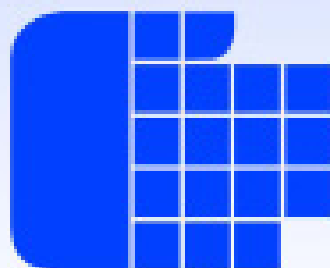


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 3 (102), май 2023 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода март и април 2023 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
КЗЛД депозира в Народното събрание Отчета си за 2022 година. Резюме на отчета	3
Приет е Правилник за изменение и допълнение на Правилника за дейността на КЗЛД и на нейната администрация	8
Започна въвеждането на системата за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения	9
КЗЛД издаде Указания за обработване на лични данни на непълнолетни при изпълнение на административно наказание	12
Председателят на КЗЛД Венцислав Караджов е кандидат за председател на Европейския комитет по защита на данните	16
Заседания на Европейския комитет по защита на данните	16
Европейският комитет по защита на данните започна своето второ координирано правоприлагащо действие	18
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	19
РЕШЕНИЯ НА КЗЛД	20
СТАНОВИЩА НА КЗЛД	27
СТАТИИ И КОМЕНТАРИ	35
Проф. Веселин Целков, член на КЗЛД - “Моделиране на взаимодействията в системата за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения”	35

СЪБИТИЯ И ИНИЦИАТИВИ

КЗЛД ДЕПОЗИРА В НАРОДНОТО СЪБРАНИЕ ОТЧЕТА СИ ЗА 2022 ГОДИНА РЕЗЮМЕ НА ОТЧЕТА



На 30 март 2023 г. Комисията за защита на личните данни депозира в деловодството на Народното събрание **Годишния отчет за дейността си през 2022 година**. Отчетът се състои от 149 страници, обособени в 12 основни раздела. Депозирани са съгласно чл. 7, ал. 6 от Закона за защита на личните данни и обхваща периода от 01.01.2022 г. до 31.12.2022 г. В Годишния отчет е представена информация по основните направления на дейност на КЗЛД и по ключови въпроси, обект на обществен интерес през

посочения период. Направен е анализ на степента на постигане на целите и приоритетите за отчетната 2022 г. и са дефинирани целите и приоритетите за 2023 г. Предоставена е обобщена информация относно разгледани жалби и сигнали, запитвания на граждани и проведените консултации по тях. Отчетена е постоянната тенденция на повишаване обема и сложността на постъпващите жалби и сигнали, както на извършваните проверки на администратори на лични данни. Направен е преглед на становища по обществено значими теми и отговори на запитвания на администратори и обработващи лични данни по въпроси с принципен характер.

През 2022 г. КЗЛД е сезирана с над 770 жалби, подадени от физически лица, с твърдения за нарушения при обработване на лични данни и упражняване на права. Подадените жалби се отличават с правна и фактическа сложност – повече от един жалбоподател и/или ответна страна; жалбоподатели, които не са български граждани или администратори на лични данни с основно място на установяване извън територията на Република България.

Запазва се тенденцията сектор „Видеонаблюдение“ да е водещ по брой жалби (178 бр.), като се наблюдават все повече колективни жалби – подадени от повече от едно физическо лице срещу един администратор на лични данни. Значително нараства и броят насрещни жалби. Продължава тенденцията по-голяма голяма част жалбите да са провокирани от дългогодишни конфликтни междуличностни проблеми на битово ниво. 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.

Ръст бележат жалбите, подадени срещу банки и дружества, предлагащи кредитни услуги (89 бр.) Основно твърденията са за неправомерно предоставяне на лични данни на колекторски фирми за събиране на задължения от физическите лица в хипотезата 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. Наблюдава се значително увеличение на жалбите, подадени срещу политически субекти (68 бр.). 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. Продължава тенденцията за увеличаване на броя на жалбите, подадени срещу физически лица, като през 2022 г. достига до 66 бр. и изпреварва броя на жалбите, подадени в сектор „Телекомуникации“ (49 бр.). Жалбите са предхождани от усложнени конфликтни отношения между страните и са насочени предимно срещу разпространение на лични данни в социални мрежи

и заснемане с мобилни средства на обществени места. Забелязва се увеличаване на броя жалби, подадени в сектор „Трудови и осигурителни услуги“ - 19 бр. Традиционно тези жалби касаят твърдения за злоупотреба с лични данни за регистрирани в НАП трудови договори, без такива да са сключвани.

Наблюдава се тенденция за драстично намаляване на броя жалби, подадени срещу държавни органи (33 бр.), като по-голяма част касаят упражняване на права или предоставяне на лични данни на трети лица без основание. Отчита се и намаляване на жалбите, подадени в сектор „Здравеопазване“ (18 бр.), както и на жалбите, подадени срещу медии (17 бр.), като се запазва относително големият процент на жалби, подадени срещу администратори на електронни медии. Други сектори, споменати в отчета, са „Застраховане“ (9 бр.) и „Образование“ (4 бр.).

С оглед крайното решение на КЗЛД произнасянията по жалби, разгледани през 2022 г. (392 бр.), са, както следва: по основателност на жалби – 225 решения (от тях за основателни са приети 143 жалби, а за неоснователни – 82); по недопустимост на жалби – 57 решения; по нередовност на жалби и искания – 74 решения; за очевидна неоснователност – 11 решения; за спиране на административно производство поради наличие на друго, образувано пред органите на МВР или прокуратурата – 1 решение. Оттеглените жалби са 24, с което КЗЛД на практика е била десезирана.

От разгледаните през 2022 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 2022 г. глоби и имуществени санкции в производството по чл. 38 от ЗЗЛД са в общ размер на 247 500 лв., почти двойно повече от размера на санкциите, наложени през 2021 г. Санкциите варират от 500 лв. (за нарушение на чл. 32 от ОРЗД) до 35 000 лв. (за нарушение на чл. 6, §1 от ОРЗД). В процес на принудително събиране от НАП към 31.12.2022 г. са санкции, наложени с Решения на КЗЛД, в размер на 655 058 лв., като през 2022 г. е събрана сума в размер на 20 500 лв. През 2022 г. са платени глоби и имуществени санкции в размер на 265 200 лева., а 56 000 лв. са в процес на събиране с покана за доброволно

Постановените от КЗЛД решения по жалби подлежат на двуинстанционен съдебен контрол по АПК. Анализът на съдебната практика показва много висок процент на потвърдени от съда решения на надзорния орган. През 2022 г. по жалби, подадени срещу постановени по този ред решения на КЗЛД, са образувани общо 109 първоинстанционни съдебни дела. Първоинстанционният съд се е произнесъл с решения по 110 дела, включително по такива, образувани и преди 2021 г. С 95 съдебни решения са потвърдени оспорените административни актове на КЗЛД, с 5 съдебни акта са частично изменени постановени от КЗЛД решения в санкционната част, отменени на първа инстанция са 10 издадени от КЗЛД решения.

