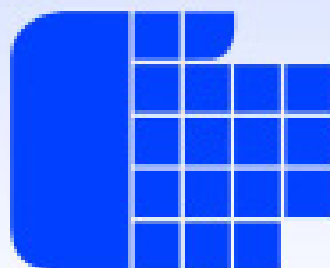


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 3 (114), май 2025 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода март и април 2025 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
Комисията за защита на личните данни депозира в Народното събрание годишния отчет за дейността си през 2024 година.	3
Заседания на Европейския комитет по защита на данните.....	9
ЕКЗД прие изявление относно прилагането на Директивата за резервационните данни на пътниците.....	10
Годишен доклад на ЕКЗД за 2024 г.: Защита на личните данни в динамичната дигитална среда	11
Започва координирано действие по изследване на приложението на правото на изтриване (право „да бъдеш забравен“).	12
КЗЛД проведе форум за възможностите пред държавата и бизнеса при приемането на България в ОИСР.....	13
Потенциални заплахи за правата на субектите на данни в контекста на предложението за Регламент CSAM	14
Информация за стандартните договорни клаузи	16
Предстоящи дейности по проект OPWNI	17
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	18
СТАНОВИЩА НА КЗЛД	19

СЪБИТИЯ И ИНИЦИАТИВИ

КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ДЕПОЗИРА В НАРОДНОТО СЪБРАНИЕ ГОДИШНИЯ ОТЧЕТ ЗА ДЕЙНОСТТА СИ ПРЕЗ 2024 Г



На 28 март 2025 г. Комисията за защита на личните данни депозира в деловодството на Народното събрание Годишния отчет за дейността си през 2024 година. Отчетът е депозирал съгласно чл.7, ал.6 от Закона за защита на личните данни и обхваща периода от 01.01.2024 г. до 31.12.2024 г. Състои се от 249 страници, обособени в 13 основни раздела.

Отчетът представя информация по всички основни направления на дейност на КЗЛД. Традиционно

годишният доклад на Комисията започва с информация за реализираните цели и приоритети през отчетната година. Представени са важни акценти от надзорната дейност на Комисията, осъществявана по линия на разглеждането на жалби и сигнали за нарушения в областта на защитата на личните данни, на уведомления за нарушения на сигурността и извършените проверки на администратори на лични данни. Осъществен е преглед на практиката на КЗЛД по изразяване на становища по въпроси с принципен характер и от значим обществен интерес. Представени са международният опит на Комисията и дейността по линия на сътрудничеството със сродни органи и организации. Направен е обобщен преглед на административния капацитет и финансовото състояние на комисията.

КЗЛД отчита, че през 2024 г. е сезирана с 1080 жалби, подадени от физически лица, не само български, но и чуждестранни граждани, с твърдения за нарушения при обработване на лични данни и упражняване на права. Забелязва се значително увеличаване на броя жалби в сравнение с предходната 2023 г., когато броят на жалбите е 900 и тези, подадени през 2022 г. – 770. Запазва се тенденцията подадените жалби да се отличават с правна и фактическа сложност – повече от един жалбоподател и/или ответни страни, жалбоподатели, не само български, но и чуждестранни граждани или администратори на лични данни с основно място на установяване извън територията на Република България. Секторите на дейност на АЛД, срещу които най-често са постъпвали през 2024 г. жалби от физически лица, са видеонаблюдение (345 жалби), банки и кредитни институции (109 жалби), физически лица (83 жалби), държавни органи (61 жалби), телекомуникации (45 жалби), политически субекти (33 жалби), здравеопазване (22 жалби), медии (22 жалби), трудови и осигурителни услуги (11 жалби), застраховане (10 жалби), образование (9 жалби).

Запазва се тенденцията сектор „Видеонаблюдение“ да е водещ по брой жалби. Разглеждането на казуси, свързани с обработване на лични данни чрез изградени системи за видеонаблюдение, отнема сериозен финансов и експертен ресурс на КЗЛД. Отчита се липсата на уреждане на обществените отношения извън тези по Закона за частната охранителна дейност, свързани с изграждане и поддържане на системи за видеонаблюдение от физически и юридически лица с цел защита на имоти. Все по-голям е броят на жалбите с предмет видеонаблюдение извън столицата, което допълнително затруднява производствата предвид липсата на териториални административни звена на КЗЛД. Допълнителен проблем е и липсата на сътрудничество в хода на производството от страна на администраторите.

Увеличен е и броят на жалбите, подадени срещу държавни органи от 33 през 2022 г., 56 през 2023 г., до 61 през 2024 г. Запазва се тенденцията тези жалби предимно да касаят упражняване на права, предоставяне на лични данни на трети лица/страни без съгласие на субекта на данни или събиране и

съхранение на лични данни без основание.

Наблюдава се нарастване на броя жалби, подадени срещу банки и дружества, предлагащи кредитни услуги. През 2023 г. техният брой е 88, а през 2024 г. – 109. Секторът остава сред водещите, срещу които най-често постъпват оплаквания. Традиционно твърденията са за неправомерно предоставяне на лични данни на колекторски фирми за събиране на задължения от физическите лица, включително в хипотеза на изтекла давност, както и твърдения, свързани с употребата на лични данни за отпускане на кредити, без същите да са поискани и/или усвоени, особено такива, сключени в електронна среда посредством кандидатстване и отпускане на кредити по електронен път. Характерно за жалбите, подадени през 2024 г. в този сектор, са твърденията на жалбоподателите за неправомерно, без тяхно съгласие обработване на личните им данни в хипотезата на ежемесечно предоставяне в Централния кредитен регистър на Българската народна банка на информация за кредитната задлъжнялост на лицето и отразяването им в този регистър на банката.

Продължава тенденцията за увеличаване на броя на жалбите, подадени срещу физически лица – през 2024 г. достига до 83. Жалбите са предхождани от усложнени конфликтни отношения между страните и са насочени предимно срещу предоставяне в хода на образувани между страните съдебни производства документи, съдържащи лични данни, и разпространение на лични данни и коментари в социалните мрежи.

Отчита се и увеличение на броя на жалбите, подадени в сектор „Здравеопазване“. През 2023 г. броят им е 14, а през 2024 г. – 22. Основен предмет на жалбите са твърдения за предоставяне на трети лица на чувствителна информация, касаеща здравния статус на субекта на лични данни и злоупотреба с лични данни за предоставяне на здравни услуги, отчитане на хоспитализации и прегледи, без такива да са реално осъществени. Въпреки относително малкия брой жалби, предвид спецификата на дейността на администраторите в този сектор, а именно лечебни заведения, лекари на индивидуална практика, диагностично-консултативни центрове и лаборатории, и големия обем от данни, които се обработват, секторът е под особено наблюдение предвид обстоятелството, че се касае за обработване на специална категория лични данни, свързани със здравословното състояние на лицата.

Наблюдава се драстично повишаване на жалбите, подадени срещу медии – 22 за 2024 г., на фона на 10 жалби за 2023 г. Твърденията за нарушения в този сектор са предимно за непропорционално обработване на лични данни, разкриване на чувствителна информация, обработване на специални категории лични данни, най-вече такива, свързани със здравословното състояние, респективно здравния статус на субекта на данни, както и непроизнасяне по подадени от субекти на данни заявления за упражняване на „правото да бъдеш забравен“ или изричен отказ на администратора да удовлетвори исканията за заличаване на лични данни и преустановяване на тяхното разпространение.

През 2024 г. е констатирано драстично намаляване на броя на жалбите, подадени срещу политически субекти. Докато през 2022 г. броят на жалбите в този сектор са 68, през 2023 г. са 60, то през 2024 г. броят им намалява до 33, като следва да се отбележи, че през 2024 г. постъпват жалби и срещу политически субекти, срещу които до момента не е имало оплаквания по отношение на обработване на лични данни в изборния процес. Жалбите касаят предимно злоупотреба с лични данни на физическите лица чрез включването им в списък на лицата, подкрепящи регистрацията на политически субект за участие в изборния процес, както и злоупотреба с лични данни за регистриране на лица като членове на секционни избирателни комисии. Причина за по-малкия брой жалби в този сектор може да се търси в издадените от КЗЛД разпореждания до политическите субекти относно обработването на лични данни в изборния процес, както и в наложените имуществени санкции.

Наблюдава се и значително намаляване на жалбите, подадени в сектор „Трудови и осигурителни услуги“. Докато през 2023 г. техният брой е 28, през 2024 г. намалява до 11. Традиционно тези жалби касаят твърдения за злоупотреба с лични данни за регистрирани в НАП трудови договори, без такива да са сключвани. Сравнително константен е броят жалби подадени срещу администратори в телекомуникационен сектор – 51 през 2021 г., 49 през 2022 г., 46 през 2023 г. и 45 през 2024 г. Секторът вече не е сред водещите по брой подадени жалби, като за това допринасят и наложените от КЗЛД имуществени санкции, издадените разпореждания и въведените от телекомуникационните дружества

допълнителни технически и организационни мерки в процеса на обработване на лични данни.

С оглед крайното решение на КЗЛД произнасянията по жалби, разгледани през 2024 г., са: основателни (213 жалби), неоснователни (102 жалби), очевидно неоснователни (30 жалби), недопустими (42 жалби), нередовни (126 жалби), оттеглени (55 жалби).

От разгледаните през 2024 г. жалби преобладаващ е броят на констатираните нарушения на чл. 6, § 1 от ОРЗД – обработване на лични данни без правно основание, както и обработване на личните данни в нарушение на принципите по чл. 5, § 1 от ОРЗД – „законосъобразност и добросъвестност“, „свеждане на данните до минимум“, „цялостност и поверителност“ и „точност“.

Наложените през 2024 г. глоби и имуществени санкции в производството по чл. 38 от ЗЗЛД варират от 500 лв. до 70 000 лв. В процес на принудително събиране от НАП към 31.12.2024 г. са санкции, наложени с Решения на КЗЛД в производството по чл. 38 от ЗЗЛД, в размер на 927 227 лв. През 2024 г. е събрана сума в размер на 220 800 лв., в т.ч. платена по сметка на КЗЛД в размер на 202 000 лв. Санкциите, наложени с Решения на КЗЛД в процес на доброволно изпълнение, са в размер на 10 000 лв.

Постановените от КЗЛД решения по жалби подлежат на двуинстанционен съдебен контрол по АПК. Анализът на съдебната практика показва висок процент на потвърдени от съда решения на надзорния орган.

През 2024 г. първоинстанционният съд се произнася с решения по 86 дела, включително по такива, образувани и преди 2023 г. По 61 дела първоинстанционният съд потвърждава оспорените административни актове, постановени от КЗЛД, с 4 съдебни акта са частично изменени постановени от КЗЛД решения, включително в санкционната част, отменени на първа инстанция са 21 издадени от КЗЛД решения.

През 2024 г. ВАС се произнася с решения по 71 дела, в това число такива, образувани преди 2023 г., като потвърждава 47 издадени от КЗЛД индивидуални административни акта, 4 постановени от КЗЛД решения се изменят, като наложените от комисията санкции се намаляват, 13 решения на КЗЛД се отменят, като по 1 от тях преписката се връща за ново разглеждане от КЗЛД, по 3 решения на КЗЛД преписките се връщат за разглеждане на първа инстанция.

Основна част от контролната дейност на КЗЛД включва работата по сигнали и искания за упражняване на надзорни правомощия. През отчетната 2024 г. в КЗЛД постъпват сигнали и запитвания по актуални въпроси във връзка с обработването на лични данни и изложени твърдения за нарушения на Регламент 2016/679 и ЗЗЛД. Работено е по 680 сигнали и искания за упражняване на законоустановените надзорни правомощия, от които са приключени 593 бр., като 637 са от 2024 г. и останали от края на 2023 г. – 43 бр. сигнали. Изготвените и изпратени на сигналоподателите отговори са 593, а при необходимост от сигнализиране за наличие на данни и за други нарушения извън компетенциите на КЗЛД получените сигнали се изпращат и на други държавни органи или институции за произнасяне по компетентност.

Преобладаваща част от исканията и сигналите касаят незаконосъобразни практики на администраторите и/или неразбиране от страна на подателите на гарантираните им от Регламента права и реда за тяхното упражняване. Подадените сигнали и искания се отнасят преобладаващо до предоставяни интернет услуги и електронна търговия – 131 бр., видеонаблюдение – 87 бр., банково дело и кредитна дейност – 47 бр., директен маркетинг – 46 бр., следвани от сигнали за незаконосъобразно обработване на лични данни от администратори на лични данни в държавната администрация – 37 бр. Постъпват сигнали срещу администратори, обработващи лични данни в сферата на хазарта – 27 бр., както и такива в сферите на телекомуникациите – 25 бр., пощенски услуги – 24 бр., и в областта на производството, търговията и услугите – 24 бр.

Сигналите и исканията на българските граждани през 2024 г. са многобройни и разнородни по своето естество, като отразяват тревогите и проблемите в обществото. Немалка част от тях са породени и от личностни конфликти между физически лица или служител – работодател, ползватели на услуги и много други обществени отношения, пораждащи конфликти и напрежение при общуване и взаимодействие.

През 2024 г. продължава тенденцията за разглеждане на множество казуси, препратени по

компетентност от прокуратурата и от органите на МВР, когато е отказано образуване на наказателно производство поради липсата на достатъчно събрани доказателства за престъпление, но има събрани факти и твърдения за евентуално извършени административни нарушения в областта на защита на личните данни.

Комисията за защита на личните данни е независим надзорен орган и прилага механизъм за ефективен контрол в областта на защитата на личните данни чрез извършване на проверки на място на администраторите по подадени жалби и сигнали за незаконосъобразно обработване на лични данни на физически лица. Проверки се извършват след решения на Комисията, по доклади, съдържащи предложения за проверки в определени сектори, където се наблюдава засилен интерес и/или повишено подаване на жалби и сигнали и/или въвеждане на нови технологии и регистри, касаещи обработването на множество лични данни на физически лица. Проверки на място се извършват при констатиране на висок риск при постъпили уведомления за нарушаване на сигурността на основание чл. 33 от Регламент 2016/679, както и проверки, касаещи обработването на лични данни на физически лица в ШИС, ВИС, както и информационни системи, свързани с издаването на визи в консулски служби и посолства.

Общият брой назначени проверки за извършване на място през 2024 г. са 521 броя, от които 146 броя, назначени в края на 2023 г. Назначените през този период проверки на място по уведомления за нарушаване на сигурността на личните данни съгласно чл. 33 от Регламент 2016/679 с висок риск са 17 бр. През отчетния период изцяло приключили с констативен акт и решение на КЗЛД са 277 бр. (вкл. 14 проверки на място по линия на уведомления за нарушения на сигурността на личните данни), в т.ч. проверките от предходната 2023 г.

Най-голям е броят на извършените проверки с предмет видеонаблюдение – 218 бр. В сферата на търговията и услугите са извършени 23 бр. проверки, в сектор държавна администрация – 5 бр., здравеопазване – 5 бр., следвани от проверки в сферата на информационните технологии – 4 бр., образование и обучение – 4 бр., банково дело и кредитна дейност – 4 бр., областна и общинска администрация – 3 бр., хотелиерство и ресторантьорство – 2 бр., други – 9 бр.

Наложените от КЗЛД корективни мерки за констатирани нарушения след постъпили сигнали са 236 бр., от които 206 бр. разпореждания, 10 бр. официални предупреждения и 20 бр. предупреждения, основно за нарушение на чл. 32, § 1, букви „б“ и „г“ от Регламент (ЕС) 2016/679, чл. 6, § 1 букви „а – е“ от Регламент (ЕС) 2016/679, чл. 38, § 6 от Регламент (ЕС) 2016/679, чл. 25 „г“ от ЗЗЛД и чл. 25 „е“ от ЗЗЛД. Прави впечатление, че броят им е значително завишен спрямо 2018 г. (когато започна да се прилага Регламент (ЕС) 2016/679), когато те са общо 14 бр. За 9 бр. решения с издадени корективни мерки са наложени санкции в размер на 18 700 лв.

Въз основа на извършени проверки на място по сигнали за 2024 г. са съставени 5 бр. акта за установяване на административни нарушения, завършили с наказателно постановление (НП). Административнонаказателни производства, приключили със споразумения, са 4 бр. (платени доброволно). Наложените санкции с наказателни постановления са в размер на 15 500 лв., а наложени със споразумения са в размер на 40 500 лв. – платени доброволно. От издадените наказателни постановления 2023 – 2024 г. към края на отчетния период 10 бр. са обжалвани и са в съдебна фаза.

В процес на принудително събиране от НАП към 31.12.2024 г. са глоби и имуществени санкции, наложени с НП в размер на 163 840 лв. През 2024 г. е събрана сума в размер на 1 035 000 лв., в т.ч. платена по сметка на КЗЛД в размер на 1 021 800 лв. Няма глоби и имуществени санкции, наложени с НП в процес на доброволно изпълнение. Събраните суми от споразумения са в размер на 40 500 лв. През 2024 г. е осъществено процесуално представителство на 41 АНП пред РС, АССГ и ВАС. Спечелено е дело срещу банка на стойност 1 000 000 (един милион) лева.

За отчетния период в КЗЛД са получени общо 73 уведомления за нарушения на сигурността на данните, като се констатира многообразие на секторите от обществения живот, в които осъществяват дейност подалите уведомления администратори: от тях държавни институции – 3 бр., банки – 2 бр., болници и лечебни заведения – 3 бр., съдилища – 2 бр., местно самоуправление – 2 бр.; за 7 от случаите прави впечатление, че основното място на установяване на администратора е САЩ. Анализът на натрупаните данни по отношение на преценения риск за правата и свободите на засегнатите от

нарушенията субекти на данни през годините сочи, че през отчетния период има значително увеличение на случаите, при които рискът за засегнатите от нарушенията физически лица е висок.

