изпълнител не може.

Въпросът, който поставя г-н М. пред КЗЛД е има ли механизъм, чрез който да се заличи и реабилитацията и присъдата, след като е настъпила абсолютна реабилитация по чл. 88а от НК.

Правен анализ:

Правото на изтриване осигурява на физическите лица механизъм за ограничаване на съхранението на личните им данни от конкретен администратор. Целеният ефект от упражняването на правото е преустановяване на по-нататъшната възможност за обработване на данните, които идентифицират лицето.

Предвид колизията, която може да се породи между интересите на конкретно физическо лице от изтриване на данните и интересите на администратора или обществения интерес от съхраняването им, правото на изтриване е предмет на детайлна уредба. С предвиждането на конкретни основания, при които правото може да бъде упражнено, и специфичните основания, на които може да се откаже неговото реализиране се цели балансиране между тези противоположни интереси. Не във всички случаи на обработване на лични данни субектът на данни разполага с право да иска тяхното изтриване от администратора.

Правото на изтриване може да бъде упражнено на основанията, посочени в чл. 17, пар. 1 от ОРЗД. Субектът на данни следва да посочи на кое от основанията (едно или повече) иска от администратора изтриване на свързаните с него лични данни:

а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните съгласно член 6, параграф 1, буква а) или член 9, параграф 2, буква а), и няма друго правно основание за обработването;

в) субектът на данните възразява срещу обработването съгласно член 21, параграф 1 [когато обработването се основава на член 6, параграф 1, буква д) (обществен интерес или официални правомощия) или буква е) (легитимен интерес)], включително профилиране, и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно член 21, параграф 2 (директен маркетинг);

г) личните данни са били обработвани незаконосъобразно;

д) личните данни трябва да бъдат изтрети с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

е) личните данни са били събрани във връзка с предлагането на услуги на информационното общество по член 8, параграф 1 (Условия, приложими за съгласието на дете във връзка с услугите на информационното общество).

Правото на изтриване на данните („правото да бъдеш забравен”) се подчинява на специални ограничения, предвидени в чл. 17, пар. 3 от ОРЗД. Тези ограничения произтичат пряко от Регламента и са израз на балансирания подход при реализиране на правомощията, включени в обхвата на

правото за защита на личните данни, и основните права на другите правни субекти, при отчитане на общественения интерес от обработването на лични данни. Предвид това правото, съгласно разпоредбата на чл. 17, пар. 3 от ОРЗД, **правото на изтриване не се прилага**, ако обработването е необходимо за следните цели:

а) за упражняване на правото на свобода на изразяването и правото на информация;

б) за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

в) по причини от обществен интерес в областта на общественото здраве и при спазване на относимите гаранции в съответствие с чл. 9 от Общия регламент относно защитата на данните;

г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност правото на изтриване да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или

д) за установяването, упражняването или защитата на правни претенции.

Съгласно чл. 85, ал. 1 от Наказателния кодекс (НК) реабилитацията заличава осъждането и отменя за в бъдеще последиците, които законите свързват със самото осъждане, **освен ако в някое отношение със закон или указ е установено противното.**

Бюлетини за съдимост се съставят за всички осъдени лица, включително и в случаите, когато осъденият е освободен от изтърпяване на наказанието или не е наказан съгласно НК, или е приложено условно осъждане, съгласно разпоредбите на Наредба № 8 от 26 февруари 2008 г. за функциите и организацията на дейността на бюроа за съдимост. Разпоредбата на чл. 17, ал. 1, т. 2 от същата изрично гласи, че в **хартиения и в електронния бюлетин за съдимост служебно се отбелязват допълнителни сведения, когато лицето е реабилитирано.**

Изхождайки от спецификата на казуса, а именно желанието на искателя да се яви на конкурс за нотариус или частен съдебен изпълнител, то следва да се обърне внимание на изискванията и условията за придобиване на правоспособност на нотариус и на частен съдебен изпълнител.