През 2022 г. пред Върховния административен съд (ВАС), като касационна инстанция, са образувани 60 дела. ВАС се е произнесъл с решения по 59 дела, в това число такива, образувани преди 2021 г., като е потвърдил 38 издадени от КЗЛД индивидуални административни акта, 8 решения на КЗЛД са отменени изцяло, едно решение е отменено и върнато за ново разглеждане от КЗЛД, отменени са три решения на първоинстанционния съд и преписките са върнати за ново разглеждане от съда.

Сигналите и запитванията са регламентиран способ за публичен контрол върху спазването на нормативните актове по отношение на личните данни. От подадените 394 бр. сигнали и искания за упражняване на надзорни правомощия са приключени 380 бр., като са изпратени съответни отговори, а при необходимост получените сигнали са изпращани и на съответните органи или институции за произнасяне по компетентност.

Значителен брой запитвания и сигнали са получени срещу администратори на лични данни, предоставящи интернет услуги и on-line търговия – 75 бр. На следващо място са сигнали в сектор банково дело и кредитна дейност – 36 бр., следвани от сигнали за незаконосъобразно обработване

на лични данни от администратори на лични данни, органи на държавната администрация – 29 бр., и такива за целите на директния маркетинг – 26 бр. Постъпили са сигнали срещу администратори, обработващи лични данни чрез изградени системи за видеонаблюдение – 23 бр., както и такива в сферите на търговията и услуги – 21 бр., и телекомуникациите – 21 бр. Част от сигналите касеа незаконосъобразно обработване на лични данни в областта на пощенските услуги – 16 бр., сферата на здравеопазването – 15 бр., дружества с предмет на дейност хазарт – 14 бр., сайтове за търсене и предлагане на работа и/или сектор човешки ресурси – 14 бр., в сферата на политиката – 13 бр. Сигналите в други сектори са общо 91 бр. Постъпилите сигнали и искания през 2022 г. са многобройни и разнородни по своето естество. Прави впечатление, че субектите на данни са добре запознати с правата си по Регламент (ЕС) 2016/679 и ЗЗЛД.

В качеството ѝ на национален надзорен орган КЗЛД прилага механизъм за ефективен надзор 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 и 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.

През 2022 г. са назначени 324 бр. проверки на място по повод постъпили в КЗЛД жалби, искания и сигнали, като 32 бр. от тях са назначени в края на 2021 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 12 бр. Изцяло приключили с констативен акт и решение на КЗЛД са 264 бр.

Във връзка с нестабилната политическа обстановка и множество изборни процеси и подписки за референдуми – местни и национални, през отчетния период в сектор политика са извършени 46 проверки. В сектор здравеопазване са извършени 8 бр. проверки, в държавната администрация – 6 бр., в сферата на търговията и услугите – 5 бр., в сферата на образованието и обучението – 4 бр., в сектор телекомуникации – 4 бр., в областта на информационните технологии – 4 бр. В отчета е предоставена информация за някои по-значими проверки и интересни казуси.

Наложените от КЗЛД корективни мерки за констатирани след извършени проверки по постъпили сигнали за нарушения са 90 бр., от които 72 бр. разпореждания, 9 бр. официални предупреждения и 9 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. 6, §1 от Регламент (ЕС) 2016/679 и чл. 38, §6 от Регламент (ЕС) 2016/679, чл. 25г от ЗЗЛД, чл. 25е от ЗЗЛД. За 5 бр. решения с издадени корективни мерки са наложени санкции в общ размер на 68 500 лв. От тях обжалвани са 3 бр. решения, които са в съдебна фаза; 1 бр. е влязло в сила и наложената санкция в размер на 2000 лв. е платена доброволно; 1 бр. решение е в процес на връчване и не е влязло в сила.

Въз основа на извършени проверки по искания и сигнали за 2022 г. са съставени 32 бр. акта за установяване на административни нарушения, издадени са 13 бр. наказателни постановления. От издадените наказателни постановления към края на отчетния период 3 бр. са обжалвани и са в съдебна фаза, а останалите 10 бр. са в процес на връчване. 10 бр. административнонаказателни производства са приключени с „предупреждение“ по чл. 28 от ЗАНН, а по 4 бр. са сключени споразумения на основание чл. 58г от ЗАНН. През 2022 г. **с наказателни постановления на председателя на КЗЛД са наложени санкции** на стойност 1 024 000 лв. В процес на принудително събиране от НАП към 31.12.2022 г. са санкции, наложени с НП, в размер на 75 631 лв., като през 2022 г. е събрана сума в размер на 6771 лв. От наложените с НП санкции през 2022 г. са платени общо 28 000 лв., а 3000 лв. са в процес на събиране с покана за доброволно изпълнение. Със сключени 4 бр. споразумения по административнонаказателни производства са наложени имуществени санкции в размер на 3700 лв.

Общо от наложените през 2022 г. глоби и имуществени санкции в решенията по жалби и наказателните постановления, към края на отчетния период в процес на принудително събиране от НАП са 730 689 лв. Към 31.12.2022 г. са събрани суми в общ размер 320 471 лв., от които 27 271 лв. са принудително събрани от НАП, а 293 200 лв. са платени доброволно. В процес на събиране с покани за доброволно изпълнение са глоби и санкции общо в размер на 59 000 лв.

Относно **уведомленията за нарушение на сигурността на данните**, за отчетния период в КЗЛД са получени общо 80 уведомления, като се констатира многообразие на секторите на дейност на подадите уведомления администратори: държавни институции – 10 бр.; учебни заведения – 5 бр.; болници – 3 бр. Общо 62 бр. са администратори с разнообразен предмет на дейност. От регистрираните пробиви на сигурността на данните 25% засягат публични институции (държавни и образователни структури), а останалите са от частния сектор. От общо подадените уведомления 16 са преценени с ниско ниво на риск 27 със средно ниво на риск и 8 - с високо ниво на риск. При 15 от случаите, свързани с нарушения на сигурността на личните данни, има трансгранично обработване, което налага КЗЛД да се конституира като засегнат надзорен орган (ЗНО) и да се регистрира като такъв в Информационната система на вътрешния пазар (ИСВП).