Най-голям процент са случаите на инциденти, свързани с външни злонамерени атаки към системите на администраторите, представляващи различни по вид киберпрестъпления, включително кражби или криптиране на бази данни, съдържащи лични данни, за което са уведомени и съответните правоохранителни органи – 84%. На следващо място, с 11% са инцидентите, свързани с разкриването на данни пред трети лица вследствие на неволни технически грешки, предизвикани от човешки фактор. В 5% от случаите нарушенията се причиняват от злоупотреба със служебно положение.

В изпълнение на задачата си да дава становища по проекти на нормативни актове или регулаторни мерки, имащи отношение към обработването на лични данни и през 2024 г. КЗЛД изразява 15 становища по приложението на законодателството за защита на личните данни, включително по 7 съгласувателни процедури по Устройствения правилник на Министерския съвет и на неговата администрация и 3 искания от Народното събрание по предложение за нормативен акт. През отчетната година КЗЛД изразява становища по четири преюдициални запитвания, които са предложени и приети като част от формиране на позицията на Република България пред Съда на ЕС.

През 2024 г. КЗЛД предоставя множество писмени консултации – 336 бр. (вкл. становищата, посочени по-горе). Същите се отнасят до разяснения в правната уредба, по които има ясна и еднозначна регламентация и/или трайна практика на надзорния орган, вкл. по линия на запитвания на физически лица и администратори на лични данни по различни въпроси, свързани с техните права и задължения в областта на защитата на личните данни.

По линия на международната дейност се реализира активно участие както във форматите за защита на личните данни, така и в тези за защита на лицата, подаващи сигнали или публично оповестяващи информация за нередност. През 2024 г. приоритет остава организацията на участието във всички международни формати, обединяващи сродни органи по защита на данните, които са провеждали онлайн заседания или в рамките на които е обменена интензивна кореспонденция по актуални теми. Тъй като по-голямата част от заседанията по международна линия продължават да се провеждат дистанционно, създават се условия за активно участие в реално време в по-голям от очаквания брой международни мероприятия в сферата на защитата на личните данни. В резултат на тази активна международна дейност се изразяват позиции (121 бр.), осъществява се участие в различни международни инициативи и в заседания (217 бр.), подготвени са отговори на чуждестранни запитвания (172 бр.) и се реализира участие в механизма за сътрудничество и съгласуваност чрез Информационната система на вътрешния пазар (120 бр.) – общо 630 бр. Отчетени са дейности по Шенген (проверки, разяснителна кампания и упражняване на правата от субектите на данни), като и по присъединяване на Република България към Организацията за икономическо сътрудничество и развитие (ОИСР). В контекста на вменените ѝ задължения по Закона за защита на лицата, подаващи сигнали или публично оповестили информация за нарушения (ЗЗЛПСПОИН), през отчетния период продължават последователните действия за международното утвърждаване в тази област на компетентност на КЗЛД.

През 2024 г. продължават усилията на КЗЛД по финализиране на национално правната рамка за защита на сигнализиращите лица и за създаване на условия за ефективно изпълнение на задачите ѝ като централен орган за външно подаване на сигнали и за защита на сигнализиращите лица по ЗЗЛПСПОИН. В Годишния отчет за 2024 г. е предоставена статистическа информация относно постъпилите сигнали при условията и по реда на ЗЗЛПСПОИН, относно взаимодействието с компетентните органи по чл. 20 от ЗЗЛПСПОИН, взаимодействието със задължените субекти по чл. 12 от ЗЗЛПСПОИН, както и статистическа информация, предоставяна на Европейската комисия. Представени са резултатите от външния одит, осъществен от омбудсмана на Република България на основание чл. 30, ал. 1 и 2 от ЗЗЛПСПОИН, обучителните инициативи по приложението на ЗЗЛПСПОИН, както и сътрудничеството с неправителствения сектор.

В своя отчет за 2024 г. КЗЛД предоставя информация за дейността си като наблюдаващ орган

относно сигурността на данните съгласно Закона за електронните съобщения, като предоставя статистика и анализ на исканията за достъп до трафични данни и на получените протоколи за унищожени трафични данни.

В изпълнение на задължението за поддържане на публичен регистър на администраторите и обработващите, които са определили длъжностни лица по защита на данните, за 2024 г. се отчита извършването на 434 регистрации, с което общият им брой става 6109.

В изпълнение на изискванията по Закона за достъп до обществена информация в Годишния отчет е включен Отчет за постъпилите заявления за достъп до обществена информация и искания за повторно използване на информация от обществеността за 2024 г. Посочено е, че на всички граждани и организации, заявили достъп до обществена информация, е предоставена такава през 2024 г. в законовия срок.

В отчета е предоставена подробна информация за институционалното взаимодействие, информационно-образователната дейност, медийната политика, административния капацитет и финансовото състояние на КЗЛД. Отражено изпълнението на целите на КЗЛД чрез реализация на проекти с национално и международно финансиране, както и подготовката на нови проектни предложения.

Предоставена е информация относно разходването на бюджета на КЗЛД през 2023 г. Със Закона за държавния бюджет на Република България за 2024 г. се утвърждава бюджетът за дейността на КЗЛД в размер на 5 808 900 лв. във функционална област „Защита на личните данни на физическите лица“. През годината по него се извършват корекции: увеличение на капиталовите разходи общо със 169 900 лв. в изпълнение на разпоредбите на ПМС № 57/21.03.2024 г. и ПМС № 107/23.04.2024 г. за одобряване на допълнителни разходи/трансфери по бюджетите на първостепенните разпоредители с бюджет за 2024 г.; увеличение на разходите за персонал с 274 603 лв. в изпълнение на разпоредбите на ПМС № 135/29.04.2024 г. за одобряване на допълнителни разходи по бюджета на КЗЛД за 2024 г. за преодоляване на диспропорции във възнагажденията на персонала; увеличение на разходите за издръжка със 150 000 лв. в изпълнение на разпоредбите на ПМС № 338/04.10.2024 г. за одобряване на допълнителни разходи по бюджета на КЗЛД за 2024 г. След извършените промени утвърденият бюджет на КЗЛД за 2024 г. е в размер на 6 403 403 лв. За обезпечаване на дейността на Комисията за защита на личните данни и нейната администрация са извършени разходи общо в размер на 6 198 880 лв., или 96,81% от утвърдените разходи за годината.

В края на годишния си отчет КЗЛД формулира следните цели и приоритети за 2025 г.:

- Приемане на Стратегия на КЗЛД за развитие в областите на защитата на личните данни и на защитата на лицата, подаващи или оповестяващи сигнали за нарушения (Хоризонт 2025 – 2030).
- Продължаване на усилията на КЗЛД за членство на Република България в ОИСР.
- Изграждане на подход за защитата на личните данни, свързан с предизвикателствата от развитието на темата на общоевропейско ниво.
- Завишена защита на личните данни на децата с цел гарантиране на техните права и свободи в онлайн средата.
- Извършване на секторни проверки.
- Целенасочена политика за повишаване на осведомеността на сигнализиращите лица и задължените субекти по ЗЗЛПСПОИН.
- Засилване на административния капацитет на институцията.
- Подготовка за мисия по оценка на достиженията на правото на Шенген.

Годишният отчет на КЗЛД за 2024 г. е публикуван на институционалния сайт – **ТУК**.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ

През март и април 2025 г. се проведеха 103-то и 104-то пленарни заседания на Европейския комитет по защита на данните (ЕКЗД). По време на пленарните заседания ЕКЗД прие ключови документи, свързани с прилагането на Директивата за резервационните данни на пътниците (PNR) и обработването на лични данни чрез блокчейн технологии. И двете теми са от съществено значение за практическото прилагане на Общия регламент относно защитата на данните (ОРЗД) в контекста на новите технологии и мерки за сигурност.

Насоки относно прилагането на PNR Директивата

На заседанието си от 13 март 2025 г. ЕКЗД прие второ становище относно прилагането на Директивата за резервационните данни на пътниците (PNR), в светлината на решението на Съда на Европейския съюз по дело C-817/19. Становището е насочено към звената за информация за пътниците (PIUs), като дава допълнителни насоки относно необходимите адаптации и ограничения при обработването на PNR данни.

PNR данните включват имена на пътници, дати на пътуване, маршрути, места в самолета, багаж, данни за контакт и начини на плащане. ЕКЗД подчертава, че срокът за съхранение на всички PNR данни не бива да надвишава първоначален период от шест месеца. След изтичането му, данните могат да се съхраняват, само ако това е необходимо и пропорционално на целите на директивата.

Становището включва и практически препоръки към националните законодателства с цел те да отразят в пълна степен решенията на Съда на ЕС, включително по въпроси като критериите за подбор на полетите, от които се събират PNR данни.

Председателят на ЕКЗД Ану Талус подчерта: „ЕКЗД признава значението на PNR Директивата за подобряване на сигурността на пътниците в Европа и за предотвратяване и разследване на терористични престъпления. Прехвърлянето на PNR данни в рамките на ЕС трябва да се извършва по хармонизиран начин и в пълно съответствие с принципите за защита на данните.“

Въпреки че някои държави членки вече са започнали процеса на адаптация, Комитетът отбелязва, че все още липсват достатъчно усилия за реално изпълнение на решението и настоява за бързи законодателни промени.

Насоки относно обработването на лични данни чрез блокчейн технологии

На 8 април 2025 г., по време на своето 104-то заседание, ЕКЗД прие нови насоки относно обработването на лични данни чрез технологии, базирани на блокчейн. Блокчейнът представлява децентрализиран дигитален регистър, който се използва за потвърждаване на транзакции и собственост, както и за осигуряване на проследимост и неизменност на данни.

ЕКЗД счита, че с оглед на нарастващото използване на блокчейн технологии, е необходимо да се подпомогнат организациите, така че те да гарантират съответствие с ОРЗД. Насоките разясняват различните архитектури на блокчейн системи и техните последици върху обработването на лични данни.

Ключови акценти от насоките:

- Принципи на защита на данните по дизайн – техническите и организационни мерки трябва да се прилагат още на етапа на проектиране на обработването;
- Ясно дефиниране на ролите и отговорностите на участниците – при проектирането на системите следва да се определи кой е администратор или обработващ;
- Оценка на въздействието (ОВЗД) – в случаите на висок риск за правата и свободите на физическите лица, следва да се извършва предварителна оценка;
- Избягване на съхранение на лични данни в блокчейн – препоръчва се съхраняването на лични данни "off-chain", за да се предотврати неограничен достъп;
- Гарантиране на права като прозрачност, коригиране и изтриване на данни – организациите

трябва да осигурят възможност за упражняване на тези права, дори при използване на децентрализирани технологии.

Насоките ще подлежат на обществено обсъждане до 9 юни 2025 г., като всички заинтересовани страни могат да представят своите коментари чрез [сайта на ЕКЗД](#).

В допълнение, Комитетът заяви готовност за тясно сътрудничество с новосъздадения AI Office във връзка с разработването на бъдещи насоки относно взаимодействието между Акта за изкуствения интелект и законодателството за защита на данните в ЕС.

ЕКЗД ПРИЕ ИЗЯВЛЕНИЕ ОТНОСНО ПРИЛАГАНЕТО НА ДИРЕКТИВАТА ЗА РЕЗЕРВАЦИОННИТЕ ДАННИ НА ПЪТНИЦИТЕ

По време на пленарното си заседание през март 2025 г. Европейският комитет по защита на данните (ЕКЗД) прие [изявление относно прилагането на Директивата за резервационните данни на пътниците \(PNR\) в контекста на решение C-817/19 на Съда на ЕС \(CEC\)](#).

Във второто си изявление относно прилагането на Директивата за резервационните данни на пътниците, което следва изявлението от 15 декември 2022 г., Комитетът дава допълнителни насоки на звената за информация за пътниците (ЗИП) относно необходимите адаптации и ограничения при обработването на резервационните данни на пътниците след решението по делото. PNR данните са лична информация, предоставена от пътниците и събирана и съхранявана от въздушните превозвачи, която включва имената на пътниците, датите на пътуването, маршрутите, местата, багажа, данните за контакт и начините на плащане.

Изложението включва практически препоръки за националните законодателства, транспониращи [Директивата за резервационните данни на пътниците](#), за да се приведат в действие заключенията на Съда на ЕС в решението по делото PNR. Препоръките обхващат някои от ключовите аспекти на решението относно резервационните данни на пътниците, като например как европейските държави следва да избират полетите, от които се събират резервационни данни на пътниците, или колко дълго следва да се съхраняват тези данни. Според Комитета периодът на запазване на всички PNR данни не следва да надвишава първоначален период от шест месеца. След изтичането на този период европейските държави могат да съхраняват резервационни данни само толкова дълго, колкото е необходимо и пропорционално на целите на Директивата за резервационните данни на пътниците.

Председателят на ЕКЗД Ану Талус заяви: „ЕКЗД признава значението на Директивата за резервационните данни на пътниците за подобряване на сигурността на пътниците в Европа и за подпомагане на предотвратяването, разкриването и преследването на терористични престъпления и тежки престъпления. Предаването на резервационни данни на пътниците в Европа следва да се извършва по хармонизиран начин и при пълно спазване на принципите за защита на данните.“

Комитетът е наясно, че някои европейски държави вече са започнали процеса на адаптиране, но все още липсват значителни усилия за прилагане във всички държави членки. Ето защо в своето изявление ЕНОЗД изтъква спешната необходимост да се приложат необходимите промени и да се изменят националните закони, като се вземе предвид решението по делото за резервационните данни на пътниците във възможно най-кратък срок.

ГОДИШЕН ДОКЛАД НА ЕКЗД ЗА 2024 Г.: ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДИНАМИЧНАТА ДИГИТАЛНА СРЕДА



На 23 април 2025 г. Европейският комитет по защита на данните (ЕКЗД) публикува своя годишен доклад за 2024 г., в който се отразяват основните дейности на Комитета през изминалата година. Докладът обобщава ключовите постижения, включително приемането на новата стратегия за периода 2024–2027 г., значителното увеличение на консултативните

становища по чл. 64, ал. 2 от Общия регламент за защита на данните (ОРЗД) и усилията за предоставяне на насоки и правна помощ.

Председателят на ЕКЗД, Ану Талус, подчерта: „През 2024 г. затвърдихме нашия ангажимент към основните права на гражданите в областта на личната неприкосновеност и защитата на данните, като продължихме да играем централна роля в осигуряването на последователно прилагане на ОРЗД в ЕС. Освен това разширихме нашите инициативи за повишаване на информираността сред бизнеса и широката общественост, включително и по отношение на новите цифрови регулации.“

Нова стратегия 2024–2027

Стратегията на ЕНОЗД очертава приоритетите за засилване и модернизиране на защитата на данните, осигуряване на еднакво прилагане на ОРЗД в държавите членки и справяне с нововъзникващи предизвикателства, включително чрез сътрудничество между различни регулаторни органи. Комитетът цели и засилено глобално присъствие чрез активно участие във водещи международни форуми.

Насоки и правна експертиза

През 2024 г. ЕКЗД прие осем становища по чл. 64, ал. 2 от ОРЗД по теми като „съгласие или плащане“ при онлайн платформи, използването на лицево разпознаване на летища и обработването на лични данни за обучение на AI модели. Също така бяха приети четири нови насоки, сред които по темите за „легитимен интерес“ и за трансфери на данни към трети страни.

Активна комуникация с заинтересовани страни

Комитетът засили диалога със заинтересованите страни чрез обществени консултации и събития, посветени на предстоящи насоки и становища. Това насърчава по-голямо разбиране и участие от страна на индустрията, академичните среди и гражданския сектор.

Сътрудничество в контекста на новото цифрово законодателство

Във връзка с прилагането на новите европейски актове – като Акта за цифровите пазари, Акта за цифровите услуги, Акта за управление на изкуствения интелект и др. – ЕКЗД активно участва в междуинституционално сътрудничество с цел осигуряване на съответствие с разпоредбите на ОРЗД.

По-достъпна информация за ОРЗД

През 2024 г. Комитетът предприе стъпки за улесняване разбирането на ОРЗД чрез създаване на ръководства, адаптирани за малки предприятия и за неспециалисти. Наръчникът за защита на личните данни за малкия бизнес вече е достъпен на 18 езика, а кратките резюмета на насоките улесняват достъпа до най-важната информация.



ЗАПОЧВА КООРДИНИРАНО ДЕЙСТВИЕ ПО ИЗСЛЕДВАНЕ НА ПРИЛОЖЕНИЕТО НА ПРАВОТО НА ИЗТРИВАНЕ (ПРАВО „ДА БЪДЕШ ЗАБРАВЕН“).



Европейският комитет по защита на данните стартира действията по изпълнение на Рамката за координирано правоприлагане за 2025 г. Това е четвъртата годишна инициатива, чиито цели включват сътрудничество между органите за защита на данните, членове на ЕКЗД. Тази година фокусът на Рамката се измества върху прилагането на друго право на субектите на данните, а именно правото на изтриване или „правото да бъдеш забравен“ (член 17 от ОРЗД). Изборът ѝ е свързан с факта, че то е едно от най-често упражняваните права от субектите

на данни, както и едно от правата, за които органите за защита на данните получават много жалби.

Това право позволява на субектите на данни да поискат изтриване на личните си данни, когато те вече не са необходими, обработват се незаконосъобразно или са оттеглили съгласието си, като това право е свързано с членове 6 (законосъобразност на обработването), 7 (условия за съгласие) и 21 (право на възражение).