Законът за нотариусите и нотариалната дейност урежда правния статут на нотариуса и на Нотариалната камара, организацията на нотариалната дейност и нотариалните такси.

Съгласно разпоредбите на чл. 8, ал. 1 от Закона за нотариусите и нотариалната дейност правоспособност на нотариус може да придобие дееспособно физическо лице на възраст до 60 години, което е български гражданин, гражданин на държава - членка на Европейския съюз, на държава - страна по Споразумението за Европейското икономическо пространство, или на Конфедерация Швейцария и отговаря на следните **изисквания:**

1. има висше юридическо образование;

2. придобило е юридическа правоспособност по Закона за съдебната власт;

3. има тригодишен стаж;

4. не е осъждано на лишаване от свобода за умишлено престъпление, независимо че е реабилитирано;

5. не е лишено от правоспособност на нотариус;

6. не е лишено от правото да упражнява адвокатска професия или търговска дейност;

7. не е в производство по несъстоятелност, не е невъзстановен в правата си несъстоятелен или не е осъждано за банкрут;

8. вписано е в регистъра на Нотариалната камара.

Законът за частните съдебни изпълнители урежда организацията и правното положение на частните съдебни изпълнители.

Правоспособност на частен съдебен изпълнител може да придобие дееспособно физическо лице, което е български гражданин и отговаря на следните изисквания (чл. 5, ал. 4 от Закона за частните съдебни изпълнители):

1. има висше юридическо образование;

2. придобило е юридическа правоспособност по Закона за съдебната власт;

3. има тригодишен юридически стаж;

4. не е осъждано на лишаване от свобода за умишлено престъпление от общ характер, независимо че е реабилитирано;

5. не е лишено от правоспособност на частен съдебен изпълнител;

6. не е лишено от правото да упражнява адвокатска професия или търговска дейност;

7. не е в производство по несъстоятелност, не е невъзстановен в правата си длъжник, обявен в несъстоятелност, и не е осъждано за банкрут;

8. издържало е конкурса за частен съдебен изпълнител.

Както е видно и в Закона за нотариусите и нотариалната дейност, и в Закона за частните съдебни изпълнители е въведено изрично изискване за придобиване на правоспособност за нотариус и за частен съдебен изпълнител лицето да **не е осъждано на лишаване от свобода за умишлено престъпление от общ характер, независимо че е реабилитирано**. За пълнота на изложението следва да се отбележи, че и със Закона за съдебната власт се въвеждат такива изисквания по отношение на изборните членове на Висшия съдебен съвет (арг. чл. 18), съдебните заседатели (арг. чл. 67), съдиите, прокурорите и следователите (арг. чл. 162).

Следователно, субектът на данни, не може да се позове на правото на изтриване (правото „да бъдеш забравен“) разписано в чл. 17 от Общия регламент относно защитата на данните (lex generalis), поради наличие на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора (чл. 17, пар. 3, б. „б“), а именно изискванията за придобиване на правоспособност разписани в Закона за нотариусите и нотариалната дейност и Закона за частните съдебни изпълнители (lex specialis).

По тези съображения и на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 вр. с чл. 10 а, ал. 1 от Закона за защита на личните данни, Комисията за защита на лични данни изрази следното

СТАНОВИЩЕ:

Администраторът на лични данни Бюрото по съдимост не може да удовлетвори искането на физическо лице за изтриване на данни („правото да бъдеш забравен“) на основание специалните ограничения, предвидени в чл. 17, пар. 3, б. „б“ от ОРЗД, съгласно които правото на изтриване не се прилага, ако обработването е необходимо за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора, а именно: в конкретния случай - Закона за нотариусите и нотариалната дейност и Закона за частните съдебни изпълнители.