През 2022 г. Комисията е била сезирана и е изразила 32 **становища** по различни въпроси в областта на защитата на личните данни. Във връзка с това в отчета е предоставена подробна информация и разяснения по ключови въпроси от обществен интерес. През 2022 г. КЗЛД е изразила 22 становища по различни казуси, поставени за разглеждане както от публични органи, така и от физически и юридически лица. Наред с това са изразени 4 становища по съгласувателни процедури по реда на Устройствения правилник на Министерския съвет и неговата администрация и 6 становища по законопроекти, предложени за разглеждане в Народното събрание. В допълнение, през 2022 г. КЗЛД е изразила становища по три преюдициални запитвания, които са предложени и приети като част от формиране на позицията на Република България пред Съда на ЕС.

И през отчетната година КЗЛД е извършила **преглед на действащото национално законодателство за съответствие с правилата за защита на личните данни** и е информирала заинтересованите страни за необходимостта от актуализиране или цялостно изменение на конкретни нормативни актове. В рамките на постоянното си задължение и приоритет за преглед на законодателството през 2022 г. КЗЛД е допълнила списъка на нормативните актове, за които се налага изменение и/или допълнение, с нови петнадесет такива.

През 2022 г. КЗЛД е предоставила множество формални писмени (660 бр.) и неформални устни **консултации на граждани и администратори** (7837 бр.) по въпроси, свързани с обработването на лични данни и тяхната защита, в т.ч. както под формата на официални становища, така и отговори/разяснения на конкретни запитвания по принципни въпроси от областта на защитата на личните данни с цел унифициране на практиката в национален план. За поредна година се отчита преобладаване на въпросите, свързани със законосъобразното извършване на видеонаблюдение и обработването на лични данни по реда на Закона за управление на етажната собственост. Постъпили са запитвания относно упражняването на право на достъп до лични данни и разликата с правото на достъп до официални документи. Комисията получава и множество запитвания по отношение на възможността за упражняването на правото на изтриване на лични данни, обработвани от финансови институции. И през 2022 г. продължава постъпването на запитвания, с които физически лица се интересуват как да спрат да получават търговски съобщения.

В изпълнение на задължението за поддържане на **публичен регистър на администраторите и обработващите, които са определили длъжностни лица по защита на данните**, през 2022 г. регистрираните в публичния регистър АЛД или ОЛД, определили ДЛЗД, са 461 бр., с което общият им брой става 5536. Данните в регистъра се набират от подадените уведомления чрез попълване на утвърден образец.

В своя отчет за 2022 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 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 2022 г. Посочено е, че на всички граждани и организации, заявили достъп до обществена информация, е предоставена такава през 2022 г. в законовия срок.

По отношение на **международната дейност**, през 2022 г. приоритет остава 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 от сферата на защитата на личните данни. Осъществено е участие в 173 бр. заседания на формати, обединяващи сродни органи по защита на данните на държавите – членки на ЕС, включително заседания на Европейския комитет по защита на данните (ЕКЗД), заседанията на изпълнителното бюро на консултативния комитет към Конвенция 108+ на Съвета на Европа и на Работна група „Обмен на информация и защита на данните“ (DAPIX), формат „Защита на данните“. През 2022 г. КЗЛД е била адресат/инициатор/участник в механизма за сътрудничество и съгласуваност чрез Информационна система на вътрешния пазар (ИСВП) в 100 бр. процедури.

През 2022 г. КЗЛД участва активно в подготовката на Република България за членство в Организацията за икономическо сътрудничество и развитие (ОИСР). Присъединяването към Организацията за икономическо сътрудничество и развитие е сред основните цели на външната политика на Република България. През отчетния период продължава ползотворното междунституционално сътрудничество с Министерството на външните работи.

През 2022 г. КЗЛД продължава да изпълнява в пълен обем дейностите по осигуряване **пълноправното присъединяване на Република България към Шенген**. През октомври 2022 г. представители на КЗЛД вземат участие в „Доброволната мисия за установяване на фактите“ за Република България по Шенген, при която е извършена цялостна проверка в областта на защитата на личните данни. Представителите на Европейската комисия са оценили нивото на представянето на Република България като изключително, а впоследствие в съобщение за медиите от 16 ноември 2022 г. Европейската комисия „... потвърди, че България и Румъния не само продължават да прилагат новите правила и инструменти, но и значително са засилили цялостното прилагане на шенгенската архитектура във всичките ѝ измерения. Освен това тези две държави доказаха, че имат отлични резултати по отношение на прилагането на шенгенските правила“.

В отчета е предоставена подробна информация за институционалното взаимодействие, информационно-образователната дейност, медийната политика, административния капацитет и финансовото състояние на КЗЛД. Отразено 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 2022 г. Със Закона за държавния бюджет на Република България (ЗДБРБ) за 2022 г. е утвърден бюджетът за дейността на КЗЛД в размер на 3 732 700 лв. През годината по него не са извършвани промени. За обезпечаване на дейността на Комисията за защита на личните данни и нейната администрация са извършени разходи общо в размер на 3 621 225 лв., или 97,01% от утвърдените разчети за годината.

В края на годишния си отчет КЗЛД формулира следните цели и приоритети за 2023 г.:

- Финализиране на подзаконовата правна уредба в областта на защитата на личните данни.
- Създаване на необходимите законови предпоставки за започване на прилагането на Закона

за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения;

- Продължаване на усилията на КЗЛД за пълноправно членство в Шенген.
- Допълнителни правомощия на КЗЛД във връзка с новите широкомащабни информационни системи на ЕС.
- Изграждане на нов подход в защитата на личните данни от КЗЛД, свързан с предизвикателствата на новите технологии.
- Прилагане на нов подход в предоставянето на обучение в сферата на защита на данните, вкл. съвременните заплахи пред защитата на данните.
- Продължаване на усилията на КЗЛД за пълноправно членство в ОИСР.
- Устойчиво прилагане на цифрови подходи в административната дейност на КЗЛД в съответствие с изискванията за дигитализация на администрацията в Република България.
- Фокусиране дейността на КЗЛД в защита на личните данни на деца в интернет пространството и социалните мрежи.
- Засилено трансгранично и международно сътрудничество.