Комисията за защита на личните данни се присъединява към инициативата, заедно с други европейски регулатори в рамките на координираното правоприлагане, за да проучи до каква степен администраторите спазват разпоредбите на законодателството, свързани с упражняване правото на изтриване. КЗЛД публикува [АНКЕТА](#) на български език до администраторите и обработващите лични данни в публичния и в частния сектор. Целта на проучването е запознаване с действията и тенденциите в прилагането на [чл. 17 от ОРЗД \(Право на изтриване на лични данни\)](#).

Анкетата се попълва анонимно и доброволно от администратори чрез онлайн системата „EUSurvey“ до 30 юни 2025 г. Тя няма да се използва за събиране на лични данни, нито за осъществяване на надзорна и контролна дейност.

Анализирането се извършва с цел по-добро общо разбиране на средата и възможност за подпомагане на организациите да прилагат на практика правото на изтриване и за упражняването на правата на физическите лица. Резултатите от това координирано действие ще бъдат обобщени, за да се получи широк преглед и да се даде възможност за специфичен мониторинг на ниво ЕС и ЕИП. Накрая, след приключване на действията, Европейският комитет по защита на данните ще публикува доклад за резултатите от всички участващи държави.

Публична информация за инициативата и публикациите на участващите надзорни органи може да видите на сайта на Европейският комитет по защита на данните. CEF 2025: Launch of coordinated enforcement on the right to erasure

Забележка: Системата „EUSurvey“ се поддържа от Европейската комисия. Политиката за

обработване на лични данни и бисквитки може да достъпите на следните линкове: Privacy notice / Cookies.

КЗЛД ПРОВЕДЕ ФОРУМ ЗА ВЪЗМОЖНОСТИТЕ ПРЕД ДЪРЖАВАТА И БИЗНЕСА ПРИ ПРИЕМАНЕТО НА БЪЛГАРИЯ В ОИСР



На 28 март 2025 г. в хотел „Хилтън“ в София се проведе форум, организиран от Комисията за защита на личните данни (КЗЛД), на който се обсъдиха възможностите и предизвикателствата пред България при приемането ѝ за пълноправен член на Организацията за икономическо сътрудничество и развитие (ОИСР). Събитието бе открито от министъра на правосъдието Георги Георгиев и председателя на КЗЛД Венцислав Караджов, а сред

участниците бяха представители на водещи институции и държавни агенции, както и представители на бизнеса и неправителствения сектор.

Целта на форума беше да се разгледат възможностите и предизвикателствата пред България при приемането ѝ за пълноправен член на ОИСР, което се очаква да се случи през 2027 г. Представители на Министерския съвет, Министерството на правосъдието, Министерството на здравеопазването, Министерството на електронното управление, както и представители на неправителствения сектор обсъдиха възможните ползи от членството в най-престижния световен икономически съюз и неговото значение за устойчивото развитие на страната.

В допълнение към обсъждането на икономическите и политическите предимства на членството в ОИСР, КЗЛД акцентира на важността на защита на личните данни и защита на сигнализиращите лица. Темите бяха представени в контекста на добрите практики и мерки, които ще бъдат приложени при процеса на присъединяване на България към ОИСР.

По време на форума беше представено и окончателното предложение за наръчника с добри практики, представляващ доброволен инструмент, който може да се използва от България и бъдещите страни, кандидати за членки в процеса на присъединяване към ОИСР. Отдалечено участие във форума осъществи и представител на ОИСР - Лимър Шмерлинг Магазаник. Тя е израелски адвокат и съветник по

управление на данни, поверителност, етика на изкуствен интелект и политика за киберсигурност.

Организацията за икономическо сътрудничество и развитие е създадена през 1961 г. и играе ключова роля в глобалната икономика, като координира политиките на своите членове в области като управление, данъчна политика, транспортна инфраструктура, селско стопанство, образование, дигитална икономика, иновации и климат. Членството в ОИСР ще постави България на картата на световната икономика и ще осигури нови възможности за устойчиво икономическо развитие.



Събитието беше важен етап в подготовката на България за пълноправно членство в ОИСР и продължава активния процес на обмен на добри практики

и знания в подкрепа на модернизацията на страната.



ПОТЕНЦИАЛНИ ЗАПЛАХИ ЗА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ В КОНТЕКСТА НА ПРЕДЛОЖЕНИЕТО ЗА РЕГЛАМЕНТ CSAM

През 2022 г. започна законодателният процес по изготвяне и приемане на предложението за Регламент на Европейския парламент и на Съвета за определяне на правила за предотвратяване и борба със сексуалното насилие над деца (CSAM). До текущия момент са преминали няколко ключови етапа. На 11 май 2022 г. Европейската комисия представи предложението за Регламент, насочен към предотвратяване и борба със сексуалното насилие над деца, както онлайн в дигиталната среда, така и извън нея. На 16 ноември 2023 г. Европейският парламент прие позицията си по предложението, като даде възможност за започване на междуинституционални преговори. На 13 декември 2024 г. министрите на правосъдието от ЕС постигнаха обща позиция по директивата по време на заседание на Съвета по правосъдие и вътрешни работи в Брюксел. В рамките на заседанието, някои държави членки са изразили загриженост относно определенията за съгласие и квалификацията на изнасилването, като са поискани по-ясни разпоредби за защита на малолетните и непълнолетните лица.

На 20 декември 2023 г. посланиците на държавите – членки на ЕС, постигнаха съгласие по мандата на Съвета за водене на преговори за Регламент за удължаване на срока на действие на временна мярка за борба със сексуалното насилие над деца онлайн. Тази временна мярка, която първоначално трябваше да изтече на 3 август 2024 г., е удължена до 3 август 2027 г., за да се даде възможност за продължаване на доброволното откриване и докладване от страна на доставчиците на услуги, докато бъде финализиран постоянният регламент. От февруари 2025 г. предложението е в процес на тристранни преговори между Европейския парламент, Съвета и Европейската комисия. Целта е да се съгласуват различните позиции и за да се създаде стабилна правна рамка, която ефективно да се занимава със борбата срещу сексуалното насилие над деца, като същевременно се защитават основните права.

Регламентът има за цел да наложи конкретни задължения на доставчиците на хостинг услуги, услуги за междуличностна комуникация, магазини за софтуерни приложения, услуги за достъп до интернет и други съответни субекти. Тези задължения включват откриване, докладване, премахване и блокиране на известни и нови онлайн материали, съдържащи сексуална злоупотреба с деца, както и справяне с подмамването на деца. За да се улеснят тези усилия, в предложението се предвижда и създаването на център на ЕС за борба с материалите, съдържащи сексуално насилие над деца. През 2022 г. Европейският комитет по защита на данните (ЕКЗД) и Европейският надзорен орган по защита на данните (ЕНОЗД) направиха оценка на предложението на Европейската комисия за CSAM Регламент. В резултат на оценката те изкарват съвместно становище 04/2022, прието на 28 юли 2022 г., в което те посочват значението на усилията за справянето със сексуалното насилие над деца, но изразяват значителни опасения относно потенциалното въздействие на предложението върху основните права.

Основни опасения, изтъкнати от ЕКЗД и ЕНОЗД включват:

- Генерализиран и безразборен преглед: Предложението би могло да доведе до широкообхватен преглед на всички видове електронни съобщения, което потенциално нарушава правата на физическите лица на неприкосновеност на личния живот и защита на данните;
- Ефективност и точност на технологиите за откриване: Надеждността на технологиите, предназначени за откриване на нови материали, съдържащи сексуално насилие над деца, е съмнителна, като процентите грешки биха могли да доведат до фалшиви положителни резултати, като по този начин биха могли да бъдат засегнати невинни лица;
- Въздействие върху поверителността на съобщенията: Прилагането на такива мерки може да застраши поверителността на съобщенията, включително тези, които са криптирани, което потенциално подкопава сигурността канали за комуникация;
- Правна неяснота и непоследователно прилагане на основните права: Предложението съдържа неясноти, които биха могли да доведат до непоследователно прилагане и потенциални конфликти с основните права, залегнали в правото на ЕС.

Предложението на Европейския съюз за Регламент за определяне на правила за предотвратяване и борба със сексуалното насилие над деца предизвиква редица реакции от страна на законодатели и политици в цяла Европа. Сред изразилите положителни до момента позиции са Съвет на Европейския съюз, който показва силна подкрепа за предложението, като подчертава необходимостта от актуализиране на правните рамки за справяне с променящите се заплахи. Позицията на Съвета включва разширяване на определението за престъпления, така че да обхване възникващи въпроси като излъчване на живо по интернет (streaming) и материали, генерирани от изкуствен интернет (ИИ), увеличаване на наказанията за нарушителите и укрепване на механизмите за подкрепа на жертвите.

Сред най-големите противници на досегашните и текущият вариант на предложението за Регламент са някои от членовете на Европейския парламент. В своите позиции, те посочват, като основни предизвикателства:

- масовото наблюдение и фалшиви положителни резултати, като подчертават, че настоящите алгоритми за контрол на комуникациите не са ненадеждни, което води до значителен брой фалшиви положителни резултати.
- въздействие върху криптирането и сигурността на устройствата, като предупреждават, че предложението може да подкопае сигурното криптиране, като компрометира безопасността на устройствата и комуникациите на потребителите. Те подчертават, че поддържането на криптиране на високо ниво е от съществено значение за защитата на личните данни и за гарантиране на киберсигурността.
- ограничения за достъпа на непълнолетните до приложения. Предложението за Регламент включва мерки, които биха попречили на потребителите на възраст под 16 години да инсталират общи мобилни приложения, с цел да ги предпазят от сприяеляване с потенциално опасни потребители.
- забрана на анонимните съобщения. Изразява се загриженост относно разпоредби, които биха забранили на потребителите да създават анонимни имейл акаунти, без да представят идентификация. Той твърди, че това би попречило на чувствителните комуникации, като например тези, свързани със сексуалността, подаването на сигнали за нередности или политическата активност, където анонимността е от решаващо значение.

Въпреки че съществува консенсус относно необходимостта от борба със сексуалното насилие над деца, предложените методи предизвикаха дебат между европейските законодатели и политици. Поддръжниците подчертават необходимостта от съгласувана правна рамка и солидни инструменти, докато критиците подчертават потенциалните рискове за неприкосновеността на личния живот и призовават за по-ясни определения и по-строги превантивни мерки.

ИНФОРМАЦИЯ ЗА СТАНДАРТНИТЕ ДОГОВОРНИ КЛАУЗИ

Европейската комисия има правомощия да приема стандартни договорни клаузи (СДК), които да предлагат подходящи гаранции за защита на данните при тяхното предаване в трети страни, съгласно чл. 46, параграф 2, точка (в) от Регламент (ЕС) 2016/679 (ОРЗД).

Дали трансферът на лични данни въз основа на СДК може да бъде осъществен или не зависи от резултатите, от извършеният от администратора анализ на съпоставимото ниво на защита. СДК заедно с възможните допълнителни мерки, ще трябва да гарантират, че правото на САЩ (или трета страна) осигуряват съпоставимо ниво на защита.

На 4 юни 2021 г. Европейската комисия прие решение за изпълнение относно модернизираните стандартни договорни клаузи съгласно Регламент (ЕС) 2016/679 за трансфери на данни от администратори или обработващи лични данни в ЕС/ЕИП на администратори или обработващи лични данни, установени извън ЕС/ЕИП. Комисията също така прие решение за изпълнение относно стандартни договорни клаузи за трансфери на лични данни на трети държави съгласно Регламент (ЕС) 2016/679. Европейският комитет по защита на данните (ЕКЗД) осъществява оценка на решението и предоставя допълнителни разяснения за заинтересованите страни, както и насоки за използването на инструментите за предаване на лични данни на трети държави в съответствие с решението “Schrems II”. СДК по Регламент (ЕС) 2016/679 заменят предходно прилаганите съгласно Директива 95/46/ЕО.

Европейският комитет взема предвид първоначалната отговорност на износителя и вносителя, когато се извършва преценка относно необходимостта от сключване на СДК: следва да се гарантира, че тези клаузи осигуряват съпоставимо ниво на защита, гарантирана от ОРЗД. Когато извършва такава предварителна оценка, износителят (при необходимост със съдействието на вносителя) следва да вземе предвид съдържащата се в СДК уредба, конкретните обстоятелства на трансфера, както и правната уредба, която се прилага в държавата на вносителя. Износителят може да прецени, че е необходимо да въведе допълнителни мерки, които са извън предвидените в СДК.

ЕКЗД отбелязва също така задълженията на компетентните надзорни органи да спрат или забранят предаването на данни към трета държава, основаващо се на СДК, когато с оглед на всички обстоятелства във връзка с това предаване компетентният надзорен орган счита, че тези клаузи не са или не могат да бъдат спазени в третата държава и когато защитата на предаваните данни не може да бъде осигурена с други средства. И по-специално, когато самият администратор или обработващ лични данни все още не е прекратил предаването.

След решението на СЕС по дело Schrems II, ЕКЗД публикува препоръки за допълнителни мерки при трансфери на данни:

- Оценка на законодателството в приемащата държава – дали властите имат достъп до личните данни без достатъчни гаранции.
- Допълнителни технически мерки – криптиране, анонимизация, разделяне на данните.
- Организационни и договорни мерки – вътрешни политики за сигурност, ангажименти за защита от страна на получателите.
- Постоянен мониторинг – организациите трябва да следят правната среда в третите държави.

На 10 юли 2023 г. Европейската комисия приема решение за адекватност относно Рамката за защита на личните данни между ЕС и САЩ. Тази рамка въвежда нови гаранции:

- Достъпът до данни от американските разузнавателни служби е ограничен до необходимото и пропорционалното.
- Създаден е независим механизъм за разглеждане на жалби на граждани на ЕС.
- Възползват се всички организации, участващи в рамката, независимо от използвания механизъм за трансфер (СДК, задължителни фирмени правила и др.).

Практика на Съда на ЕС във връзка със СДК, по делото Schrems I (C-362/14) – през 2015 г. води до анулиране на рамката „Safe Harbour“, защото САЩ не гарантират адекватна защита на данните. По делото Schrems II (C-311/18) – през 2020 г. рамката „Privacy Shield“ е обявена за невалидна, но СДК остават валидни, като се въвежда изискване да се подкрепят с допълнителни мерки. По делото T-354/22 – Съдът потвърждава, че администраторите са длъжни да правят индивидуални оценки на рисковете при трансфери.

ПРЕДСТОЯЩИ ДЕЙНОСТИ ПО ПРОЕКТ OPWHI



През месец юни 2025 г. предстои да се проведе третата международна среща по изпълнението на проект „OPWHI – Open the Whistle: Protecting Whistleblowers Through Transparency, Cooperation and Open Government Strategies“ по програмата „Граждани, равенство, права и ценности“ на Европейския съюз.

В рамките на срещата ще бъде завършен Инструментът за почтеност в подаването на сигнали за нередности, по който ще бъде публикуван наръчник включващ, както разяснения, така и най-добри практики, които могат да бъдат заимствани от организациите в публичния и частния сектор в тяхната дейност в сферата на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения.

Наръчникът ще обхваща теми, свързани с осигуряването на прозрачност и добра комуникация на системите за докладване, похватите за правилно разследване и управление в рамките на вътрешните системи за подаване на сигнали за нередности, осигуряването на адекватно ниво на защита на данните, защита и подкрепа на лицата, сигнализиращи за нередности, както и препоръки относно измерването и оценката на ефективността на дадена система и оценка на създаването на култура на подаване на сигнали за нередности.

Освен завършването на наръчника, по време на срещата ще започне подготовката за осъществяване на заложените в проекта обучителни програми за специализирано обучение, включително подход за обучение на обучаващи, адаптиран за националните и регионалните органи, държавните служители и частните организации, участващи в прилагането на Директива (ЕС) 2019/1937. Същите ще бъдат реализирани до края на изпълнението на проекта.

Във връзка с тези проектни инициативи се засилват и дейностите по разпространение на резултатите и разработените материали по проекта. С публикуването на наръчника ще продължи и комуникационна кампания, в рамките на която ще бъдат адресирани потребностите на задължените лица по Директива (ЕС) 2019/1937 и по Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Кампанията действа като основа за популяризирането на обучителните програми по проекта и тяхното успешно и ефективно провеждане.

Проект „OPWHI – Open the Whistle: Protecting Whistleblowers Through Transparency, Cooperation and Open Government Strategies“ съфинансиран по програмата „Граждани, равенство, права и ценности“ на Европейския съюз с номер на договор 101140801 – OPWHI – CERV-2023-CHAR-LITI.