Разпоредбите на чл. 8, ал. 1, т. 4 от Закона за нотариусите и нотариалната дейност, както и чл. 5, ал. 4, т. 4 от Закона за частните съдебни изпълнители въвеждат задължително изискване при придобиване на правоспособност за нотариус и за частен съдебен изпълнител лицето да **не е осъждано на лишаване от свобода за умишлено престъпление от общ характер, независимо че е реабилитирано.**

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/



ОБОБЩЕНА ПРАКТИКА НА КЗЛД СЛЕД 25 МАЙ 2018 Г. ПО ВЪПРОСИ, СВЪРЗАНИ С ОСЪЩЕСТВЯВАНО ВИДЕОНАБЛЮДЕНИЕ

Видеонаблюдението е един от фокусите на внимание на КЗЛД, както с оглед на неговото естество, така и във връзка с множеството жалби и сигнали пред Комисията с твърдения за незаконосъобразно обработване на лични данни на физически лица. Многократно КЗЛД е извършвала проверки с цел изясняване на отделни случаи, произнасяла се е с решения по жалби, упражнявала е своите корективни правомощия в съответствие с разпоредбите на Регламент (ЕС) 2016/679 и ЗЗЛД. В настоящия материал предлагаме обобщение на практиката на КЗЛД след 25 май 2018 г. по въпроси, свързани с осъществявано видеонаблюдение.

Видеонаблюдението представлява дейност по обработване на лични данни, когато се извършва чрез запис от технически средства за видеонаблюдение, който се съхранява. Съдържащата се в записите от средствата за наблюдение информация за физическото лице – образ, попада в обхвата на понятието лични данни, тъй като лицето може да бъде идентифицирано. Събирането и съхраняването на тези лични данни са операции по обработване по смисъла на чл. 4, т. 2 от Регламент (ЕС) 2016/679 и следва да се извършват при спазване на правилата за защита на личните данни. Това предполага **наличие на поне едно от правните основания, посочени в чл. 6, § 1 от Регламент (ЕС) 2016/679, спазване на всички принципи за обработването на лични данни по чл. 5 от същия регламент, както и на останалите изисквания в областта на защитата на данните.**

С оглед предмета на жалбите и сигналите пред КЗЛД с твърдения за незаконосъобразно обработване на личните данни на физически лица чрез видеонаблюдение могат да бъдат разграничени следните хипотези: видеонаблюдение, осъществявано в сгради в режим на етажна собственост, видеонаблюдение на имот в режим на съсобственост, видеонаблюдение между съседи и видеонаблюдение на работното място. Независимо от това в коя хипотеза попада даден случай на осъществявано видеонаблюдение, КЗЛД винаги следи за спазването на разпоредбите на Регламент (ЕС) 2016/679 и по-специално на следните изисквания:

1. Да е налице законна цел за видеонаблюдението. В зависимост от целите, за които се извършва видеонаблюдението, се прилагат различни правила по отношение на правното основание за извършването му, обхвата на камерите, записите и сроковете за тяхното съхранение. Обичайно, когато видеонаблюдението се използва с охранителна цел в защита на легитимен интерес (свой или на трета страна), администраторите на лични данни трябва да разположат видеокамерите по такъв начин, че да заснемат единствено охранявания обект. Администраторите нямат право да заснемат обществени места като улици, тротоари, площади, паркинги и други подобни. Друг е случаят, когато видеонаблюдението се извършва в обществен интерес за охрана на обществения ред и сигурност от публичен орган. Тогава камерите обхващат именно публични обекти – улици, площади, паркове и др. Съществува и видеонаблюдение, което е законово регламентирано – напр. видеозаснемането по Закона за движението по пътищата. Комисията за защита на личните данни разглежда всеки конкретен случай отделно и самостоятелно, съобразно спецификата на обстоятелствата и приложимото право, например съгласно Закона за частната охранителна дейност, специалните разпоредби в областта на банковата сигурност и др.

2. Да е налице правно основание за обработването на лични данни чрез технически средства за видеонаблюдение съгласно чл. 6, § 1 от Регламент (ЕС) 2016/679, което е предпоставка за законосъобразност на обработването. Отговорност на администратора е да установи и обоснове наличието на изискванията за законосъобразност във всеки един конкретен случай. В случай че видеонаблюдението се позовава на разпоредбата на чл. 6, § 1, б. „е“ (легитимен интерес на администратора или на трета страна), от съществено значение е да се извърши преценка и да се балансират законните интереси на администратора или третата страна и правата и свободите на субектите на данни, засегнати от видеонаблюдението.