Годишният отчет на КЗЛД за 2022 г. е публикуван на институционалния сайт – [ТУК](#).

ПРИЕТ Е ПРАВИЛНИК ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ПРАВИЛНИКА ЗА ДЕЙНОСТТА НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И НА НЕЙНАТА АДМИНИСТРАЦИЯ

На 28 април 2023 г. в бр. 38 на Държавен вестник е обнародван [Правилник за изменение и допълнение на Правилника за дейността на Комисията за защита на личните данни и нейната администрация](#).

В периода от 31 март до 14 април 2023 г. се проведе обществено обсъждане на проект на Правилник за изменение на Правилника за дейността на Комисията за защита на личните данни и нейната администрация. Информация относно общественото обсъждане е публикувана на [Портала за обществени консултации](#) и на [институционалния сайт на КЗЛД](#).

КЗЛД е постоянно действащ независим надзорен орган в областта на защитата на личните данни и осъществява контрола по спазването на [Общия регламент относно защитата на данните \(GDPR, ОРЗД\)](#) и [Закона за защита на личните данни](#).

В допълнение, с влизането в сила на [Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения \(ЗЗЛПСПОИН\)](#), считано от 4 май 2023 г. КЗЛД ще осъществява и функциите на Централен орган за външно подаване на сигнали и за защита на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, станала им известна при или по повод изпълнение на трудовите или служебните им задължения или в друг работен контекст.

В изпълнение на § 8 от Заключителните разпоредби на ЗЗЛПСПОИН, в тримесечен срок от обнародването на този закон Комисията е задължена да приведе правилника за дейността си в съответствие с него. С Правилника се предприемат мерки по чл. 22 от ЗЗЛПСПОИН, който изисква създаване на самостоятелно структурно звено в структурата на КЗЛД, изпълняващо функциите на канал за външно подаване на сигнали. За тази цел се създава дирекция „Канал за външно подаване на сигнали“ като част от специализираната администрация на институцията, разписват се нейните функционални задължения и се разработват правила за разглеждане на сигнали за нарушения в

рамките на самостоятелно производство пред Комисията по силата на новия закон. Актуализират се и редица други разпоредби на Правилника на КЗЛД и на нейната администрация с цел отчитане на новите правомощия на Комисията, произтичащи от ЗЗЛПСПОИН.

Същевременно, с измененията и допълненията се оптимизират правилата за работа на КЗЛД и нейната администрация по линия на Регламент (ЕС) 2016/679 и ЗЗЛД. Натрупаната практика по прилагане на новата правна рамка в областта на защитата на личните данни (считано от 25 май 2018 г., когато започва изпълнението на Общия регламент относно защитата на данните) позволява актуализиране на редица разпоредби в правилника на Комисията, така че да се гарантира високо ниво на защита на физическите лица и безпрепятствено изпълнение на задачите и правомощията на надзорния орган. Затова в правилник са предвидени промени, които са свързани с функционалните задължения на дирекциите от специализираната администрация, съответните административни производства и значително увеличения обем от работа след 25 май 2018 г.

Очакваните резултати са пряко свързани със създаването на нормативни и практически условия за изпълнение на задачите на КЗЛД по ЗЗЛПСПОИН, подобряване на качеството на надзорната дейност в областта на защитата на личните данни и оптимизиране на сроковете за произнасяне по ключови въпроси по ОРЗД и ЗЗЛД.

ЗАПОЧНА ВЪВЕЖДАНЕТО НА СИСТЕМАТА ЗА ЗАЩИТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАЩИ ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ

На 4-ти май 2023 г. влезе в сила **Законът за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения** (ЗЗЛПСПОИН). Законът е публикуван в бр. 11 на Държавен вестник от 02.02.2023 г. С него се уреждат условията, редът и мерките за защита на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, които застрашават или увреждат обществен интерес и правото на Европейския съюз, както и редът и условията за подаване и разглеждане на такива сигнали или публично оповестена информация.

Законът въвежда задължение за изграждане на национален механизъм за защита на лицата, подаващи сигнали или публично оповестяващи информация, както и за извършване на проверка и предприемане на действия по всеки сигнал. Предвидени са задължения за създаване на канали за вътрешно и външно подаване на информация за нарушения, като **КЗЛД е определена да действа като централен орган за външно подаване на сигнали**.

КЗЛД прие и на 10 март 2023 г. публикува на своя институционален сайт „Пътна карта“, която очертава основните етапи по въвеждането на системата за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. В съответствие със сроковете, определени в закона, Пътната карта очертава 4 основни времеви етапа и детайлизира конкретните и належащи задачи, произтичащи от него:

Първи етап – в 3-месечен срок от обнародването на ЗЗЛПСПОИН (до 04.05.2023)

- Анализ на информационната инфраструктура на КЗЛД с цел ресурсно осигуряване на Комисията за изпълнение на вменените ѝ нови задължения по ЗЗЛПСПОИН;
- Откриване на обществените поръчки за ресурсното осигуряване на КЗЛД;
- Изменение, обществено обсъждане, отразяване на коментари и предложения и обнародване на **Правилника за дейността на КЗЛД и нейната администрация**;
- Изработване и публикуване на указания към сигнализиращите лица и към задължените субекти по чл. 12 за организиране на вътрешно подаване на сигнали;

- Разработване на **образец на формуляр за приемане на сигнали по ЗЗЛПСПОИН**;
- Приемане на **модел на Регистър на сигналите по ЗЗЛПСПОИН**;
- Публикуване на сайта на КЗЛД на **информацията по чл. 21 от ЗЗЛПСПОИН**;
- Инициране на предварителна среща на КЗЛД с компетентните органи по чл. 20 от ЗЗЛПСПОИН за обсъждане на практическата реализация на закона;
- Реализиране на първоначални информационни събития с оглед развитието на правната рамка и нейните адресати, както и задълженията за публичност и поверителност – разработване и разпространение на тематични информационно-разяснителни материали за сигнализиращи лица, за задължените субекти по чл. 12 и за компетентните органи по чл. 20;
- **Поставяне начало на национална информационна кампания.**

Втори етап – в 6-месечен срок от обнародването на ЗЗЛПСПОИН (до 04.08.2023):

- Въвеждане в експлоатация на информационната система на КЗЛД, предназначена за канал за външно подаване и приемане на сигнали;
- Изработване, обществено обсъждане, отразяване на коментари и предложения и обнародване на Наредба за воденето на регистър и за препращане на вътрешните сигнали по ЗЗЛПСПОИН;
- Започване подготовката за провеждане на предстоящи обучения. Идентифициране на проблемни области, грешки, често възникващи въпроси и др. предизвикателства по приложението на правната рамка.