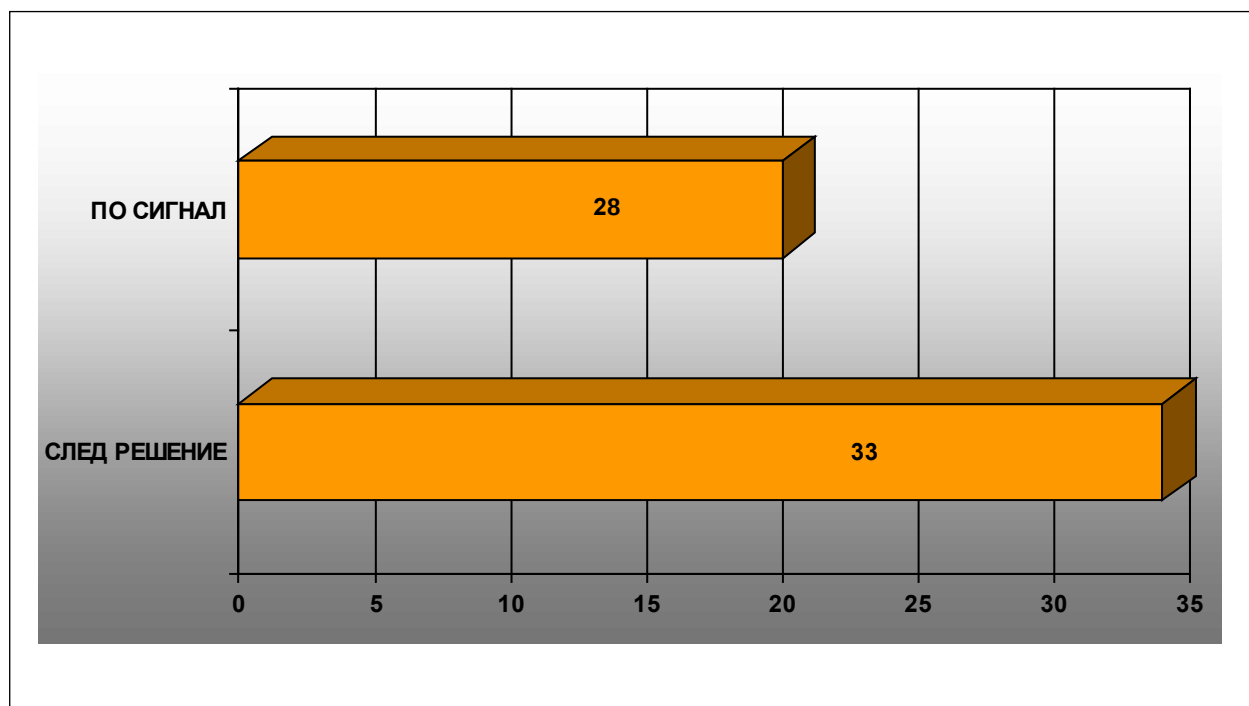


Съфинансирано от Европейския съюз

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАРТ-АПРИЛ 2025 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета за м. март и април 2025 г. са извършени общо 61 проверки - 28 след постъпили в КЗЛД сигнали и 33 след решение на КЗЛД.



Разгледани са 104 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 издадени 17 Разпореждания, отправени са 3 Предупреждение, 1 Официално предупреждение, съставени са 2 Акта за установяване на административно нарушение и е издадено 1 Наказателно постановление.

СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № ПНМД-01-24/2025 г. гр. София, 13.03.2025 г.

ОТНОСНО: Обмен на данни по Закона за защита от домашното насилие

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 12.03.2025 г., разглежда писмо с вх. № ПНМД-01-24/14.02.2025 г. от министъра на вътрешните работи, с което се отправя искане за изразяване на становище по въпроси, свързани с приложението на Закона за защита от домашното насилие (ЗЗДН). От МВР посочват, че с промените в ЗЗДН (обн. в ДВ., бр. 66 от 2023 г.) е предвидено създаването на Национален съвет за превенция и защита от домашно насилие (НСПЗДН), като в чл. 6а, ал. 2 е регламентирано, че „Националният съвет е специализиран постоянно действащ колективен и консултативен орган за осъществяване на държавната политика по превенция и защита от домашното насилие чрез координация, наблюдение и оценка на политиките и мерките за предотвратяване и защита от домашното насилие“. В чл. 6б, т. 6 от същия закон е посочено, че НСПЗДН: „създава и поддържа национална информационна система за случаите на домашно насилие, осъществени на територията на страната, или по отношение на български граждани в чужбина, които са потърсили помощ и подкрепа, и списък на юридическите лица, които осъществяват дейности по превенция и защита от домашното насилие по реда на този закон, при спазване на изискванията на Закона за защита на личните данни“.

В Глава първа „в“ от ЗЗДН е регламентирано какви данни ще се съдържат и съхраняват в Национална информационна система за превенция и защита от домашното насилие (НИСПЗДН), като информацията, подлежаща на вписване в нея, редът за събирането и предоставянето ѝ, организацията и функционирането на системата, и нивото на достъп, се определят с Правилника за прилагане на Закона за защита от домашното насилие (ППЗЗДН).

От началото на 2025 г. в МВР е внедрена в експлоатация ведомствена Автоматизирана информационна система „Домашно насилие и насилие основано на пола“ (АИС ДННОП). Системата е разработена за вътрешно ползване от служители на МВР. Тя е уеб базирано приложение и е проектирана така, че да може да обменя данни с други системи. МВР информира, че няма техническа пречка да бъде изградена интеграция с НИСПЗДН.

Предвид спецификата на лицата, чиито лични данни обработва, а именно данни на потърпевши от и извършители на домашно насилие, както и по отношение на обмена на информация между НИСПЗДН и АИС ДННОП, МВР счита, че:

- о НИСПЗДН не трябва да съхранява лични данни на потърпевши от и/или извършители на домашно насилие, а тези данни следва да се обработват (получават) от заинтересованото лице, което има правно основание за това (съдия, прокурор, социален работник и други) само по повод на конкретен случай;
- о Следва да предоставя пълна информация за случаите на домашно насилие, регистрирани в системата АИС ДННОП, при поискване на информация за конкретно лице или лица, пострадали или извършители на домашно насилие;
- о Е необходимо да получава чрез НИСПЗДН автоматизирано данни за заповеди, решения, откази и определения за защита, с оглед разпоредбата на чл. 21 от ЗЗДН, разписваща задължение на полицейските органи при наложена мярка по чл. 5, ал. 1, т. 1–5 да следят за изпълнението на заповедта;
- о В съответствие с проекта на Координационен механизъм, който е на финална фаза и предстои да бъде приет от Министерския съвет, следва да получава чрез НИСПЗДН, автоматизирано, данни от Карта

за предварителна оценка на риска, попълнена при идентифициране на случаи на домашно насилие на лице от компетентните органи за проверка на случая;

о При необходимост е възможно да предоставя анонимизирани данни (на потърпевши/извършители) при потвърдени сигнали за домашно насилие за съхранение в базата данни на НИСПЗДН, което ще позволи изготвяне на необходими на Националния съвет статистически справки за наблюдение и оценяване на политиките и мерките за предотвратяване и защита от домашното насилие.

От МВР посочват, че репликирането на личните данни на посочените по-горе категории лица по сигналите за домашно насилие, от фонда на МВР, за съхранение в система на друга администрация, носи висок риск от търсене на отговорност и упрек към МВР, респективно към администратора на лични данни по смисъла на чл. 29 от ЗМВР в случай на неправомерен достъп или изтичане на информацията относно потърпевшите, които биха могли да бъдат и малолетни и непълнолетни лица или относно извършителите от националната система. Предоставяне на личните данни на тези категории лица за съхранение от информационна система на друг орган, лишава МВР от възможност за контрол на достъпа до тях. От МВР обръщат внимание, че в АИС ДННОП се съхраняват и лични данни на уязвими лица, малолетни и непълнолетни лица, предвид че за психическо насилие върху дете се смята и всяко домашно насилие, извършено в негово присъствие.

Становището на експертите на МВР е, че не следва да се предоставя за съхранение информация, включваща лични данни (на потърпевши и/или на извършители), за случаите на домашно насилие, регистрирани от МВР. Лицата, обърнали се за съдействие към МВР очакват да получат както помощ и защита, така и запазване на конфиденциалността по случая. Лицата се обръщат към МВР като държавен орган, който е сигурен гарант за запазване на техните лични данни.

Предвид необходимостта МВР да предоставя данни към Националната информационна система за превенция и защита от домашното насилие, на основание чл. 10а, ал. 1 от ЗЗЛД във връзка с чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679, министърът отправя искане за становище по следните въпроси:

1. Следва ли МВР да предоставя за съхранение лични данни на потърпевши и извършители към Национална информационна система за превенция и защита от домашното насилие или личните данни, предоставяни за съхранение, да бъдат анонимизирани? Ако МВР следва да предоставя лични данни на потърпевши и/или извършители за съхранение, в какъв обем да бъдат те?

2. Може ли МВР да предоставя лични данни за потърпевши и извършители на домашно насилие, когато заинтересовано лице от посочените в чл. 6д, ал. 6 от ЗЗДН, което има правно основание за това, направи такова запитване към Национална информационна система за превенция и защита от домашното насилие, без да предоставя тези данни за съхранение в Национална информационна система за превенция и защита от домашното насилие?

3. Може ли МВР да получава чрез НИСПЗДН автоматизирано данни за заповеди, решения, откази и определения за защита, в предвид, че съгласно чл. 21 от ЗЗДН „При наложена мярка по чл. 5, ал. 1, т. 1–5 полицейските органи следят за изпълнението на заповедта“, които да се съхраняват в АИС ДННОП?

Водени от обществената значимост, както и от фактическата и правна сложност на повдигнатите въпроси, организирахме експертна работна среща с представители на МВР, на която в оперативен порядък се обсъдиха дискуссионните въпроси преди да пристъпим към изразяване на настоящото становище.

Правен анализ:

В МВР е създадена и функционира Автоматизирана информационна система „Домашно насилие и насилие основано на пола“ (АИС ДННОП). Системата е предназначена за вътрешно ползване от служителите на МВР, изпълняващи функции по превенция и защита от домашно насилие. Системата отговаря на изискванията за обработване на лични данни в информационните фондове на МВР, като отчита целите и изискванията на следните нормативни актове, относими към тази дейност:

- о Наказателен кодекс;
- о Наказателно-процесуален кодекс;
- о Граждански процесуалния кодекс;

- о Административнопроцесуалния кодекс;
- о Закон за Министерството на вътрешните работи;
- о Закон за закрила на детето;
- о Закон за защита от домашното насилие;
- о Правилник за прилагане на Закона за защита от домашното насилие (обн. ДВ бр. 45 от 15 юли 2010 г.);
- о Закон за защита на личните данни;
- о Закон за българските лични документи;
- о Инstrukция № 8121з-1280/07.10.2021 г. за реда за обработка на лични данни в МВР;
- о Инstrukция № Из-2673 от 10.11.2010 г. за реда за осъществяване на взаимодействието между органите на Министерството на вътрешните работи и на Министерството на труда и социалната политика при защита от домашно насилие;
- о Наредба № I-51 от 12 март 2001 г. за условията и реда за предоставяне на полицейска закрила на детето;
- о Методически указания за действията на служителите на Министерството на вътрешните работи по Закона за защита от домашното насилие, утвърдени със заповед на министъра на вътрешните работи № 8121з-78/19.01.2024 г.;
- о Указание за организацията на работа на Прокуратурата на Република България по преписки и досъдебни производства, образувани по съобщения за осъществено домашно насилие, за закана с убийство и за нарушена заповед за защита от домашно насилие;
- о Технологична инструкция рег. № Из-1239/17.08.2006 г. за организацията и правилата за работа в мрежата за предаване на данни на МВР;
- о Вътрешни правила № 951/29.04.2014 г. за реда и условията за осъществяване на контрол върху извършваните от потребителите на автоматизирани информационни фондове на Министерство на вътрешните работи дейности.

В АИС ДННОП постъпват данни от сигнали, свързани със случаи на домашно насилие, в това число лични данни за извършители, потърпевши, деца, лица от други уязвими групи, специални категории данни и т.н., необходими за целите на предотвратяването, разследването, разкриването или наказателното преследване на този род престъпления, както и за изпълнение на целите на ЗЗДН. Обработването на лични данни за тези цели попада в приложното поле на Глава осма от ЗЗЛД, с която е транспонирана Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.

Събирани за тези цели, личните данни могат да се предоставят на Националния съвет за превенция и защита от домашно насилие (НСПЗДН) към Министерския съвет, който съгласно чл. 6б, т. 6 от ЗЗДН създава и поддържа Националната информационна система за превенция и защита от домашното насилие (НИСПЗДН), за целите на ЗЗДН, при спазване на условията за последващо обработване по чл. 45, ал. 2 от Закона за защита на личните данни (ЗЗЛД).

(2) Обработването на лични данни от администратор, който първоначално ги е събрал, или от друг администратор за която и да е от целите по чл. 42, ал. 1, различна от целта, за която личните данни са събрани, се разрешава, при условие че:

1. администраторът е оправомощен да обработва лични данни за такава цел в съответствие с правото на Европейския съюз или законодателството на Република България, и
2. обработването е необходимо и пропорционално на тази различна цел в съответствие с правото на Европейския съюз или със законодателството на Република България.

...

(4) Администраторът носи отговорност за спазването на ал. 1, 2 и 3 и трябва да е в състояние да го докаже.

Съгласно чл. 6д от ЗЗДН Националният съвет създава и поддържа Национална информационна система за превенция и защита от домашното насилие, в която се съхраняват данни за случаите на домашно насилие, осъществени на територията на страната, или по отношение на български граждани в чужбина, които са потърсили помощ и подкрепа, която съдържа данни за:

1. актовете на домашно насилие;
2. пострадалите лица, извършителите и взаимоотношенията между тях;
3. вида насилие – физическо, психическо, сексуално, икономическо, ограничаване на права и други;
4. продължителността на насилието;
5. причинените вреди на пострадалото лице;
6. историята на насилието;
7. подадените молби за издаване на заповед за защита, заповед за незабавна защита или искания на прокурора по реда на чл. 8, ал. 2 от ЗЗДН;
8. наложените мерки по ЗЗДН, Закона за Министерството на вътрешните работи (ЗМВР), Закона за закрила на детето (ЗЗДт) и предоставените социални услуги по реда на Закона за социалните услуги (ЗСУ) по отношение на лица, пострадали от домашно насилие;
9. юридическите лица, които осъществяват дейности по превенция и защита от домашното насилие по реда на ЗЗДН;
10. ползваните услуги по реда на ЗЗДН.

Националният съвет осигурява регистрирането, съхраняването и поддържането в актуално състояние на посочените по-горе данни.

Информацията, подлежаща на вписване в НИСПЗДН, редът за събирането и предоставянето ѝ, организацията и функционирането на системата и нивото на достъп се определят с Правилника за прилагане на ЗЗДН (ППЗЗДН). ППЗЗДН определя и реда, по който органите на изпълнителната власт, съдебната власт, органите на местното самоуправление и местната администрация и юридическите лица предоставят на Националния съвет горепосочената информация.

Длъжностните лица от МВР, Агенцията за социално подпомагане (АСП), Държавната агенция за закрила на детето (ДАЗД) и органите на съдебната власт имат право на достъп до данните в НИСПЗДН.

Законът предвижда, че личните данни в системата се съхраняват за период от не повече от двадесет години.

За нуждите на системата Националният съвет има право на достъп до данни за извършителите на домашно насилие и в Единната информационна система за противодействие на престъпността (ЕИСПП) по чл. 378 от Закона за съдебната власт по ред, определен с ППЗЗДН.

Функциите и правомощията на Националния съвет са изчерпателно посочени в чл. 6б, ал. 1 от ЗЗДН, както следва:

1. определя приоритетите в политиките в областта на превенцията и защитата от домашното насилие;
2. осъществява координация, мониторинг и оценка на изпълнението на политиките и мерките в областта на превенцията и защитата от домашното насилие;
3. разработва и актуализира координационен механизъм за помощ и подкрепа на лица, пострадали от домашно насилие, и го представя за приемане от Министерския съвет, следи за ефективното му функциониране и дава указания и препоръки по прилагането му;
4. разработва национална програма за превенция и защита от домашното насилие въз основа на определените приоритетни дейности за финансиране и я внася за приемане от Министерския съвет, като прави предложения за актуализирането ѝ при необходимост;
5. изисква и получава информация от държавни органи, юридически лица и други, които имат отношение към превенцията и защитата от домашното насилие;
6. създава и поддържа национална информационна система за случаите на домашно насилие, осъществени на територията на страната, или по отношение на български граждани в чужбина, които са потърсили помощ и подкрепа, и списък на юридическите лица, които осъществяват дейности по превенция и защита от домашното насилие по реда на този закон, при спазване на изискванията на ЗЗЛД;

7. обобщава и анализира резултатите от изпълнението на политиките в областта на превенцията и защитата от домашното насилие и предлага мерки за повишаване на тяхната ефективност;
8. публикува и разпространява статистическа информация във връзка с домашното насилие при спазване на изискванията на Закона за статистиката и Закона за защита на личните данни;
9. организира провеждането на информационни, разяснителни и обучителни кампании по въпроси, свързани с домашното насилие;
10. разработва и актуализира проекти на стратегии, програми и планове в областта на превенцията и защитата от домашното насилие и следи и отчита тяхното изпълнение;
11. дава становища и прави предложения за изменение на действащи и за приемане на нови нормативни актове в областта на превенцията и защитата от домашното насилие;
12. разработва проекти на нормативни актове във връзка с превенцията и защитата от домашното насилие и ги внася в Министерския съвет чрез председателя на Националния съвет;
13. одобрява методически указания и участва съвместно с други представители на организации, институции и съдебни органи в разработването на документи, свързани с оценката на риска по този закон;
14. осъществява международно сътрудничество с международни организации и институции с дейност в сферата на превенцията и защитата от домашното насилие, като обменя информация и добри практики;
15. одобрява процедурите по подбор на дейностите за превенция на домашното насилие и специализираните услуги за защита от домашното насилие, финансирани по реда на чл. 6е, ал. 6 от ЗЗДН, и осъществява контрол за изпълнението на условията по договора за финансиране;
16. одобрява програмите за обучение на служители за изпълнение на функции във връзка с превенцията и защитата от домашното насилие;
17. поддържа и развива национална телефонна линия за помощ на лица, пострадали от домашно насилие и в риск;
18. извършва наблюдение и оценка на въздействието на мерките за превенция и защита от домашното насилие.