3. Физическите лица, обект на видеонаблюдение, да бъдат уведомявани за използването на технически средства за наблюдение в съответния обект. За целите на извършването на видеонаблюдение, съответният администратор на лични данни, който го извършва или който е взел решение за извършването му, е длъжен да уведоми субектите на данни за факта, че се обработват техни данни чрез заснемане с технически средства за видеонаблюдение, без да е необходимо да се уточнява местоположението им. Това свое задължение администраторът може да изпълни чрез **поставяне на видно място на уведомителни табели/информационни табла**, на които задължително трябва да бъде предоставена информация, която идентифицира администратора и координатите за връзка с него, целите и правното основание за обработването, категориите лични данни, които се обработват. **Пълният обем на информацията**, която трябва да се предостави от администратора на субекта на данни при обработване на лични данни чрез видеонаблюдение, **е посочен в чл. 12 и 13 от Регламент (ЕС) 2016/679.**

4. Да бъдат предприети подходящи технически и организационни мерки за сигурност на данните. Съгласно чл. 24 от Регламент (ЕС) 2016/679, след като вземе предвид естеството, обхвата, контекста и целите на обработването, администраторът следва да въведе подходящи технически и организационни мерки, за да гарантира, както и във всеки един момент да е в състояние да докаже, че обработването се извършва в съответствие с правилата на Регламента. Още на етапа на изграждането на системите за видеонаблюдение следва да се отчетат рисковете с различна вероятност и тежест за правата на физическите лица, обект на видеонаблюдението, и съответно да се въведат подходящите мерки (технически и организационни), които ще осигурят законосъобразното протичане на дейностите по обработване. По този начин ще се отговори и на изискванията на чл. 25 от Регламента – защита на данните на етапа на проектирането и по подрабаване.

Изискването на чл. 24 от Регламент (ЕС) 2016/679, което е и проявление на принципа на отчетност (чл. 5, § 2 от Регламента), означава, че конкретните мерки се определят само и единствено от администратора. Независимо от това, в контекста на извършването на видеонаблюдение би било целесъобразно да бъде определен ограничен кръг от лица, които ще имат достъп до техническите средства, на които ще се съхраняват видеозаписите, предварително да е одобрен редът за достъп до помещението, в което се съхраняват те, да се обосноват сроковете за съхранението на записите съобразно целите на видеонаблюдението, мерките за сигурност при достъпването им и т. н. Прилагането на подходящи технически и организационни мерки изисква да бъде взето предвид и правото на достъп на субекта на данни, уредено в чл. 15 от Регламент (ЕС) 2016/679. Субектът има право да получи информация за целите на обработването, категориите лични данни, които се обработват, сроковете за съхранение и други изрично посочени аспекти на обработването. Администраторът следва да отчита и задължението си да предостави копие от личните данни в процес на обработване на физическото лице, подало съответното заявление за достъп до свои лични данни. Изпълнението на това задължение предполага наличие на техническа възможност за заличаване на данните на трети лица, ако такива попадат в заснетите видеокадри и за чиито лични данни не е налице правно основание за предоставянето им. Правото на достъп, вкл. на копие от личните данни, се отнася до всички субекти на данни.

При дефинирането на основните параметри на видеонаблюдението и на конкретните подходящи технически и организационни мерки от ключово значение е спазването на принципа „свеждане на данните до минимум“. Комисията за защита на личните данни има утвърдена и трайна практика – администраторите не могат да извършват видеонаблюдение на съседни сгради и обществени пространства. Заснемането на публични площи от отделни лица надхвърля охранителните цели, за които обикновено се монтират системите за видеонаблюдение.