Трети етап – 11 месечен срок (до 04.01.2024 г.)

- Приемане на условия и ред за разглеждане с приоритет на сигнали за тежки нарушения;
- **От 17.12.2023 г.** – започва прилагане на ЗЗЛПСПОИН от работодателите в частния сектор, които имат между 50 и 249 работници и служители.

Четвърти етап – след 15 месеца (от 04.05.2024 г.)

- Изпълнение на задължението на КЗЛД за ежегодно предоставяне на статистическа информация на Европейската комисия и публикуването ѝ на институционалния сайт при спазване изискванията за защита на личните данни и на Закона за защита на класифицираната информация;
- Изпълнение на задължението най-малко веднъж годишно да се организира обща среща с органите по чл. 20, на която се анализира дейността по работа със сигналите, както и с цел събиране на статистическите данни за нуждите на изготвянето на доклада до Европейската комисия;
- КЗЛД редовно и най-малко веднъж на три години следва да преразглежда своите правила за външно подаване на сигнали и за последващи действия по тях, да извършва анализ на практиката по прилагането на този закон и при необходимост актуализира правилата.

На 10 март 2023 г. КЗЛД публикува на сайта си **Пътна карта за изпълнение на ЗЗЛПСПОИН** и предостави информация относно непосредствените предстоящи стъпки за започване прилагането на закона. В информацията КЗЛД обръща внимание, че от 4 май 2023 г. работодателите от публичния и частния сектор, които се явяват задължени субекти по чл. 12, ал. 1 от ЗЗЛПСПОИН (*с изключение на работодателите в частния сектор, които имат между 50 и 249 работници или служители, за които тази дата е 17 декември 2023 г.*) имат задължение да осигурят възможност за вътрешно подаване на сигнали по смисъла на закона. За тази цел на 4 май 2023 г. на сайта на КЗЛД е стартирана **функционалност за генериране на Уникален идентификационен номер (УИН) на сигнал**, който ще следва да се взима от определените по чл. 14 от закона служители, отговарящи за разглеждането на сигнали. Този номер ще се използва от тях за нуждите на регистриране на подадените до задължените субекти сигнали. Функцията на УИН е гарантирането, че всеки постъпил сигнал при задължените

субекти ще бъде регистриран и разгледан. Чрез издаването на УИН се осигурява отчетност и проследимост на всеки сигнал във връзка с контролните правомощия на КЗЛД, задължението ѝ за предоставяне на статистическа информация към Европейската комисия по чл. 22, както и задълженията на субектите по чл. 12 от ЗЗЛПСПОИН.

За получаването на УИН служителът, отговарящ за разглеждането на сигнала ще трябва да предостави следната информация:

- Наименование и ЕИК/БУЛСТАТ на работодателя, при когото е подаден сигналът;
- Идентификационни данни на служителя, отговарящ за разглеждането на сигнала;
- Предмет на сигнала (съответните области, предвидени в чл. 3, ал. 1 и ал. 2 от ЗЗЛПСПОИН);
- Начин на получаване (писмено или устно).

На 19 април 2023 г. КЗЛД утвърди **Формуляр за подаване на сигнал** и модел на **Регистър на сигналите**. Същите са предоставени за използване от всички задължени по ЗЗЛПСПОИН субекти и са налични на сайта на КЗЛД в раздел „**Утвърдени от КЗЛД образци по ЗЗЛПСПОИН**”.

На 28 април 2023 г. в Гранд Хотел София се проведе кръгла маса на тема „**Популяризиране на влизането в сила на Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения – въпроси и отговори**“. Събитието бе организирано от КЗЛД съвместно с Базелския институт за управление и Българския институт за правни инициативи. Целта е да бъдат представени и обсъдени основни въпроси, свързани с техническата организация и правните аспекти по прилагането на ЗЗЛПСПОИН. Поради големия интерес към него и ограничения брой места, присъствието бе организирано с покани.

Председателят на КЗЛД, Венцислав Караджов и членът на КЗЛД Цанко Цолов представиха особеностите на канала за вътрешно подаване на сигнали и на канала за външно подаване на сигнали за нарушения. Проф. Веселин Целков, член на КЗЛД разясни модела на системата за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Членът на КЗЛД Мария Матева говори за осигуряване защита и възможност на лицата за подаване сигнали за нередности без страх от последващи репресивни действия, както и за роля на КЗЛД в този процес.

От друга страна, Цветомир Тодоров от Български институт за правни инициативи и адв. Михаил Бояджиев представиха Директива (ЕС)2019/1937 за защитата на лицата, които подават сигнали за нарушения, и разгледаха въпросите за отговорността за вреди при транспониране на тази директива. Адв. Йордан Владов и Мария Йорданова, главен експерт в Правна програма на Центъра за изследване на демокрацията говориха за исковете за вреди, причинени на сигнализиращите лица и разгледаха възможностите за защита на правата на сигнализиращите лица.

Мероприятието е **част от националната информационна кампания на КЗЛД** по темата и на него бяха представени и обсъдени новите елементи в сигнализирането и защитата на лицата, подаващи сигнали, както и новата роля и отговорности на институциите и частния бизнес при изпълнението на Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. На сайта на КЗЛД са публикувани изнесените на Кръглата маса презентации - **ТУК**.