Съгласно чл. 6в от ЗЗДН за осъществяване на дейностите по превенция и защита от домашното насилие Националният съвет взаимодейства с органите на изпълнителната власт, органите на съдебната власт, органите на местното самоуправление и местната администрация и юридическите лица, които осъществяват дейности по превенция и защита от домашното насилие. Взаимодействието се осъществява по реда на координационен механизъм за помощ и подкрепа чрез:

1. обмен на информация за идентифицираните случаи на насилие, оценката на риска, насочването към компетентните органи и/или организации, определянето на мерките за защита и подкрепа, молбите за защита от домашно насилие и по повод на изпълнението на мерките; и/или
2. извършване на съвместни действия при превенцията и защитата от домашното насилие.

Видно от установените в ЗЗДН задачи и правомощия на Националния съвет, същият не разполага с разследващи правомощия, а извършва предимно аналитични, методически, координационни, информационни и консултативни функции, за чието изпълнение не е необходимо да осъществява достъп до персонализирани данни, обработвани чрез системата. Такива персонализирани данни могат да се обработват (обменят, достъпват, предоставят и пр.) само ако са подходящи, необходими и пропорционални за изпълнението на целите на ЗЗДН, при отчитане на специалните задачи правомощия на отделните органи и организации по чл. 6д, ал. 5 от ЗЗДН.

Спецификата на обработването на лични данни чрез НИСПЗДН, от различни органи и организации, за различни цели, предполага, че по отношение на защитата на личните данни се прилага както Регламент (ЕС) 2016/679, така и на Директива (ЕС) 2016/680 (респ. Глава осма от ЗЗЛД).

С Глава пета от ППЗЗДН се регламентира информацията, подлежаща на вписване в НИСПЗДН, редът за събирането и предоставянето ѝ, организацията и функционирането на системата и нивата на достъп.

С чл. 52 от ППЗЗДН се определят следните цели на НИСПЗДН:

1. централизирано събиране, управление, съхраняване и обмен на информация за случаите на домашно насилие на територията на Република България и по отношение на български граждани в чужбина;
2. осигуряване на достъп до актуална и точна информация за органите и институциите, ангажирани с превенцията и защитата от домашно насилие;
3. подобряване на координацията между институциите и организациите, работещи в областта на домашното насилие;
4. изготвяне на анализи за формиране на държавната политика в областта на превенцията и защитата от домашното насилие.

Разпоредбата на чл. 52 от ППЗЗДН на практика допълва и разширява целите на НИСПЗДН, установени в ЗЗДН, което се отразява пряко на обработването на лични данни чрез нея. Със следващия чл. 53 от ППЗЗДН се въвеждат и принципи за функционирането на системата. По този начин уреждането на въпросите за целите и принципите за функциониране на системата, на подзаконово равнище, излиза от законовата делегация на чл. 6д, ал. 4 от ЗЗДН.

Дублирането на законовия текст от чл. 6д, ал. 2 относно данните, които се съдържат в системата, в чл. 54, ал. 1 от ППЗЗДН, освен неправилна нормотворческа техника, не способства за детайлизирането на информацията, подлежаща на вписване в системата, каквато е именно законовата делегация за приемането на ППЗЗДН. Това не способства и за изпълнението на принципите за обработване на лични данни, по-специално уточняването на конкретните категории данни, подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват. При осигуряването на съответствие с принципите за обработване на лични данни следва да се отчита предимно специалното законодателство, уреждащо дейността на органите и организациите, имащи функции по превенция и защита от домашно насилие. В нормите на ППЗЗДН липсват и изискуемите гаранции за правата и свободите на засегнатите субекти на данни, като липсва ясно разграничение на целите на обработването от различните органи и организации (арг. чл. 5, пар. 1 от Регламент (ЕС) 2016/679 и/или чл. 45, ал. 1 от ЗЗЛД). Това създава предпоставки за размиване на отговорността както по отношение гарантирането на сигурността на обработваните чрез системата лични данни, така и по отношение на упражняването на правата от засегнатите субекти на данни. При спазване на принципа за отчетност задължението на всеки от администраторите, обработващ лични данни чрез НИСПЗДН, е да е в състояние да докаже, че то съответства на изискванията за защита на личните данни (Регламент (ЕС) 2016/679, съответно Глава осма от ЗЗЛД).

Законодателството за защита на личните данни въвежда принципно положение, според което исканията за разкриване на данни, изпратени от публичните органи, следва винаги да бъдат в писмена форма, да са обосновани и да засягат само отделни случаи и не следва да се отнасят до целия регистър с лични данни или да водят до свързване на регистри на лични данни (съображение 31 от Регламент (ЕС) 2016/679, респ. съображение 22 от Директива (ЕС) 2016/680). Това принципно положение, въведено от европейския законодател, би следвало да препятства дублирането/репликирането на регистри с лични данни.

Разпоредбата на чл. 70 от ППЗЗДН предвижда режим за неограничен и безусловен достъп на всяко лице до собствените му лични данни, който е несъвместим с правилата на Регламент (ЕС) 2016/679 и Глава осма от ЗЗЛД. Следва да се има предвид, че по смисъла на ЗЗЛД, когато личните данни се обработват от компетентните органи по чл. 42 от ЗЗЛД за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, правото на достъп може да бъде ограничено (арг. чл. 55, ал. 3 от ЗЗЛД) при следните условия:

1. да не се допусне възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури;
2. да не се допусне неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;
3. да се защити общественият ред и сигурност;
4. да се защити националната сигурност;
5. да се защитят правата и свободите на други лица.

В продължение на направения анализ дотук заслужава да се отбележи и обстоятелството, че още през 2022 г. на етапа на съгласуване на предложенията по един от законопроектите за изменение и допълнение на Закона за защита от домашното насилие, КЗЛД разясни, че преди приемането на предвидения подзаконен нормативен акт по приложение на ЗЗДН (към онзи момент наредба) от Министерския съвет, трябва задължително да се пристъпи към производство по предварителна консултация с КЗЛД по чл. 36, пар. 4 от Регламент (ЕС) 2016/679 във връзка с чл. 12, ал. 2 от ЗЗЛД, като това изискване на законодателството обаче не е изпълнено.

С цел да докаже съответствие с приложимото законодателство за защита на личните данни, всеки от администраторите трябва да въведе подходящи технически и организационни мерки за защита, които зачитат принципите още на етапа на проектирането и по подразбиране, особено когато се отнася за толкова комплексна информационна система, засягаща включително дейността на компетентни органи във връзка с целите по чл. 42 от ЗЗЛД. Принципно положение е, че разработването на една система трябва да следва нейното нормативно регламентиране, а обратният процес е недопустим и крайно порочен.

Безспорно е, че Министерският съвет е администратор на лични данни по отношение на НИСПЗДН. В това си качество, същият не е задължително да има достъп до личните данни, които се обработват в системата, която създава и поддържа. Независимо от това, той носи отговорност за сигурността на тези данни. Доколкото има данни, че чрез НИСПЗДН се стига и до съвместно администриране, основополагащо е да се изяснят ролите на отделните органи и организации с достъп до системата, включително правата за коригиране и изтриване, както и по прозрачен начин да се уредят съответните им отговорности, по-специално що се отнася до упражняването на правата от страна на субекта на данни, и съответните задължения за предоставяне на информацията. В този ред на мисли може да се определи и точка за контакт за субектите на данни.

Аргументи в тази посока могат да се намерят в Насоки 07/2020 на Европейския комитет по защита на данните относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД, по-специално в т. 56 от изложението. Практиката на Съда на ЕС е в същата посока, като пример в това отношение са:

- о Решение от 5 юни 2018 г., *Wirtschaftsakademie Schleswig-Holstein*, C 210/16, EU:C:2018:388, т. 43;
- о Решение от 10 юли 2018 г., *Jehovan todistajat*, C 25/17, EU:C:2018:551, т. 69; и
- о Решение от 5 декември 2023 г., *Nacionalinis visuomenės sveikatos centras*, C 683/21, EU:C:2023:949, т. 42.

Именно изредените по-горе принципни положения представляват подходящите гаранции за правата и свободите на субектите на данни в едно демократично общество

По конкретните въпроси:

1. НИСПЗДН следва да служи като среда за обмен на данни между органите и организациите по чл. 6д, ал. 5 от ЗЗДН. Чрез НИСПЗДН те следва да обменят данни, които са строго необходими за изпълнението единствено на техните задачи и правомощия. Дублирането на базите данни на тези органи, като първични администратори, и предаването им за съхранение от техните системи към НИСПЗДН, не съответства на изискванията за защита на личните данни и изискванията за информационна сигурност.

2. За изпълнението на функциите и задачите си по чл. 6б, ал. 1 от ЗЗДН Националният съвет за превенция и защита от домашно насилие не следва да получава достъп до лични данни на потърпевши и извършители, обменяни чрез НИСПЗДН между органите и организациите по чл. 6д, ал. 5 от ЗЗДН. Той може получава агрегирана и обобщена по различни критерии деперсонализирана информация, която му е необходима с оглед неговите функции и задачи по ЗЗДН.

3. МВР може да съхранява автоматизирано получените чрез НИСПЗДН данни за заповеди, решения, откази и определения за защита, доколкото полицейските органи имат за задача да следят за изпълнението на наложените мерки за защита от домашно насилие по чл. 5, ал. 1, т. 1–5 от ЗЗДН.

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 и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Като администратор на лични данни – министърът на вътрешните работи не следва да предоставя за съхранение на Националния съвет за превенция и защита от домашно насилие към Министерски съвет, поддържащ НИСПЗДН, лични данни на потърпевши и извършители на такива деяния. За целите на изпълнение на функциите и задачите си по чл. 6б, ал. 1 от ЗЗДН Националният съвет за превенция и защита от домашно насилие може да получава от органите и организациите по чл. 6д, ал. 5 от ЗЗДН само необходимата му агрегирана и обобщена по различни критерии деперсонализирана информация.

2. Чрез НИСПЗДН министърът на вътрешните работи може да предоставя лични данни на потърпевши и извършители на такива деяния единствено на органите и организациите по чл. 6д, ал. 5 от ЗЗДН, отправили чрез системата мотивирано искане за конкретно лице. Тези данни трябва да са от такова естество и в такава съвкупност, че да са подходящи, пропорционални и строго необходими за изпълнението на техните задачи и правомощия по ЗЗДН.

3. МВР може да съхранява автоматизирано получените чрез НИСПЗДН данни за заповеди, решения, откази и определения за защита, доколкото полицейските органи имат за задача да следят за изпълнението на наложените мерки за защита от домашно насилие по чл. 5, ал. 1, т. 1–5 от ЗЗДН.

4. Министерският съвет е администратор на лични данни по отношение на НИСПЗДН. Доколкото обаче има данни, че чрез НИСПЗДН се стига и до съвместно администриране, основополагащо е в ППЗДН да се уредят ролите на отделните органи и организации с достъп до системата, включително правата за коригиране и изтриване, както и по прозрачен начин да се уредят съответните им отговорности, по-специално що се отнася до упражняването на правата от страна на субекта на данни, и съответните задължения за предоставяне на информацията. В този ред на мисли може да се определи и точка за контакт за субектите на данни.

5. Поради принципния характер на настоящото становище то е валидно и за дейността по обработване на лични данни чрез НИСПЗДН и от всички други органи и организации, които осъществяват дейности по превенция и защита от домашно насилие по чл. 6д, ал. 5 от ЗЗДН.

ПРЕДСЕДАТЕЛ:

ВЕНЦИСЛАВ КАРАДЖОВ

ЧЛЕНОВЕ:

МАРИЯ МАТЕВА

ЦАНКО ЦОЛОВ

ВЕСЕЛИН ЦЕЛКОВ

СТ А Н О В И Щ Е
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-40/2025 г. и № ПНМД-01-44/2025 г.
гр. София, 14.03.2025 г.

ОТНОСНО: Излъчване в реално време (с образ и звук) на заседанията на общински експертен съвет по устройство на територията и осигуряване на публичен достъп до записите чрез публикуването им на интернет страницата на община или в онлайн платформа

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 02.04.2025 г., разглежда писма с вх. № ПНМД-01-40/14.3.2025 г. и № ПНМД-01-44/25.03.2025 г. от кметовете на Община Варна и на Столична община, съдържащи идентични искания за изразяване на становище относно допустимостта на излъчване в реално време (с образ и звук) на заседанията на общински експертен съвет по устройство на територията и осигуряване на публичен достъп до записите чрез публикуването им на интернет страницата на община или в онлайн платформа.

По отношение на искането на кмета на Община Варна:

В него се посочва, че на свое заседание от 30.05.2024 г., Общински съвет – Варна с решение № 224-10, приема обръщение към кмета на Община Варна, заседанията на експертния съвет по устройство на територията да се излъчват на живо чрез онлайн платформи и да бъдат публично достъпни като видео и аудио запис на/чрез сайта на Община Варна.

Кметът информира, че в изпълнение на чл. 6, ал. 7 от Закона за устройство на територията, с негова заповед № 0413/19.02.2024 г. е определил условията и редът за работа на общинския експертен съвет по устройство на територията в Община Варна.

В искането се посочва, че съгласно чл. 6 от Закона за устройство на територията (ЗУТ) в състава на експертните съвети могат да се включват и специалисти извън администрацията, към която са създадени, както и представители на професионални организации в областта на устройственото планиране, инвестиционното проектиране и строителството. В състава на експертния съвет се включват и представители на специализираните контролни и съгласувателни органи, когато тяхното становище, решение или разрешение се изисква по закон. ЗУТ предвижда, че кметът на общината (района) назначава общински (районен) експертен съвет по устройство на територията, като задължително се канят представители на Камарата на инженерите в инвестиционното проектиране, на Камарата на архитектите в България и на Съюза на архитектите в България (чл. 5, ал. 4 от ЗУТ).

Общинският експертен съвет по устройство на територията в Община Варна е помощен орган към кмета на Община Варна (ЕСУТ) с консултативни и експертни функции. Общинският експертен съвет по устройство на територията разглежда искания за разрешаване изработване на подробни устройствени планове (ПУП), включително комплексни проекти за инвестиционна инициатива (КПИИ) и тяхното изменение, приемане на ПУП, инвестиционни проекти, разглежда схеми на преместваеми обекти, в случай че това е предвидено в нормативен акт. За осъществяване на своята дейност, според различните по сложност и специфичност задачи, ЕСУТ може да провежда своите заседания в специализирани състави. В зависимост от характера на разглежданите доклади, планове и проекти, кметът или упълномощено от него длъжностно лице определя със заповед отделните специализирани състави на ЕСУТ.

При обявяване и одобряване на устройствените планове, работата на ЕСУТ се съобразява с чл. 127 и чл. 128 от ЗУТ, в които изрично са указани сроковете, способите и местата на обявяване или публикуване, както и когато подлежат на публично обсъждане. Посочени са и начините на провеждане, обявяване,

разгласяване на обществено обсъждане, включително и начина на документиране – писмен протокол, който се прилага към документацията за експертния съвет и за общинския съвет.

Кметът на Община Варна информира, че административните преписки, които са включени в дневния ред на ЕСУТ се докладват от главните архитекти на районите, съответно експерт в района или от длъжностни лица в общинската администрация на Община Варна и от проектантите на проектите. Докладващите лица се явяват външни за състава на ЕСУТ, назначен с изрична заповед на кмета.

Анализът на кмета показва, че горепосочената правна уредба не регламентира правна възможност заседанията на експертния съвет по устройство на територията да се излъчват на живо чрез онлайн платформи и да бъдат публично достъпни като видео и аудио запис на/чрез интернет сайт съответната община.

Предвид изложеното дотук, кметът на Община Варна отправя молба за изразяване на становище по следните въпроси:

1. Има ли право Община Варна да излъчва на живо заседанията на експертния съвет по устройство на територията чрез онлайн платформи?
2. Може ли Община Варна да предостави публичен достъп до видео и аудио запис на/чрез сайта на Община Варна?
3. Ако отговорът на горния въпрос е положителен, какъв е максималният срок, в който Община Варна би могла законосъобразно да осигурява такъв публичен достъп?

Към искането е приложен препис-извлечение на Решение № 224-10/11/30.05.2024 г. на Общинския съвет и копие на заповед № 0413/19.02.2024 г., с която са определени условията и редът за работа на Общинския експертен съвет по устройство на територията в Община Варна.

По отношение на искането на кмета на Столична община:

С него той също иска от КЗЛД да изрази становище относно допустимостта на излъчване в реално време (с образ и звук) на заседания на общинския експертен съвет по устройство на територията и осигуряването на публичен достъп до записите в рамките на изпълнение на задача от обществен интерес по смисъла на ОРЗД. Задачата произтича от възможността за живо излъчване на заседанията на Столичния общински експертен съвет по устройство на територията (СОЕСУТ). Кметът счита, че тя е важна стъпка в своевременното осигуряване на информираност, публичност, откритост, прозрачност, достъп до информация и участие на обществеността в постигане на обществено съгласие и подкрепа в процеса на вземане на решения от компетентните общински органи в областта на пространственото развитие и устройството на територията на Столична община.