5. За осъществяване на видеонаблюдение в режим на етажна собственост се налага да бъдат спазени и редица специфични изисквания, произтичащи от специалната правна уредба на Закона за управление на етажната собственост (ЗУЕС). Необходимо е да се отчита изискването на чл. 17, ал. 3 от ЗУЕС, съгласно което решенията следва да се приемат с мнозинство повече от 50 на сто от представените идеални части от общите части на етажната собственост. Решението за инсталиране на видеосистема за наблюдение в жилищна сграда в режим на етажна собственост

също следва да бъде взето с такова мнозинство. Обработването на лични данни в този случай е въз основа на легитимния интерес на живущите в жилищната сграда, т.е. на основание чл. 6, § 1, б „е“ от Регламент (ЕС) 2016/679. Следва да се има предвид, че решенията на етажната собственост имат обвързваща сила и за лицата, които не са присъствали, както и спрямо тези, които са гласували против. Аргументите за това могат да се извлекат от практиката на Върховния касационен съд съгласно Решение № 39 от 19.02.2013 г. по гр. д. № 657/2012 г., Г. К., I Г. О. на ВКС. Върховният касационен съд приема, че след влизането им в сила решенията на етажните собственици са задължителни за всички етажни собственици, включително за тези, които са гласували против, за неучаствалите във вземането им и за лицата, които по-късно ще станат етажни собственици или обитатели. Следователно, решението за извършване на видеонаблюдение е задължително и за собствениците, подали уведомление, че не желаят да бъдат заснемани.

Монтирането на видеокамери в сграда в режим на етажна собственост, без за това да е взето решение по гореописаната процедура, би било в нарушение на Регламент (ЕС) 2016/679 и ЗУЕС. Физическо лице би могло да претендира, че извършва дейността по видеонаблюдение за лични цели единствено, ако камерите са монтирани в границите на неговия имот и не заснемат общи части от сградата.

Независимо от това, че всеки конкретен случай следва да бъде разглеждан самостоятелно с цел отчитане на неговия специфичен контекст, с настоящия информационен материал КЗЛД прави обобщение на своята трайна/обичайна практика при разглеждането на жалби или сигнали с предмет видеонаблюдение. Практиката е относима както към спорове между физически лица, породени от междуличностни конфликти, при които едно физическо лице (*засегнато от осъществявано видеонаблюдение*) търси защита срещу друго физическо лице (*лице, което е изградило система за видеонаблюдение*), така и в отношенията администратор на лични данни-субекти на данни. При разглеждането на жалби и сигнали с предмет видеонаблюдение КЗЛД следи за спазване на всички правила на Регламент (ЕС) 2016/679, вкл. за посочените по-горе специфични изисквания.

С решенията, с които надзорният орган се произнася по казуси с предмет видеонаблюдение, той упражнява своите корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като издава съответно разпореждания (на основание чл. 58, § 2, б. „г“), предупреждения (на основание чл. 58, § 2, б. „а“) или официални предупреждения (на основание чл. 58, § 2, б. „б“). Във всеки конкретен случай, съобразно естеството на наложените корективни мерки и тежестта, която те създават върху администратора на лични данни, Комисията определя възможно най-кратък срок за тяхното изпълнение, като се отчитат правата на засегнатите субекти на данни (напр. 14-дневен, 1-месечен, 3-месечен и др.).

Диспозитивът на всяко решение се формулира по начин, който е съобразен с конкретната фактическа обстановка (*напр. видеонаблюдение, което засяга съседи; видеонаблюдение в режим на етажна собственост и др.*) и индивидуалния предмет на спора, в рамките на следните алтернативни принципни положения, групирани съобразно упражняването от КЗЛД корективно правомощие:

I. РАЗПОРЕЖДАНЯ

Комисията за защита на личните данни издава разпореждания на администраторите на основание чл. 58, § 2, б. „г“ във връзка с чл. 57, § 1, б. „а“ и чл. 83, § 2 от Регламент (ЕС) 2016/679, **за нарушение на разпоредби** на този Регламент във връзка с осъществявано видеонаблюдение. В тези случаи КЗЛД „РАЗПОРЕЖДА“ на съответния администратор да съобрази операциите по обработване на лични данни с разпоредбите на Регламент (ЕС) 2016/679 (напр. с чл. 6, § 1, букви „а-е“) и, ако е целесъобразно, указва начин и определя срок за това. Трайната практика на КЗЛД в случаите на незаконосъобразно видеонаблюдение е да разпорежда на администратора да:

- преустанови видеонаблюдението на обществени места и на имота на съответния жалбоподател и постави обозначителни табели за осъществяването в имота си видеонаблюдение;

- преустанови видеонаблюдението/заснемането на публични площи (*посочва се относимото, като напр. улица/части от прилежащата улица, части от уличното платно, тротоари, търговски обект - магазин „Х“, съседни/чужди имоти, жилищни сгради/част от фасадата на блок № Х, междублокови и затревени площи, алеи и др.*) посредством изградената система за видеонаблюдение в даден имот, като пренасочи камерата така, че да заснема само границите на собствения му имот. При невъзможност за пренасочване на камерата, същата следва да бъде демонтирана;

- преустанови заснемането на общи части (етажна площадка) на жилищната сграда – етажна собственост, посредством изградената от него система за видеонаблюдение;

- преустанови заснемането на общи части на жилищната сграда – входната врата и фойето на партерния етаж на сградата, общите коридори и подходите към подземните гаражи, както и коридора на съответния етаж в сградата, посредством изградената система за видеонаблюдение, като премахне камерите;

- преустанови заснемането на общи части на жилищната сграда – етажна площадка на съответния етаж и асансьора, вътрешния коридор на същия етаж и подстъпа към него, посредством изградената система за видеонаблюдение на адреса, чрез премахване на камерите, които са поставени без правно основание – при липса на представено в КЗЛД решение на етажната собственост;

- преустанови видеонаблюдението на общи части от етажната собственост, както и на чужди имоти, посредством изградената система за видеонаблюдение в жилищната сграда – етажна собственост, като пренасочи камерата и да заснема само неговото жилище и гараж. При невъзможност за пренасочване на камерата, същата следва да бъде демонтирана;

- преустанови видеонаблюдението на общи части на етажната собственост, посредством изградената система за видеонаблюдение в жилищната сграда – етажна собственост, докато не бъде взето легитимно решение на Общо събрание на етажната собственост, съгласно чл. 11 от ЗУЕС. В случай, че в срока на разпореждането такова решение не бъде взето, камерите следва да бъдат премахнати;

- преустанови видеонаблюдението на общи части от етажната собственост, публични площи (улици и тротоари) и прозорци на чужди имоти, посредством изградената система за видеонаблюдение в жилищна сграда – етажна собственост, чрез премахване на камерите;

- преустанови заснемането на общия вход на жилищната сграда на същия адрес, както и подстъпът към него, посредством изградената система за видеонаблюдение;

- преустанови видеонаблюдението на общи части от етажната собственост, в т.ч. входни врати на чужди жилища, както и на публични места (улици, тротоари), посредством изградената система за видеонаблюдение в жилищната сграда – етажна собственост;

- преустанови видеонаблюдението на публични места (части от уличното платно и прилежащите тротоари) и чужди имоти посредством изградената система за видеонаблюдение чрез корекция на ъгъла на видеозаснемане, където е възможно, или чрез въвеждане на система за замъгляване на публични места, или чрез премахване на видеокамерите, които извършват видеонаблюдението на публични места и чужди имоти;

- преустанови видеонаблюдението на публични места (части от уличното платно), посредством изградената система за видеонаблюдение, чрез корекция/пренасочване на ъгъла на видеонаблюдение на камера № камера №, или чрез въвеждане на частни зони чрез софтуерно замъгляване. В случай, че нито един от посочените два подхода не може да бъде приложен, камера № и камера № да бъдат премахнати;

- преустанови видеонаблюдението на публични места (улици и тротоари), посредством изградената система за видеонаблюдение в жилищната сграда – етажна собственост, чрез репозициониране на камерата, така че да заснема физическите лица, след влизането им в етажната собственост.