КЗЛД ИЗДАДЕ УКАЗАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА НЕПЪЛНОЛЕТНИ ПРИ ИЗПЪЛНЕНИЕ НА АДМИНИСТРАТИВНО НАКАЗАНИЕ

Във връзка с постъпил сигнал относно практика за публикуване на информация на интернет страниците на общините, на свое редовно заседание, проведено на 29 март 2023 г. КЗЛД прие следните указания:

УКАЗАНИЯ

на

Комисията за защита на личните данни за обработване на лични данни на непълнолетни лица при изпълнение на административното наказание „обществено порицание“

В Комисията за защита на личните данни (КЗЛД) постъпи сигнал относно наложена практика по публикуване на интернет страниците на общините на обявления за наложени административни наказания „обществено порицание“ на непълнолетни лица. Чрез тях се оповестяват публично, до неограничен брой лица и за неограничен срок, имената на непълнолетните лица, данни за точния им адрес и извършеното от тях нарушение. Отчитайки високата обществена значимост на сигнала, както и необходимостта от привеждане на изпълнението на административното наказание „обществено порицание“, съгласно действащия Закон за административните нарушения и наказания (ЗАНН), в съответствие с нормативните изисквания за защита на личните данни, КЗЛД счита, че се налага да бъдат дадени навременни и конкретни указания към ангажираните с тази дейност администратори на лични данни (административни органи) – административнонаказващите органи, общините и създадените към тях местни комисии за борба срещу противообществените прояви на малолетните и непълнолетните.

I. Недопустимост за публикуване в интернет

В изпълнение на чл. 12 от ЗАНН административните наказания се налагат с цел да се предупреди и превъзпита нарушителят към спазване на установения правен ред и да се въздейства възпитателно и предупредително върху останалите граждани. Наказанието „обществено порицание“ се изразява в публично порицание на нарушителя пред трудовия колектив, където работи, или пред организацията, в която членува (чл. 14 ЗАНН). Когато е наложено наказанието „обществено порицание“, препис от наказателното постановление или решението на съда се изпраща на съответната обществена организация, в която наказаният членува, или на ръководството на предприятието, учреждението или организацията, където той работи, съобразно указаното в наказателното постановление или решението на съда (чл. 75 ЗАНН). Изпълнението на наказанието става чрез прочитане на наказателното постановление или решението на съда пред събрание на обществената организация или трудовия колектив, на което се поканва да присъства и нарушителят (чл. 76 ЗАНН).

Горепосочените норми определят както начините за изпълнение на наказанието, така и кръга от лица, пред които може да се изпълни. Видно от законовите текстове кръгът от лица, пред които може да се оповести наказанието, е свързан с трудовия колектив или обществената организация, в която наказаният членува (т.е. той е законово ограничен). Съгласно чл. 10 от Регламент (ЕС) 2016/679 обработването на лични данни, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност, въз основа на чл. 6, пар. 1 от същия, се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни. Видно от нормата на чл. 76 от ЗАНН законодателят не е предвидил хипотеза, при която изпълнението на наказанието „обществено порицание“ да става по друг начин, неопределен в закона, а именно чрез обявяване в

интернет, респ. не е въвел и подходящи гаранции за правата и свободите на субектите на данни, които да отчитат рисковете от подобно обработване на лични данни чрез публичното им разпространение.

Публикуването на лични данни в интернет, по подразбиране, представлява действие по разгласяването им пред неограничен кръг от лица от цял свят (вж. Решение от 06.11.2003 г. на Съда на ЕС по дело Bodil Lindqvist, C-101/01). От гледна точка на защитата на личните данни, такова публикуване винаги е свързано с повишени рискове за основните права и свободи на физическите лица. Тези рискове могат да доведат до физически, материални или нематериални вреди, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на личните данни, защитени от професионална тайна, или други значителни икономически или социални неблагоприятни последствия. В тези случаи субектите на данни могат да бъдат лишени от свои права и свободи, както и от упражняване на контрол върху своите лични данни, особено когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в професионална организация. Същото се отнася и за обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот, както и за присъди **и нарушения** или свързани с тях мерки за сигурност. Рискове могат да възникнат и когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или **поведението**, местонахождението или движенията в пространството, с цел създаване или използване на лични профили. Когато се обработват лични данни на уязвими лица, **по-специално на деца** или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни е задължително да се въведат и прилагат подходящи мерки за тяхната сигурност (съобр. 75 на Регламент (ЕС) 2016/679).

В тази връзка, следва да се има и предвид, че в съответствие с чл. 2 от Конвенцията на ООН за правата на детето дискриминацията е недопустима. Рискът от възникване на дискриминация се отчита и от Общ коментар № 10¹ (2007) към Конвенцията, озаглавен „Правата на децата при правосъдие спрямо ненавършили пълнолетие лица“, като се посочва, че много намиращи се в конфликт със закона деца са също така и жертви на дискриминация, например по отношение достъпа до образование или до пазара на труда. В този смисъл, националното ни законодателство въвежда изискване за закрила на личността на детето, по силата на което сведения и данни за дете **не се разгласяват** без съгласието на неговите родители или законни представители (арг. чл. 11а от Закона за закрила на детето). Балансираната защита на конкуриращите се права и интереси следва да се води от принципа за висшия интерес на детето, прогласен от чл. 24 от Хартата на основните права на Европейския съюз² (ХОПЕС), още повече, че в конкретния случай законодателят е преценил, че административните нарушения се характеризират с по-ниска степен на обществена опасност.

По повод публикуването в интернет съществува и друга заплаха. Обработване на лични данни, извършвано от лице „което управлява интернет търсачка, може да засегне в значителна степен основните права на зачитане на личния живот и на защита на личните данни, когато търсенето с помощта на тази търсачка се осъществява въз основа на името на физическо лице, при положение че посоченото обработване на данни позволява на всеки потребител на интернет да получи чрез списъка на резултатите структурирано изложение на информацията относно лицето, потенциално свързана с редица аспекти на личния му живот, която може да се намери в интернет и която без посочената търсачка не би могла или само трудно би могла да бъде обединена, и това да му позволи да изгради повече или по-малко подробен профил на съответното лице“³. Такова профилиране може

¹ Точки 7, 29, 64, 67 от Общ коментар № 10 (2007) към Конвенцията за правата на детето

² Чл. 24, пар. 2 от ХОПЕС: При всички действия, които се предприемат от публичните власти или частни институции по отношение на децата, висшият интерес на детето трябва да бъде от първостепенно значение.

³ Точка 80 от Решение на Съда (голям състав) от 13 май 2014 г. по дело C 131/12 Google Spain SL и Google Inc. срещу Agencia Española de Protección de Datos (AEPD) и Mario Costeja González по претъжбуване, отправено от Audiencia Nacional.

да доведе до нежелана оценка на личните аспекти във връзка с дадено физическо лице, анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите в образованието или работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията, когато то поражда правни последици по отношение на лицето или го засяга също толкова значително. Това засягане обаче не е могло да бъде преценено от законодателя към момента на въвеждането на наказанието в нормативната уредба, също както и неговите правни последици.