Кметът съобщава, че съгласно чл. 44, ал. 1, т. 12 от Закона за местното самоуправление и местната администрация и чл. 5, ал. 4 от ЗУТ общинските съвети и кметовете на общините в рамките на предоставената им компетентност определят политиката и осъществяват дейности по устройство на територията на съответната община. С Решение № 661 по Протокол № 41 от 12.10.2017 г., изм. – Решение № 3914 от 11.06.2018 г. на АдмС – София по адм.д. № 2707/2018 г., изм. и доп. – Решение № 1 по Протокол № 26 от 14.01.2021 г. на Столичен общински съвет, е приета Наредба за реда и начина за провеждане на обществени обсъждания в областта на пространственото развитие и устройството на територията на Столична община (наричана по-нататък „Наредбата“). С нея се уреждат обществените отношения, свързани с реда и начина за провеждане на обществени обсъждания, на заинтересованите общности, за оповестяване на общественото обсъждане и за определяне на резултатите от него в областта на пространственото развитие и устройството на територията на Столична община. Обществените консултации между органите на власт и обществеността, в резултат на които се вземат управленски решения чрез съвместно обсъждане с вносителя и общинската администрация, както и чрез представяне на становища, мнения, предложения, възражения, бележки и препоръки от страна на заинтересованата общност. Съгласно чл. 11 от Наредбата по време на общественото обсъждане се прави протокол и аудиозапис, а при наличие на техническа възможност и видеозапис и онлайн излъчване на дискусиата, като протоколът, аудиозаписът, съответно видеозаписът, се публикуват на интернет страницата на Направление „Архитектура и градоустройство“, на единния електронен портал на обществените консултации към интернет страницата на Столична община и на интернет страницата на съответния район. Също така съгласно Наредбата, по преценка на кмета, съответно на главния архитект, обществените обсъждания

могат да се провеждат и дистанционно (онлайн), като присъствието се осигурява чрез конферентна или друга връзка, позволяваща участие в представянето на проекта и заключителната дискусия.

Общественото обсъждане на проекти на устройствени планове и на техни изменения се извършва преди разглеждането им от Общинския експертен съвет по устройство на територията, като кметът на Столична общината назначава столичен общински експертен съвет по устройство на територията, за което е издадена заповед № СОА25-РД91-28/03.02.2025 г. При провеждане на заседанията на съвета участват и представители на Камарата на инженерите в инвестиционното проектиране, Камарата на архитектите в България и на Съюза на архитектите в България. В състава на експертния съвет могат да се включват и специалисти извън администрацията, както и представители на професионални организации в областта на устройственото планиране, инвестиционното проектиране и строителството. В експертния съвет се включват и представители на специализираните контролни и съгласувателни органи, когато тяхното становище, решение или разрешение се изисква по закон. На своите заседания, съветът разглежда проекти за подробни устройствени планове и дава становища по тях. Подробните устройствени планове са ключови документи в устройственото планиране и тяхното влизане в сила предопределя бъдещото възможно застрояване в рамките на конкретните имоти. Експертният съвет се произнася дали даден проект да бъде одобрен, отложен за допълнителни проучвания или отхвърлен. Това е и етапът, на който гражданите и засегнатите страни могат да изразяват мнения, да подават възражения и препоръки. В случай на несъгласие, това е най-ранният момент, в който дадено решение може да бъде обжалвано, а не когато строителството е в ход.

С оглед осигуряването на публичност на работата на експертния съвет кметът планира да се осъществява пряко излъчване на заседанията му на интернет страницата на направление „Архитектура и градоустройство“, което да се извършва с автоматични средства – видеокамера за събиране на информация, като същевременно ще извършва и запис на излъчването. В писмото се посочва, че в тази връзка е подготвена заповед за допълване, с която е уреден редът за излъчване на живо на заседанията (live streaming) на съвета, с оглед изпълнение на изискванията за опазване на служебната и държавната тайна, както и на сведения, отнасящи се до личния живот и доброто име на гражданите. В съответствие с чл. 32 от Регламент (ЕС) 2016/679 са предприети технически и организационни мерки за повишаване мерките за сигурност на личните данни, като недопускане попадането на документи, чертежи и др., съставляващи част от разглежданите преписки под обсега или обхвата на заснемане. Целта е да се осигури по-голяма откритост и достъпност прогласени в чл. 2, ал. 1, т. 2 от Закона за администрацията (ЗАДм), който се прилага субсидиарно и за органите на местното самоуправление (арг. чл. 1, ал. 3 от ЗАДм). Кметът счита, че в процеса на градоустройствено планиране чрез живите излъчвания (т.н. live streaming) ще даде възможност на гражданите, организациите и всички заинтересовани страни да участват и да следят обсъжданията и решенията в реално време.

Предвид изложеното дотук, кметът на Столична община отправя молба за изразяване на становище по следните въпроси:

1. Допустимо ли е излъчване на живо на заседанията (live streaming), предвид разпоредбата на чл. 6, пар. 1, б. „д“ (обработването е необходимо за изпълнението на задача от обществен интерес) от ОРЗД, което е едно от алтернативните основания за законосъобразност на обработването на лични данни?

2. Допустимо ли е видеозаснемане на заседанията на съвета и в какъв срок следва да се съхраняват записите, отчитайки принципа за ограничение на съхранението по чл. 5, пар. 1, б. „д“ от Регламент (ЕС) 2016/679?

3. Предвид вмененото задължение в т. 2.12 от заповед № СОА25-РД91-28/03.02.2025 г. на определени служители от Направление „Архитектура и градоустройство“, които не са членове на съвета, да докладват въпросите от определения дневен ред, следва ли същите да се приемат като субекти на лични данни, ползващи се със защита по ОРЗД и трудовото законодателство? По т. 2.8 от същата заповед, поканените за участие в заседанието външни лица също имат възможност да се запознаят със съдържанието на предвидените за разглеждане от съвета административни преписки.

Правен анализ:

Съгласно Закона за местното самоуправление и местната администрация (ЗМСМА) кметовете на общини възлагат или разрешават изработването на устройствени планове и техни изменения за територията на общината или за части от нея и одобряват определени устройствени планове при условията и по реда на Закона за устройство на територията (ЗУТ), както и организират изпълнението им. От своя страна, общинските съвети имат правомощието да приемат решения за създаване и одобряване на устройствени планове и техни изменения за територията на общината или за части от нея при условията и по реда на ЗУТ. По силата на чл. 5, ал. 1 от ЗУТ общинските съвети и кметовете на общините в рамките на предоставената им компетентност със ЗМСМА определят политиката и осъществяват дейности по устройство на територията на съответната община.

Статутът и функциите на общинските (районните) експертни съвети по устройство на територията са уреди в ЗУТ. Той предвижда, че кметът на общината (района) назначава общински (районен) експертен съвет по устройство на територията, като задължително се канят представители на Камарата на инженерите в инвестиционното проектиране, на Камарата на архитектите в България и на Съюза на архитектите в България. Експертните съвети извършват консултативна и експертна дейност, като в състава им могат да се включват и специалисти извън администрацията, към която са създадени, както и представители на професионални организации в областта на устройственото планиране, инвестиционното проектиране и строителството. В състава на експертния съвет се включват и представители на специализираните контролни и съгласувателни органи, когато тяхното становище, решение или разрешение се изисква по закон. Условията и редът за работа на експертните съвети се уреждат със заповед на органа, който ги назначава.

Видно от нормативната уредба дейността на общинските експертни съвети по устройство на територията е пряко свързана с планирането на градоустройството на територията на дадена община. Градоустройство е процесът на планиране, организиране и развитие на територии в урбанизираната среда с цел създаване на функционални, устойчиви и естетически приемливи градове и селища. То обхваща всички аспекти на развитието на урбанистичните пространства, като включва както архитектурния дизайн, така и инфраструктурните и социални нужди на населението. Целта на градоустройството е да осигури ефективно, безопасно и комфортно пространство за живот и работа на хората в урбанизираните райони. Процесът на планиране и организиране на градските територии има важни социални, икономически и екологични последици, които се отразяват на качеството на живот на всички жители на един град или населено място. Ето защо градоустройството се разглежда като дейност, която е от съществено значение за обществото като цяло.

Излъчването на живо (с образ и звук) на заседанията на общинските експертни съвети по устройство на територията предполага извършване на дейности по обработване на лични данни на физическите лица, попадащи в обхвата на записващите/излъчващите оптични или аудиовизуални устройства (камери). В този смисъл правилата на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) се прилагат и за излъчването на живо на образни и/или аудио данни за лица чрез автоматични средства – камери. Именно поради това излъчването на живо следва да се приеме като дейност по обработване на лични данни, попадаща в материалния обхват на ОРЗД. Това разбиране е възприето и от Европейския комитет по защита на данните (ЕКЗД), в чиито Насоки № 03/2019 относно обработването на лични данни чрез видеоустройства[1] се посочва, че „В определени случаи наблюдението в реално време може да представлява по-голяма намеса от съхранението и автоматичното изтриване на видеозаписи след изтичане на определен срок [...]“.

За да бъде законосъобразно обработването на лични данни, то трябва да се осъществява въз основа на някое от алтернативните правни основания, посочени в чл. 6, пар. 1 (за общите категории) и/или чл. 9, пар. 2 (за специалните категории) от ОРЗД, както и да бъдат приложени ефективно принципите за обработването им, прогласени в неговия чл. 5.

В конкретния случай излъчването в реално време на образни и аудио данни в интернет води до тяхното разкриване чрез предаване и разпространяване до неограничен кръг от лица. Нещо повече, в т. 31 от Насоки № 02/2021 относно виртуалните гласови асистенти[2] ЕКЗД акцентира, че

"гласовите данни по своята същност представляват биометрични лични данни"[3]. Биометричните данни попадат в обхвата на т.нар. специални категории лични данни, чието обработване е подчинено на по-високи изисквания за защита и е допустимо само при наличие на някое от условията по чл. 9, пар. 2 от ОРЗД. Обработването на специални категории лични винаги е съпроводено от повишени рискове за правата и свободите на гражданите и поради това прагът за защита на правата и свободите им също е по-висок.

Анализът дотук показва, че правната уредба не въвежда изрично задължение на кметовете на общини (райони) да осигуряват излъчване на живо на заседанията на общинските експертни съвети по устройство на територията. Въпреки това обаче осигуряването му може да се разглежда като мярка за гарантиране на публичността, прозрачността и участието на обществеността в постигането на обществено съгласие и подкрепа в процеса на вземане на решения от компетентните общински органи в областта на пространственото развитие и устройството на територията на дадена община. Именно поради това излъчването на живо на заседанията на общинските експертни съвети по устройство на територията може да се приеме като обработване на лични данни, необходимо за изпълнението на задача от обществен интерес.

При тези обстоятелства излъчването на живо (с образ и звук) на заседанията на общинските експертни съвети по устройство на територията би могло да се извършва единствено въз основа на чл. 6, пар. 1, б. „д“, пр. 1 и пар. 3 вр. с чл. 9, пар. 2, б. „ж“ от ОРЗД, а именно:

- о обработването е необходимо за изпълнението на задача от обществен интерес; и
- о обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

Въпреки това, за целите на гарантиране на правната сигурност, предвидимост и прозрачност на тяхната работа, възможността за излъчване на живо следва да бъде *de lege ferenda* регламентирана в съответния нормативен акт, уреждащ дейността на експертните съвети по устройство на територията. Този подход ще обезпечи и прилагането на основния принцип в публичното право, според който на публичните органи следва да е „разрешено само това, което е изрично предвидено в закон“.

Тъй като към момента липсва такава изрична правна регламентация, общините следва да въведат правила, политики и процедури, които да способстват за повишаване на мерките за сигурност на личните данни, като напр. недопускане попадането в обсега на заснемане на документи, чертежи и др., съставляващи част от разглежданите преписки и съдържащи лични данни. Тези мерки следва да включват и правила за провеждане на открити (с излъчване) и закрити (без излъчване) заседания, както гаранции и мерки срещу нерегламентирано разкриване на друга информация, защитена със закон (напр. класифицирана информация, търговска тайна и пр.). Въведените от общините мерки могат да включват и гаранции за защита на интелектуалната собственост. Като част от тези мерки следва да се разгледа и актуализацията на политиките за поверителност на общините, чрез които на субектите на данни да се предостави нужната информация по чл. 13 от ОРЗД. Участващите в заседанията длъжностни лица следва да са обвързани да спазват изискванията за защита на личните данни, както и да не разгласяват данни, отнасящи се до личния живот и доброто име на гражданите. Освен субекти на данни, те имат и качеството на лица, действащи под ръководството на администратора, който им е осигурил достъп до подлежащи на обработване лични данни, необходими за изпълнението на служебните им задължения (арг. чл. 29 от ОРЗД).

Не е налице нормативна пречка за общините, на същите основания, да осигурят и публичен достъп до записите от проведените заседания чрез публикуването им на техните интернет страници или в онлайн платформи, върху които имат контрол. Периодът, за който могат да бъдат публикувани записите, респ. да бъдат достъпни в интернет, трябва да се определи от общините, отчитайки принципа за „ограничение на съхранението“, прогласен в чл. 5, пар. 1, б. „д“ от ОРЗД. Той изисква личните данни да се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за постигане на целите, за които се обработват. Индикативни критерии за

определянето на този период могат да бъдат сроковете за обжалване на актове, приети от общинските експертни съвети по устройство на територията (ако има такива) или срокът за подаване на жалба по чл. 38, ал. 1 от Закона за защита на личните данни.

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 и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Общините могат да извършват излъчване на живо (с образ и звук) на заседанията на общинските експертни съвети по устройство на територията в изпълнение на техни задачи от обществен интерес, установени в Закона за местното самоуправление и местната администрация и Закона за устройство на територията. Въпреки това, за целите на гарантиране на правната сигурност, предвидимост и прозрачност на тяхната работа, възможността за излъчване на живо следва да бъде *de lege ferenda* регламентирана в съответния нормативен акт, уреждащ дейността на експертните съвети по устройство на територията.

2. На основание по т. 1 общините могат да осигуряват и публичен достъп до записите от проведените заседания чрез публикуването им на техните интернет страници или в онлайн платформи, върху които имат контрол. Периодът, за който могат да бъдат публикувани записите, респ. да бъдат достъпни в интернет, трябва да се определи от общините, отчитайки принципа за „ограничение на съхранението“, прогласен в чл. 5, пар. 1, б. „д“ от Регламент (ЕС) 2016/679. Той изисква личните данни да се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за постигане на целите, за които се обработват. Индикативни критерии за определянето на този период могат да бъдат сроковете за обжалване на актове, приети от общинските експертни съвети по устройство на територията (ако има такива) или срокът за подаване на жалба по чл. 38, ал. 1 от Закона за защита на личните данни.

3. При излъчването на живо общините следва да въведат и прилагат правила, политики и процедури, които да способстват за повишаване на мерките за сигурност на личните данни, като напр. недопускане попадането в обсега на заснемане на документи, чертежи и др., съставляващи част от разглежданите преписки и съдържащи лични данни. Тези мерки следва да включват и правила за провеждане на открити (с излъчване) и закрити (без излъчване) заседания, както гаранции и мерки срещу нерегламентирано разкриване на друга информация, защитена със закон (напр. класифицирана информация, търговска тайна и пр.). Въведените от общините мерки могат да включват и гаранции за защита на интелектуалната собственост. Като част от тези мерки следва да се разгледа и актуализацията на политиките за поверителност на общините, чрез които на субектите на данни да се предостави нужната информация по чл. 13 от Регламент (ЕС) 2016/679. Участващите в заседанията длъжностни лица следва да са обвързани да спазват изискванията за защита на личните данни, както и да не разгласяват данни, отнасящи се до личния живот и доброто име на гражданите. Освен субекти на данни, те имат и качеството на лица, действащи под ръководството на администратора, който им е осигурил достъп до подлежащи на обработване лични данни, необходими за изпълнението на служебните им задължения.

ПРЕДСЕДАТЕЛ:

ВЕНЦИСЛАВ КАРАДЖОВ

ЧЛЕНОВЕ:

ЦАНКО ЦОЛОВ

МАРИЯ МАТЕВА

ВЕСЕЛИН ЦЕЛКОВ

[1] Публикувани на интернет страницата на ЕКЗД:

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_bg.pdf

[2] Публикувани на интернет страницата на ЕКЗД:

https://www.edpb.europa.eu/system/files/2022-02/edpb_guidelines_202102_on_vva_v2.0_adopted_bg.pdf

[3] В чл. 4, пар. 14 от ОРЗД биометричните данни са определени като „лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни“.

**СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-52/2025 г.
гр. София 30.04.2025 г.**

ОТНОСНО: Използване на система за видеонаблюдение с функционалност за лицево разпознаване в търговски обекти (магазини)

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 30.04.2025 г., разгледа писмо от охранително дружество, с което се отправя молба за изразяване на становище относно допустимостта на използване на система за видеонаблюдение с функционалност за лицево разпознаване в търговски обекти (магазини).

Фактическа страна:

Дружеството информира, че оперира в сферата на частната охранителна дейност, като предоставя специализирани охранителни услуги с действащ лиценз, съобразно Закона за частната охранителна дейност (ЗЧОД). Като част от своето клиентско портфолио на дружеството се възлага и охраняването на множество магазини за търговия на дребно на територията на Република България, включително от страна на клиенти-възложители, разполагащи с широка търговска мрежа и многобройни обекти в цялата страна.

В искането се посочва, че към настоящия момент на територията на магазините, охранявани от дружеството, обичайно се осъществява видеонаблюдение чрез видеокамери, обхващащи търговските зони с цел опазване на имуществото в търговските обекти и осигуряване на обществения ред в тях. Дружеството счита това за „стандартно видеонаблюдение“.

То разяснява, че хардуерната и софтуерната инфраструктура за това „стандартно видеонаблюдение“ се осигуряват от самия клиент, записите се съхраняват в законово установения допустим срок на сървъри, които също по правило са собственост на клиента. Самият фактически контрол чрез „стандартното видеонаблюдение“ се осъществява от охранителното дружество, което е легитимирано чрез своя лиценз да упражнява тази дейност.