II. ПРЕДУПРЕЖДЕНИЯ

Комисията за защита на личните данни издава предупреждения на администраторите на основание чл. 58, § 2, б. „а“ във връзка с чл. 57, § 1, б. „а“ и чл. 83, § 2 от Регламент (ЕС) 2016/679, когато има вероятност операции по обработване на данни, които те възнамеряват да извършат (в случая видеонаблюдение), да нарушат разпоредбите на Регламента. В тези случаи КЗЛД ОТПРАВЯ „ПРЕДУПРЕЖДЕНИЕ“ на съответния администратор за това, че:

- в изградената система за видеонаблюдение във всеки един момент може да бъде променена посоката на камерата и да извършва видеонаблюдение на чужд съседен имот, собственост на друго лице, като има вероятност да обработва лични данни без наличие на правно основание, с което да наруши разпоредбите на чл. 6, § 1, букви „а“, „е“ от Регламент (ЕС) 2016/679;

- въвеждането в експлоатация на съответната система за видеонаблюдение, има вероятност да наруши разпоредбите на Регламент (ЕС) 2016/679. Ако бъде въведена в експлоатация в този вид, администраторът ще наруши правилата за обработване на лични данни. За да бъде функционираща система, тя трябва да отговаря на изискванията: да не снима публични места (обществени територии), да има решение на общото събрание, а не само съгласие на собственици на апартаменти, за които не е ясно каква идеална част от общата сграда притежават, следва да има решение и протокол, от които ясно да се вижда, че са спазени изискванията на Закона за управление на етажната собственост;

- има вероятност операциите по обработване на лични данни, посредством видеозаснемане с камери №..... и №, ако камерите работят и в обхвата им попадат публични зони и чужди имоти, да нарушат разпоредбите на Регламент (ЕС) 2016/679.

III. ОФИЦИАЛНИ ПРЕДУПРЕЖДЕНИЯ

Официални предупреждения КЗЛД отправя, когато операциите по обработването на лични данни **са нарушили** разпоредбите на Регламент (ЕС) 2016/679, **но нарушението не е налице или вече е отстранено от администратора на лични данни към момента на издаване на индивидуалния административен акт** съобразно чл. 142 от АПК. В такива случаи на основание чл. 58, § 2, б. „б“ във връзка с чл. 57, § 1, б. „а“ и чл. 83, § 2 от Регламент (ЕС) 2016/679, **Комисията за защита на личните данни ОТПРАВЯ „ОФИЦИАЛНО ПРЕДУПРЕЖДЕНИЕ“** на съответния администратор:

- за нарушение на чл. 6, § 1 от Регламент (ЕС) 2016/679;

- предвид обстоятелството, че обработването на лични данни чрез осъществявано от него видеонаблюдение на обществени територии-улицы и прилежащи към тях тротоари, както и чужди имоти и жилищни сгради посредством описаните в съответното решение на КЗЛД камери е в нарушение на чл. 5, § 1, б. „а“ и „в“ от Регламент (ЕС) 2016/679.

При постъпване на жалби с предмет незаконосъобразно обработване на лични данни посредством видеонаблюдение КЗЛД извършва проверки по предмета на жалбите. Така тя изпълнява задължението си за служебно събиране на доказателства с цел изясняване на отделните случаи от правна и фактическа страна, съблюдавайки застъпените в административния процес принципи на служебно начало и истинност. Констативните актове от извършените проверки се приобщават към съответното административно производство, след което Комисията се произнася по допустимостта и основателността на подадените жалби.

Комисия за защита на личните данни

Председател: Венцислав Караджов

Членове: Цанко Цолов

Мария Матева

Веселин Целков

Информационен бюлетин № 1 (94) 2022 г.

Издава се съгласно чл. 10, ал. 3 от ЗЗЛД

Уеб сайт на КЗЛД: www.cdpd.bg

Разпространява се в електронен вид

ISSN 2367-7759