По тези съображения, в случаите, когато наказанието „обществено порицание“ не може да се изпълни по реда и условията на чл. 76 от ЗАНН, информация за него трябва да се обявява единствено на определените за това места (напр. информационни табла) в сградите на общините.

II. Свеждане на данните до минимум

Тъй като обявяването на информация за наложеното административно наказание „обществено порицание“, само по себе си, представлява операция по обработване на лични данни, приложение намират принципите, прогласени в чл. 5 от Регламент (ЕС) 2016/679. В конкретния случай, личните данни следва да се оповестяват за конкретни, изрично указани и легитимни цели (изпълнение на въпросното наказание) и не трябва да се обработват по-нататък по начин, несъвместим с тези цели. Личните данни, които се оповестяват при изпълнение на наложено наказанието „обществено порицание“, трябва да бъдат подходящи, свързани със и ограничени до строго необходимото за постигане целите на наказанието.

Законодателят е предвидил, че по отношение на непълнолетните административното наказание глоба се заменя с обществено порицание (чл. 15, ал. 2 ЗАНН). При обявяване на наказанието „обществено порицание“ обаче, винаги следва да се съблюдава обемът от данни, който се разкрива, така че да не се надхвърлят целите на самото наказание. Неограничаването на оповестените данни води до несъразмерност и значително по-тежки последици за наказаното лице, отколкото при налагане на глоба на пълнолетно лице – ефект, който не се цели от ЗАНН и в същото време противоречи на изискванията на Регламент (ЕС) 2016/679. Така например разкриването на информация, в пълнота, за постоянния/настоящия адрес на наказаното лице, може да създаде заплаха от саморазправа, проявяване на интерес от страна на педофили или други форми на противоправна дейност.

Ето защо данните, които се оповестяват във връзка с изпълнението на наказанието, трябва да се ограничат до строго необходимото, както следва:

- собствено, бащино и фамилно име на наказаното лице;
- общината/населеното място по постоянен/настоящ адрес на наказания, без да се обявява информация за точния му адрес;
- описание на извършеното нарушение, включително правната му квалификация;
- информация за административнонаказващия орган.

При изпълнение на наложено административно наказание „обществено порицание“ не трябва да се разкрива информация за ЕГН, дата и място на раждане, номер на документ за самоличност, точен адрес, лични данни на трети лица и други лични данни, които нямат връзка с целите на наказанието.

III. Ограничение на срока

Когато наложено административно наказание „обществено порицание“, обективизирано в наказателно постановление, се изпраща за изпълнение на общините/ местните комисии за борба срещу противообществените прояви на малолетните и непълнолетните (МКБППМН) към тях, последните, в качеството им на администратори на лични данни, трябва да го обявяват само на определени за това места (напр. информационни табла) в сградите на общините, за срок, който да позволява идентифицирането на наказаното лице, но не по-дълъг от необходимото за постигане на

целите на наказанието. Така например продължителният срок на публикуване може съществено да засегне възможностите на лицето да си намери подходяща работа, след настъпване на пълнолетие, както и да насочи претенциите си срещу администратора, засегнал правата му.

Доколкото нормата на чл. 76 от ЗАНН предвижда изпълнението на наказанието „обществено порицание“ да става чрез прочитане (т.е. еднократен във времето акт), когато се прибегва до изпълнение чрез общините, последните, в качеството им на администратори на лични данни, трябва да ограничат оповестяването за срок от 1 месец.

По тези съображения и на основание чл. 58, пар. 6 от Регламент (ЕС) 2016/679 във връзка с чл. 10а, ал. 2, т. 2 от Закона за защита на личните данни, КЗЛД дава следните

УКАЗАНИЯ:

1. Когато наложено административно наказание „обществено порицание“ се изпраща за изпълнение на общините/МКБППМН към общините, последните, в качеството им на администратори на лични данни, не трябва да го обявяват на своите интернет страници.

2. Информация за наложено административно наказание „обществено порицание“ трябва да се обявява единствено на определените за това места (напр. информационни табла) в сградите на общините. При обявяването ѝ по този начин общините могат да разкриват само личните данни, които са строго необходими и пропорционални за нуждите на изпълнение на наказанието, респ. за постигането на неговите цели, а именно:

- собствено, бащино и фамилно име на наказаното лице;
- общината/населеното място по постоянен/настоящ адрес на наказания, без да се обявява информация за точния му адрес;
- описание на извършеното нарушение, включително правната му квалификация;
- информация за административнонаказващия орган.

3. При изпълнение на наложено административно наказание „обществено порицание“ не трябва да се разкрива информация за ЕГН, дата и място на раждане, номер на документ за самоличност, точен адрес, лични данни на трети лица и други лични данни, които нямат връзка с целите на наказанието.

4. Обявлението трябва да е видно на мястото по т. 2 за срок от 1 месец, считано от датата на обявяването му, след което трябва да се премахне.

5. Общините трябва да извършат преглед на съдържанието на интернет страниците си и в случай че установят наличие на обявления за наложено наказание „обществено порицание“, да предприемат необходимите действия по премахването им в срок до 1 месец от издаването на настоящите указания.

6. При липса на предприети действия от общините в срока по т. 5, КЗЛД ще упражни корективните си правомощия по чл. 58, пар. 2 от Регламент (ЕС) 2016/679.

7. Указанията по т. 1 – 6 се прилагат за обработването на лични данни на непълнолетни лица при изпълнение на административното наказание „обществено порицание“.

ПРЕДСЕДАТЕЛЯТ НА КЗЛД ВЕНЦИСЛАВ КАРАДЖОВ Е КАНДИДАТ ЗА ПРЕДСЕДАТЕЛ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



На проведеното на 26 април 2023 г. заседание на Европейския комитет по защита на данните започна процедурата за избор на негов нов председател. Комитетът е ключов орган на ЕС по отношение на правната рамка за защита на данните, който подпомага гарантирането, че Общият регламент се прилага съгласувано в целия ЕС, и работи за осигуряване на ефективно сътрудничество между органите за защита на данните. В съответствие с Регламент (ЕС) 2016/679 Комитетът избира един председател и двама заместник-председатели измежду своите членове с обикновено мнозинство за мандат от 5 години, който може да бъде подновен само веднъж. Мандатът на настоящия председател на ЕКЗД изтича на 25 май т.г.