В писмото се информира, че на ежедневна база през търговските обекти преминава огромен поток от клиенти/посетители – стотици хиляди души на ден. Дружеството, в изпълнение на своите задължения като лицензирана охранителна фирма, ежедневно се опитва да и на практика предотвратява всякакви дребни кражби или опити за изнасяне на различни по вид и стойност продукти, без същите да бъдат заплатени на каса, както и всевъзможни други противообществени прояви (напр. агресия, вандалски актове и т.н.). Въпросните кражби касаят не само собственост на клиентите му – юридически лица, но и джебчийски посегателства към други крайни клиенти, респ. посетители в хипермаркетите. В нередки случаи се стига и до физическа конфронтация с охранителите или други крайни клиенти на магазините.

По гореописаните причини дружеството счита „стандартното видеонаблюдение“ за недостатъчно, така че качествено да изпълнява възложените му задължения, тъй като охранителите в отделните хипермаркети обективно и физически не могат да осигурят адекватен контрол спрямо обема на човекопотока с цел минимизиране на рисковете. Дружеството желае да предложи на своите клиенти – юридически лица, услуга с добавена стойност под формата на продажба на лицензи и интегриране към вече изградената система за стандартно видеонаблюдение, на допълнителни функционалности на

камерите и свързания с тях софтуер (дружеството го нарича „разширено видеонаблюдение“), а именно:

- При констатиран опит за кражба от магазин на посетител и/или нарушаване на обществения ред в търговски обект на клиент, клиентът ще използва записите от „стандартното видеонаблюдение“ за въвеждане на лицето на нарушителя в специализирана база данни за целите на неговата последваща уникална идентификация;
- Въвеждането ще се извършва „ръчно“ от служител на клиента - чрез човешка намеса, а самата специализирана база данни ще се съхранява на локални сървъри на клиента, който е и остава администратор на данните по смисъла на действащото законодателство, като достъпът до нея ще бъде строго ограничен и осъществяван при стриктно спазване на принципа „необходимост да се знае“, а именно – служителите на дружеството няма да имат достъп до цялата база данни, а единствено ще могат да наблюдават вече въведени лица, както е описано по-долу;
- След въвеждането на лицето в специализираната база данни, при повторно негово влизане в търговски обект на клиент камерите, в чийто обхват попада той, ще идентифицират (разпознаят) лицето и ще индикират на локалните охранители, че същото е с предходни противообществени прояви на територията на този или други търговски обекти, собственост на клиента. От самото отбелязване няма да следват други преки, вкл. негативни последици за съответния човек – единствено ще бъде обърнато внимание на дежурния охранител на съответния магазин за присъствието му на територията на охранявания от него обект с цел непосредствено осъществяване на целенасочено по-завишено наблюдение и контрол;
- Данните на лицата, въведени за целите на т.нар. „разширено видеонаблюдение“, ще бъдат съхранявани за период от 3 години, след което ще бъдат автоматично изтривани;
- Клиентът, като администратор на данните по смисъла на действащото законодателство, ще предоставя подробна информация за този процес по обработване, като постави информацията по чл. 13 от Регламент (ЕС) 2016/679 (ОРЗД) на видно място във всеки свой магазин, както и чрез публикуването ѝ на официалния си уебсайт.

Правна обосновка на дружеството:

То пояснява, че при разширеното видеонаблюдение ще се използва лицевият образ на физически лица за целите на уникалната им автоматизирана идентификация от системата.

Дружеството отчита, че съгласно чл. 4, т. 14 от ОРЗД „биометрични данни“ са лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни. Дружеството приема за безспорно, че в настоящия случай би било налице обработване на биометрични лични данни, които съставляват и „специална категория данни“ по смисъла на чл. 9, пар. 1 от ОРЗД, тъй като:

- данните са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице;
- данните са „получени в резултат на специфично техническо обработване“; и
- данните се използват с цел уникално идентифициране на физическо лице.

Дружеството отбелязва, че използването на биометрични данни и по-конкретно на разпознаване на лица е свързано с повишени рискове за правата на субектите на данните. То счита, че от решаващо значение е използването на такива технологии да се предприема при надлежно зачитане на залегналите в ОРЗД принципи на законосъобразност, необходимост, пропорционалност и свеждане на данните до минимум, като в този смисъл са и Насоки № 3/2019 на Европейския комитет по защита на данните относно обработването на лични данни чрез видеоустройства.

По отношение на законосъобразността: Съгласно чл. 9, пар. 1 от ОРЗД, обработването на

специални категории данни по общо правило е забранена. Параграф 2 от същата разпоредба въвежда редица изключения, от анализа на които става ясно, че обработването на специални категории данни може да се извършва на различни основания спрямо тези по чл. 6 от ОРЗД. Сред тях обаче не са включени легитимните интереси на администратора, което правно основание обичайно намира приложение, когато се използва „стандартно видеонаблюдение“ от страна на клиентите на дружеството в качеството им на администратори.

От възможностите за законосъобразно обработване на специални категории лични данни за целите на уникално лицево разпознаване чрез система за разширено видеонаблюдение дружеството счита, че следното правно основание би било относимо и излага принципните си съображения за приложимост на изключението:

Чл. 9, пар. 2, б. „ж“ от ОРЗД

Дружеството посочва, че съгласно визираната разпоредба обработването на специални категории данни (включително биометрични такива) е допустима, когато „обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните“.

От дружеството изразяват мнение, че за всяко едно общество от съществен интерес е запазването на реда и безопасността на гражданите на публични места. Основни характеристики относно определянето на това дали един процес е от съществен обществен интерес са:

- Възможният брой и категории засегнати лица;
- Интересите на обществото, които могат да бъдат накърнени;
- Местата, на които може да се реализира рискът.

Ежедневно през търговски обекти, собственост на клиенти на дружеството, преминава огромен поток от хора (става дума за стотици хиляди души на ден), като немалка част от тях традиционно са възрастни хора, семейства с малки деца и други уязвими групи граждани. Съобщава, че почти ежедневно се установяват различни по вид и характер противообществени прояви.

Дружеството счита, че обществените интереси, които могат да бъдат накърнени, при липса на система за разширено видеонаблюдение, засягат основни човешки права съгласно Хартата на основните права на ЕС и Европейската конвенция за правата на човека, а именно: правото на лична неприкосновеност (напр. при нападение), правото на собственост (при кражби) и т.н.

Визираните по-горе търговски обекти, които се охраняват от дружеството, са обществено достъпни места за гражданите/находящите се лица на територията на Република България, без ограничение от какъвто и да било характер. Дружеството излага доводи, че дори и при предходни противообществени прояви, с оглед правото на всеки човек да се поправи, клиентите му по правило не спират достъпа на тези лица до своите търговски обекти, като все пак същият би могъл по изключение да бъде ограничен по преценка на клиент. По този начин и с оглед огромния брой посетители е възможно да бъде засегнат неограничен кръг от лица.

Дружеството акцентира, че общественият интерес е застъпен и в правото на Съюза – в Европейската конвенция за правата на човека, както и в националното законодателство на Република България. Така например, съгласно чл. 2 от ЗЧОД, „частната охранителна дейност е търговска дейност, насочена към опазване на живота и здравето на физическите лица, охраняване на имуществото на физическите и юридическите лица“. Дружеството е на мнение, че дори законово вменената функция на лицата, които биха били ангажирани с използването на система за разширено видеонаблюдение, е именно да опазват обществения ред, здравето, живота и имуществото на физически и юридически лица.

С оглед гореизложеното дружеството счита, че правно основание за обработване на биометрични лични данни на лицата, извършили всякакъв вид противообществени прояви на територията на охранявани търговски обекти на негови клиенти, чрез система за разширено видеонаблюдение, включваща лицево разпознаване, намира изразение в чл. 9, пар. 2, буква „ж“ от ОРЗД.

По отношение на необходимостта: Дружеството счита обработването на лични данни чрез въпросната система за разширено видеонаблюдение за категорично необходима, тъй като единствено чрез нейното внедряване би могло да се осигури подходящ и адекватен контрол на лица, за които има обосновано повишен риск от извършване на противообществени прояви. Някои от търговските обекти на негови клиенти са със значителна площ, която трябва да се контролира от лицата, ангажирани със сигурността. Контролът върху т.нар. стандартно видеонаблюдение, както и физическата охрана на хипермаркетите се осъществява от ограничен брой служители на дружеството. Отчитайки броя хора, които ежедневно преминават през охраняваните от дружеството търговски обекти, то счита, че е необходима диверсификация на лицата, което единствено може да позволи ефективна защита на здравето и неприкосновеността на посетителите, а и на служителите в магазините. По този начин служители на дружеството – охранители биха могли да реагират много по-бързо при евентуална повтораемост в незаконосъобразното поведение на лицето.

С оглед на това дружеството счита, че обработването на личните данни чрез система за разширено видеонаблюдение се явява необходима.

По отношение на пропорционалността: За да се докаже пропорционалността на мярката, е необходимо да се демонстрира, че използването на системата за разширено видеонаблюдение би осигурила значително по-ефективна защита срещу повторни нарушения в сравнение с алтернативни, по-малко инвазивни методи, като например стандартно видеонаблюдение без автоматизирана идентификация. Дружеството е на мнение, че в този случай системата ще е строго ограничена до лица, за които има обективна предходна информация, че са извършвали противообществени прояви в обекти, собственост на негови клиенти, което гарантира, че останалите крайни клиенти – физически лица, не са подложени на ненужно следене. Освен това, според дружеството, обработването на биометричните данни е времево ограничено и се извършва само докато съществува реален и обоснован риск от повторни нарушения, което означава, че данните няма да се съхраняват за неопределен период, а ще се заличават при отпадане на необходимостта. Достъпът до системата би бил строго регулиран и предоставен само на оторизирани лица, които имат право да реагират при установяване на конкретна заплаха, без да се допуска неоправдано широк кръг лица да разполага с тази чувствителна информация. Нещо повече, достъп до базата данни ще имат единствено служители на клиента. Според дружеството тези мерки ще засегнат възможно най-малък брой субекти на данни, ще ограничат въздействието върху личната сфера на гражданите и ще гарантират, че обработването остава в рамките на необходимото за постигане на легитимната цел – предотвратяване на нарушения и защита на имуществото и сигурността в обекта. Друг основен аргумент на подателя на искането е, че дори лицата, които ще бъдат засичани от разширеното видеонаблюдение, няма да бъдат подлагани на рестриктивни мерки. За дружеството единствената цел на обработването на личните им данни е по-бърза и ефективна реакция от страна на охранителите на място в обект при необходимост.

По отношение на свеждането на данните до минимум: Дружеството информира, че в базата данни, използвана от системата за разширено видеонаблюдение, ще бъдат въвеждани единствено лица, които имат доказани предходни противообществени прояви на територията на магазини на негови клиенти. Техните противообществени прояви ще са доказани с констативни протоколи от представители на наетите охранителни дружества, действащи съгласно ЗЧОД. В самата база данни няма да има информация за имена или друга идентифицираща съответното лице информация. Информацията за характера на предходното незаконосъобразно поведение на лицето – напр. дали е направило опит за кражба, проява на насилие, хулиганство и т.н. ще бъде криптирана и достъпна единствено за лицата, които имат фактически контрол върху базата данни, но не и за охранителите. По този начин клиентите на дружеството ще свеждат обработваните данни до абсолютен минимум, който все пак да позволява функционирането на системата. Налице ще е и определен срок за съхранение на данните, който е съобразен например с принципа за ограничаване на съхранението съгласно ОРЗД.

Допълнителна информация от дружеството:

Дружеството отчита факта, че използването на система за разширено видеонаблюдение, включваща технологии за лицево разпознаване, представлява нововъведение, което изисква внимателна и

задълбочена оценка на въздействието върху защитата на данните (ОВЗД). В съответствие с изискванията на ОРЗД и принципа на отчетност, дружеството съобщава, че клиентите му ще извършат ОВЗД преди внедряване на системата, като основният фокус ще бъде анализът на потенциалните рискове за правата и свободите на субектите на данни и определянето на адекватни и детайлни технически и организационни мерки за тяхното минимизиране. Оценката ще включва повторно индивидуално за юридическото лице – администратор подробно разглеждане на необходимостта и пропорционалността на системата, ефективността на предвидените мерки за защита на личните данни, както и потенциалното въздействие върху засегнатите лица. Дружеството изтъква, че въз основа на резултатите от ОВЗД и евентуално положително становище на КЗЛД по настоящото искане, всеки отделен негов клиент ще вземе информирано решение дали внедряването на системата е оправдано и дали рисковете за субектите на данни са сведени до приемливо ниво. Дружеството заявява, че имплементирането на разширеното видеонаблюдение ще се осъществи единствено при наличие на ясни доказателства, че обработването на лични данни няма да създаде непропорционални рискове за правата на физическите лица и след като администраторът въведе всички необходими предпазни мерки за осигуряване на законосъобразност, прозрачност и защита на личната неприкосновеност.

За пълнота на изложението си дружеството подчертава, че в случай на положително становище от КЗЛД относно законосъобразността и пропорционалността на внедряването на разширеното видеонаблюдение, клиентите му ще пристъпят към разработване и въвеждане на конкретни индивидуални вътрешни политики, уреждащи всички аспекти, свързани с функционирането на системата. Тези политики ще включват подробни правила за събиране, съхранение, достъп и обработване на биометрични данни, както и ясни процедури за защита на правата на субектите на данни, включително упражняване на правото на достъп, коригиране, заличаване и възражение срещу обработването. Освен това, политиките ще регламентират вътрешните механизми за сигурност, като например ограничения за достъп до базата данни, мерки за предотвратяване на неоторизирано разкриване или злоупотреба с данни, както и редовни одити и оценки на ефективността на въведените мерки. Дружеството декларира, че ще бъде отделено специално внимание на обучението на лицата, които ще работят със системата, за да се гарантира, че те са наясно с изискванията на ОРЗД и могат да прилагат процедурите за защита на личните данни в практиката, в това число на лицата, които ще обработват данните по възлагане по смисъла на чл. 28 от ОРЗД. Наред с това ще бъде осигурена прозрачност за субектите на данни чрез предоставяне на достъпна информация за начина, по който работи системата, целите на обработването и гаранциите за защита на техните права. Въвеждането на подобни политики ще бъде неразделна част от процеса по имплементиране на системата, като те ще бъдат редовно преглеждани и актуализирани в зависимост от евентуални промени в законодателството, указанията на КЗЛД или идентифицирани рискове при експлоатацията на системата.

С оглед на гореизложеното дружеството отправя молба за изразяване на становище по следните въпроси:

1. „Допустимо ли е използването на система за видеонаблюдение, която включва лицево разпознаване на субекти на данни, чиито биометрични данни са въведени ръчно в база данни поради предходни техни противообществени прояви на територията на магазин(и), собственост на клиенти на Дружеството?“
2. „В случай че е допустимо, може ли администраторът на лични данни, по чието възлагане Дружеството ще обработва личните данни като „обработващ“ да основава този тип обработка на лични данни на чл. 9, параграф 2, буква „ж“ от ОРЗД?“
3. „Ако не е допустимо, има ли друго конкретно правно основание, на което клиентите на Дружеството могат да се позоват, за да интегрират системата за Разширено Видеонаблюдение?“

Правен анализ:

Видеонаблюдението е дейност, свързана със събиране и съхранение на образни и/или аудио данни

за лица, попадащи в обхвата на наблюдавана зона, които подлежат на пряко или косвено идентифициране въз основа на техния външен вид или други специфични признаци. Съществен елемент от тази дейност е, че самоличността на лицата може да бъде установена въз основа на тези данни, а също така се създава възможност за обработване на данни относно присъствието и поведението на лицата в съответната зона. Събирането и съхранението на образни и/или аудио данни за лицата, представлява обработване на лични данни чрез автоматични средства – оптични или аудиовизуални устройства (камери). Именно поради това то се приема като дейност по обработване на лични данни, попадаща съгласно чл. 2, пар. 1 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) в неговия материален обхват, респ. следва да се осъществява съобразно неговите изисквания.

Обичайно, конвенционалното видеонаблюдение (наричано в искането „стандартно“) се осъществява за охранителни цели, като напр. за защита от противоправни посегателства на имущество на администратора, защита на здравето и живота на служители, посетители и др. категории субекти на данни. В повечето случаи тези цели обуславят наличието на легитимен интерес за обработване на данните от администратора, който има преимущество пред интересите или основните права и свободи на субектите на данни (чл. 6, пар. 1, първа алинея, б. „е“ от ОРЗД).

Видеонаблюдение, включващо и функционалност за лицево разпознаване на субектите, попадащи в обхвата на заснемане обаче, освен събирането и съхранението на „общи“ категории лични данни, предполага обработването и на специални категории данни от вида на биометричните. Биометричните данни са лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни (чл. 4, т. 14 от ОРЗД). Те могат да позволят удостоверяване на самоличността, идентифициране или категоризиране на физически лица, както и разпознаване на емоции на физически лица.

В обобщение, с оглед на текста на чл. 4, т. 14 и чл. 9, пар. 1 от ОРЗД трябва да бъдат отчетени три критерия:

- характер на данните: данни, свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице,
- средства и начин на обработване: данни, „получени в резултат на специфично техническо обработване“,
- цел на обработването: данните трябва да се използват с цел уникално идентифициране на физическо лице.

Обработването на специални категории лични данни винаги е свързано с повишени рискове за правата и свободите на субектите на данни, поради това, прагът за тяхната защита е много по-висок. Повишените рискове при обработване на тези данни са обусловени от много по-тясната връзка между тях и притежателя им – субектът на данни. Така например при инцидент, свързан със сигурността на общи категории лични данни (напр. тел. номер, имейл адрес и пр.) субектът на данни би могъл да предприеме сравнително лесно действия за евентуална промяна на тези данни с „нови“, докато подмяната на специални категории данни в много случаи се явява обективно невъзможна.

Системите за видеонаблюдение обикновено събират големи обеми данни, които могат да разкрият информация с подчертано личен характер, и дори специални категории данни. Трябва да се подчертае, че на пръв поглед събрани чрез видеонаблюдение данни без особено значение могат да се използват за получаване на друга информация за постигане на различни цели (напр. за анализ на навиците и поведението на физическо лице). Въпреки това, видеонаблюдението не във всички случаи се счита за обработване на специални категории лични данни. Видеозапис на физическо лице не може да се счита сам по себе си за биометрични данни, ако той не е бил подложен на специфична техническа обработка, за да може да допринесе за идентифицирането на това лице. Когато система за видеонаблюдение се използва за обработване на специални категории данни, администраторът на данните трябва да определи както изключение за обработване на специални категории данни по чл. 9, пар. 2 (изключения от общото

правило за недопустимост на обработването на специални категории данни), така и правно основание по чл. 6 от ОРЗД.

Както се посочи по-горе, използването на биометрични данни и по-конкретно на разпознаване на лица е свързано с повишени рискове за правата на субектите на данните. От решаващо значение е използването на такива технологии да се предприема при надлежно зачитане на заложените в ОРЗД принципи на законосъобразност, необходимост, пропорционалност и свеждане на данните до минимум. Макар че използването на такива технологии може да се разглежда като особено ефективно, администраторите на данните следва преди всичко да оценят въздействието върху основните права и свободи, и да преценят възможностите за използване на алтернативи средства за постигане на законната цел на обработването, които представляват по-малка намеса в правата и свободите на субекта на данни.

Системите за видеонаблюдение могат да са полезни както за частния, така и за публичния сектор, повишавайки сигурността и позволявайки анализиране на лицата, попадащи в обхвата му и дори за извършването на персонализирана реклама. Ефективността им се увеличава с интелигентен видео анализ, включващ както комплексни биометрични технологии, така и прости алгоритми. Запазването на анонимността и личния живот е предизвикателство, а правният анализ варира в зависимост от използваната технология. Наред с въпросите, свързани с неприкосновеността на личния живот, съществуват и рискове, свързани с възможно неправилно функциониране на тези системи и с предубеденост, която те могат да породят. Според данните от научни изследвания, софтуерът, който се използва за идентифициране, разпознаване или анализ на лица, функционира с различна ефективност в зависимост от възрастта, пола и етническия произход на лицата. Алгоритмите могат да се използват по отношение на различни демографски групи, поради което наличието на необективност или отклонения при разпознаването на лица може да задълбочи предразсъдъците в обществото.

Какво всъщност представлява лицевото разпознаване?

Лицевото разпознаване е технология, която използва изкуствен интелект (ИИ), за да разпознае или потвърди самоличността на човек чрез анализ на неговите лицеви характеристики. Системата за лицево разпознаване засича лице в снимка или видео, измерва уникални характеристики като разстоянието между очите, формата на носа или линията на челюстта и ги сравнява с вече съхранени данни. Често се използва за отключване на телефони, видеонаблюдение, летищен контрол, сигурност и дори за автоматично отбелязване (тагване) на хора в снимки в социалните мрежи.

Доколкото лицевото разпознаване се осъществява на базата на изкуствен интелект, приложение намира и Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 година за установяване на хармонизирани правила относно изкуствения интелект (Акт за изкуствения интелект), чиито основи разпоредби (глави I и II) вече се прилагат, считано от 2 февруари 2025 г. В съображение 15 от същия се посочва, че понятието „биометрична идентификация“, следва да се определи като автоматизираното разпознаване на физически, физиологични и поведенчески характеристики на човека, например лице, движение на очите, форма на тялото, глас, ритъм и интонация на говора, походка, стойка, сърдечен ритъм, кръвно налягане, мирис и особености на натиска на клавиши, с цел установяване на самоличността на дадено лице чрез сравняване на биометрични данни на това лице със съхранени биометрични данни на лица в референтна база данни.

Актът за ИИ въвежда и понятието „биометрично категоризиране“. То се дефинира като отнасяне на физически лица към конкретни категории въз основа на техните биометрични данни. Подобни конкретни категории могат да са свързани с аспекти като пол, възраст, цвят на косата, цвят на очите, татуировки, поведенчески или личностни черти, език, религия, принадлежност към национално малцинство, сексуална или политическа ориентация. В този смисъл въвеждането в системата за видеонаблюдение на един магазин на данни за лицевите изображения на лица, които са извършили кражба на стоки от същия, води несъмнено до тяхното биометрично категоризиране.

Тъй като биометричните данни представляват специална категория лични данни, е целесъобразно да се класифицират като високорискови няколко случая на критично използване на биометрични системи, доколкото тяхното използване е разрешено съгласно съответното право на Съюза и национално законодателство. Техническите неточности на системите с ИИ, предназначени за дистанционна

биометрична идентификация на физически лица, могат да доведат до опорочени от предубеденост резултати и до дискриминация. Рискът от такива опорочени от предубеденост резултати и дискриминация е от особено значение във връзка с възраст, етническа принадлежност, раса, пол или увреждане. Поради това системите за дистанционна биометрична идентификация следва да бъдат класифицирани като високорискови с оглед на рисковете, които поражда. Тази класификация изключва системите с ИИ, предназначени да бъдат използвани за биометрична проверка, включително за удостоверяване на самоличността, чиято единствена цел е да се потвърди, че конкретно физическо лице е лицето, за което се представя, и да се потвърди самоличността на физическо лице единствено за да се получи достъп до услуга, да се отключи устройство или да се придобие сигурен достъп до помещения. Освен това следва да бъдат класифицирани като високорискови системите с ИИ, предназначени да се използват за биометрично категоризиране в съответствие с чувствителни признаци или характеристики, защитени съгласно чл. 9, пар. 1 от Регламент (ЕС) 2016/679, въз основа на биометрични данни, доколкото те не са забранени съгласно Акт за изкуствения интелект, и системи за разпознаване на емоции, които не са забранени съгласно същия акт. Биометричните системи, които са предназначени да се използват единствено с цел да се позволи предприемането на мерки за киберсигурност и за защита на личните данни, не следва да се считат за високорискови системи с ИИ (съображение 54 от Акта за ИИ).

За целите на настоящия анализ заслужава да се отбележи, че Актът за ИИ, като специален нормативен акт за защита на физическите лица по отношение на обработването на лични данни чрез използването на системи с ИИ, въвежда множество рестрикции за дистанционна биометрична идентификация, дори когато се извършва от правоохранителните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления (вж. чл. 5 „Забранени практики в областта на ИИ“ от Акта за ИИ).

В т. 82 от своите Насоки № 3/2019 относно обработването на лични данни чрез видеоустройства Европейският комитет по защита на данните счита (ЕКЗД) посочва, че когато администратор на данни желае да установи повторно влизане на субект на данни в зоната под наблюдение, целта би била уникално идентифициране на физическо лице, което означава, че от самото начало операцията попада в обхвата на чл. 9 от ОРЗД. Тъй като системата използва физически характеристики, за да установи конкретни физически лица, които навлизат повторно в обхвата на камерите (напр. посетители на търговски център) и да ги проследява, се използва технология за биометрично идентифициране, тъй като целта е разпознаване посредством специфично техническо обработване.

ЕКЗД отбелязва, че някои биометрични системи са инсталирани в неконтролирана среда, което означава, че системата заснема в движение лицата на всички физически лица, които влизат в обхвата на камерите, включително лицата, които не са дали съгласието си за използване на биометричното устройство, и по този начин създава биометрични модели. Тези модели се сравняват с моделите, създадени за субект на данни, чиито образи са предварително въведени в база данни, за да може администраторът на данните да установи дали съответното лице е потребител на биометричната технология. В подобни случаи, какъвто е и настоящият, често системата е настроена да разграничава физическите лица, които трябва да разпознава въз основа на база данни, от лицата, които не са регистрирани. Тъй като целта е уникално идентифициране на физически лица и в този случай е необходимо изключение от разпоредбата на чл. 9, пар. 2 от ОРЗД за всички лица, заснети (сканирани) от камерите.

За да бъде обработването на лични данни законосъобразно, то трябва да се осъществява въз основа на някое от правните основания, посочени в чл. 6, пар. 1, първа алинея и/или чл. 9, пар. 2 от ОРЗД, както и да бъдат приложени ефективно принципите за обработването им, прогласени в чл. 5 от същия. Обработването на биометрични данни за целите единствено на идентифицирането на физическо лице по правило е забранено (вж. чл. 9, пар. 1 от ОРЗД), но може да се осъществява при наличие на някое от изключенията по чл. 9, пар. 2, б. „а“ – „й“ от ОРЗД.

Изложеният в искането правен анализ за приложимост на условието по чл. 9, пар. 2, б. „ж“ от ОРЗД (обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността

на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните) не може да бъде споделен поради следните съображения:

Освен правна, понятието „обществен интерес“ има и нравствено-етична величина, която се променя с развитието на едно общество, поради което е изключително трудно, а и рисковано, да бъде дефинирано в нормативен акт, който има за цел да урежда трайни обществени отношения. Както много други нормативни актове, в които се използва, така и ОРЗД не въвежда легална дефиниция на понятието „обществен интерес“. Въпреки това неговите основни характеристики могат да бъдат извлечени от правната доктрина и юриспруденция. Според тях „обществен интерес“ означава това, което е важно, полезно или необходимо за доброто на обществото като цяло, а не за отделен човек, група или организация. Общественият интерес следва да се разбира като съвкупност от ценности, цели или действия, които служат за защита, развитие или благосъстояние на цялото общество или на значителна част от него.

Общественият интерес намира проявление в области като:

- сигурността и здравето на гражданите;
- опазване на околната среда;
- осигуряване на прозрачност в управлението;
- подобряване на образованието и здравеопазването;
- гарантиране свободата на словото и правото на информация;
- противодействие на корупцията и изпирането на пари;
- обезпечаване на демократичността на изборния процес и пр.

ОРЗД изисква общественият интерес или критериите за неговото определяне да бъдат установени в правото на Съюза или в правото на държава членка, което е пропорционално на преследваната цел, защита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните. Това правно основание може да включва конкретни разпоредби за адаптиране на прилагането на ОРЗД, *inter alia* общите условия, които определят законосъобразността на обработването от администратора, видовете данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани лични данни, и целите, за които се разкриват; ограниченията по отношение на целите на разкриването; периодът на съхранение и операциите и процедурите за обработване, включително мерки за гарантиране на законосъобразното и добросъвестно обработване, като тези за други конкретни случаи на обработване, предвидени в глава IX на ОРЗД. Правото на Съюза или правото на държавата членка трябва да се съобразява с обществения интерес и да е пропорционално на преследваната легитимна цел.

Въвеждането и последващото обработване на данни за лицевите изображения на клиенти, за които е констатирано, че са направили опит или са извършили кражба на стока от магазин, или са имали друго противоправно поведение, за целите на тяхното лицево разпознаване от система за видеонаблюдение при следващо посещение в обект на търговската верига, не може да представлява причина от важен обществен интерес по смисъла на чл. 9, пар. 2, б. „ж“ от ОРЗД. Такава причина, от една страна, трябва да е установена в законодателството, а от друга страна, трябва да отчита естеството на дейност на администратора на лични данни и да се явява необходима, подходяща и пропорционална мярка в едно демократично общество, която да гарантира отношения от важен обществен интерес. Кражбата или опитът за кражба в условията на „маловажен случай“ по Наказателния кодекс не може да бъде причина от важен обществен интерес по смисъла на ОРЗД, която да превърне клиентите на един магазин в „ходещи баркодове“.

Такава причина от важен обществен интерес може да бъде обезпечаването на сигурността в обекти на националната сигурност или елементи от критичната инфраструктура на страната. Например в атомна електроцентрала или в друго предприятие, чиято дейност е свързана с генериране на изключително високи рискове за живота и здравето на субектите на данни (напр. в областта на фармацевтичното

производство, производството на оръжия и боеприпаси, химическата промишленост, самолетостроенето и др. под.).

За пълнота на настоящия анализ трябва да се отбележи, че и никое от останалите по чл. 9, пар. 2 от Регламент (ЕС) 2016/679 условия за допустимост на обработването на биометрични данни, за целите единствено на идентифицирането на физическо лице, не намира приложение, и не може да обоснове планираното обработване на такива данни за посочените от искателя цели. В това число не е приложимо и съгласието на субектите на данни. Уведомяването на субектите на данни (чрез указателни табели/стикери и публикуването на известия за защита на личните данни), че се извършва видеонаблюдение с лицево разпознаване и тяхното фактическо влизане в търговски обект, не могат да бъдат тъждествени на даването на изрично съгласие по смисъла на чл. 9, пар. 1, б. „а“ от ОРЗД.

Формирането на отделен регистър с лицеви изображения на клиенти, за които е констатирано, че са направили опит или са извършили кражба на стока от магазин, като форма на последващо обработване на лични данни, не отговаря и на принципа за „ограничение на целите“ по чл. 5, пар. 1, б. „б“ от ОРЗД, както и на изискванията за обработване на данни за цели, различни от първоначалните, за които са били събрани (арг. чл. 6, пар. 4 от ОРЗД). Не на последно място, освен че обработването на данни за лицевите изображения на клиенти накърнява правото на защита на личните данни и неприкосновеността на личния им живот, то би породило и форми на дискриминация спрямо тях.

Поради всички тези причини планираното обработване се явява незаконосъобразно.

В подкрепа на това заключение е и практиката на други европейски надзорни органи по защита на личните данни:

1. През 2020 г. нидерландският надзорен орган по защита на личните данни (Autoriteit Persoonsgegevens) упражнява корективните си правомощия, като отправя към супермаркет официално предупреждение за това, че използваната от него система за видеонаблюдение с лицево разпознаване нарушава изискванията на ОРЗД. Информация за случая е публикувана на интернет страницата на ЕКЗД: https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en (Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology);

2. През 2021 г. испанският надзорен орган по защита на личните данни (Agencia Española de Protección de Datos) налага имуществена санкция в размер на 2,5 млн. евро на верига супермаркети за използването на система за видеонаблюдение с лицево разпознаване. Информация за случая е публикувана в интернет портала GDPRhub на следния линк: [https://gdprhub.eu/index.php?title=AEPD_\(Spain\)_-_PS/00120/2021](https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS/00120/2021)

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 и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Въвеждането и последващото обработване на данни за лицевите изображения на клиенти, за които е констатирано, че са направили опит или са извършили кражба на стока от магазин, или са имали друго противоправно поведение, за целите на тяхното лицево разпознаване от система за видеонаблюдение при следващо посещение в обект на търговската верига, не представлява причина от важен обществен интерес по смисъла на чл. 9, пар. 2, б. „ж“ от Регламент (ЕС) 2016/679.

2. Никое от останалите по чл. 9, пар. 2 от Регламент (ЕС) 2016/679 условия за допустимост на обработването на биометрични данни, за целите единствено на идентифицирането на физическо лице, не намира приложение, и не може да обоснове планираното обработване на такива данни за посочените от искателя цели. В това число не е приложимо и съгласието на субектите на данни. Това налага извода, че планираното обработване не съответства на изискванията на Регламент (ЕС) 2016/679, поради което се явява недопустимо.

3. Обработването на биометрични данни посредством технология за лицево разпознаване може

да се осъществява въз основа на причина от важен обществен интерес, когато тя е установена в правото на ЕС или националното законодателство, отчита естеството на дейност на администратора на лични данни и се явява необходима, подходяща и пропорционална мярка в едно демократично общество, която гарантира цел от важен обществен интерес.

4. Такава причина от важен обществен интерес може да бъде обезпечаването на сигурността в обекти на националната сигурност или елементи от критичната инфраструктура на страната.

ПРЕДСЕДАТЕЛ:

ВЕНЦИСЛАВ КАРАДЖОВ

ЧЛЕНОВЕ:

МАРИЯ МАТЕВА

ВЕСЕЛИН ЦЕЛКОВ

[1] След продажбата и интеграцията дружеството няма да отговаря за контрола върху разширеното видеонаблюдение с лицево разпознаване, нито за поддръжката му.

[2] Съгласно § 1, т. 3 от ДР на ЗЧОД „Видеонаблюдение“ е техническа форма на обработка и съхранение в предвидения в закона срок на лични данни, извършвани при спазване на изискванията за защита на личните данни и на разпоредбите и на този закон, свързани с изискванията при обработката на лични данни съгласно чл. 5 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ, L 119/1 от 4 май 2016 г.), включваща заснемане на лица в охраняван обект и запис на получените данни.

[3] Вж. т. 68 от Насоки № 3/2019 на Европейския комитет по защита на данните (ЕКЗД) относно обработването на лични данни чрез видеоустройства, публикувани на интернет страниците на ЕКЗД и КЗЛД.

[4] Повече информация може да се намери в Насоки № 05/2022 на Европейския комитет по защита на данните относно използването на технология за лицево разпознаване в областта на правоприлагането, публикувани на интернет страниците на ЕКЗД и КЗЛД.



Комисия за защита на личните данни

Председател: Борислав Божинов

Членове: Василка Рангелова

Ивайло Станев

Цветана Червенякова – Илиева

Цветелин Софрониев

Информационен бюлетин № 3 (114) 2025 г.

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

Уеб сайт на КЗЛД: www.cpdf.bg

Разпространява се в електронен вид

ISSN 2367-7759