Председателят на Комисията за защита на личните данни – Венцислав Караджов представи кандидатурата си пред пленарния състав на Комитета. Към момента председателят на КЗЛД е заместник-председател на ЕКЗД, избран на 25 май 2018 г., на първото заседание на създадения с Регламент (ЕС) 2016/679 Европейски комитет за защита на личните данни.

Освен г-н Караджов, в надпреварата за избор на нов председател на ЕКЗД участват и ръководителите на финландския и нидерландския надзорни органи по защита на личните данни. Изборът на новия председател ще се проведе по време на пленарното заседание на ЕКЗД на 25 май 2023 г. Повече информация за процедурата и кандидатите може да намерите [ТУК](#).

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



На състоялото се на **28 март 2023 г.** заседание ЕКЗД прие окончателна версия на „**Насоки относно правата на субектите на данни - Право на достъп**“, след проведена обществена консултация. Насоките анализират различните аспекти на правото на достъп и предоставят по-точни насоки за това как правото на достъп трябва да се прилага в различни ситуации. Освен това, Насоките предоставят пояснения относно

обхвата на правото на достъп; информацията, която администраторът трябва да предостави на субекта на данните; формата на искането за достъп; основните условия за предоставяне на достъп и понятието за очевидно неоснователно или прекомерно искане.

На същото заседание ЕКЗД прие окончателни версии на целевите актуализации на „**Насоки за определяне на водещ надзорен орган на администратор или обработващ лични данни**“ и „**Насоки за уведомяване за нарушение на сигурността на данните**“. И двата документа се отнасят до актуализиране на насоки по същите теми на Работна група по чл. 29. Обществената консултация засегна само параграфите от насоките, които бяха актуализирани и в резултат на нейното провеждане

някои отзиви бяха включени в актуализираните Насоки относно уведомяването за нарушаване на сигурността на данните. По-специално, новата версия пояснява, че уведомяването е отговорност на администратора. Освен това някои заинтересовани страни изразиха загриженост относно оперативни въпроси, в случай че за нарушение на сигурността на личните данни трябва да бъдат уведомени няколко органа за защита на данните. ЕКЗД обръща внимание, че целевата актуализация просто привежда текста на насоките в съответствие с текста на ОРЗД, който не предвижда обслужване на едно гише за администратори, които не са установени в ЕИП. Комитетът взе предвид отзивите на заинтересованите страни и реши в близко бъдеще да публикува на своя уебсайт списък с данни за контакт в случай на уведомяване за нарушаване на сигурността на данните – съответните връзки и приети езици за всички органи по защита на данните в ЕИП. Това ще улесни администраторите при намирането на данните за контакт и изискванията на съответния надзорен орган.

ЕКЗД прие и текст на **писмо до Европейския парламент, Съвета на ЕС и Европейската комисия относно споделянето на данни за целите на борбата с изпирането на пари и финансирането на тероризма**. Това писмо подчертава значителните рискове за неприкосновеността на личния живот и защитата на данните, породени от някои изменения, въведени от Съвета, които биха позволили на частни субекти, при определени условия, да споделят лични данни помежду си за целите на борбата с изпирането на пари и финансирането на тероризма, във връзка с „подозрителни транзакции“ и събрани данни в хода на изпълнение на задълженията за комплексна проверка на клиент. ЕКЗД изразява сериозни опасения относно законосъобразността, необходимостта и пропорционалността на тези разпоредби, които биха могли да доведат до широкомащабно обработване на лични данни от страна на частни субекти. ЕКЗД счита, че измененията не уточняват по подходящ начин условията, при които подобна обработка е оправдана, и че не предоставят достатъчни гаранции, като се има предвид, че подобна обработка може да има значително въздействие върху лицата, като например включване в черен списък и изключване от финансови услуги. ЕКЗД препоръчва на съзакондателите да не включват тези разпоредби в окончателния текст на предложението си.

На заседанието, състояло се на **13 април 2023 г.**, ЕКЗД прие **решение със задължителен характер** за разрешаване на спор на основание чл. 65 от ОРЗД относно проект на решение на Ирландския надзорен орган относно законността на прехвърлянето на данни към Съединените щати от Meta Platforms Ireland Limited (Meta IE) за нейната услуга Facebook. Тъй като не е бил постигнат консенсус по възраженията, подадени от няколко засегнати надзорни органа, Комитетът е призован да уреди спора между органите в рамките на два месеца. Решенията със задължителен характер на Комитета играят ключова роля за гарантиране на правилното и последователно прилагане на Регламента от националните надзорни органи. Приетото на 13 април решение разглежда важни правни въпроси, произтичащи от проекторешението на ирландския орган в качеството му на водещ надзорен орган по отношение на Meta IE. В решението ЕКЗД урежда спора дали административна глоба и/или допълнително разпореждане за привеждане на обработването в съответствие с изискванията на ОРЗД трябва да бъдат включени в окончателното решение на ирландския надзорен орган. Най-късно един месец след като ЕКЗД е уведомил за решението си водещият надзорен орган и засегнатите надзорни органи, Ирландският надзорен орган, в качеството му на водещ, следва да приеме своето окончателно решение въз основа на решението на Комитета, като вземе предвид неговата правна оценка. Решението на ЕКЗД ще бъде публикувано на неговия уебсайт след като Ирландският надзорен орган уведоми администратора за своето окончателно решение.

На **17 април 2023 г.** Европейският комитет по защита на данните представи своя **годишен отчет за 2022 г.** Отчетът обобщава работата, извършена от ЕКЗД през последната година и включва резултатите от прегледа на насоките, извършен сред заинтересованите страни, както и първия тематичен сборник с подбрани примери на окончателни решения в резултат на прилагането на принципа за обслужване „едно гише“. По думите на председателя на ЕКЗД Андеа Йелинек *„Този доклад ясно демонстрира колко работа е свършена от ЕКЗД в рамките на една година по отношение на издаване на насоки, документи за съгласуваност, правни съвети и приемане на решения със задължителен характер. Ролята на ЕКЗД се промени значително от 2018 г. насам. Ние се превърнахме*

във влиятелен играч в цифровата икономика на Европейското икономическо пространство. Ние не само гарантираме, че законодателството за защита на данните се прилага съгласувано в ЕИП, но помагаме за оформянето на цифровото бъдеще на Европа“.

На 27 април 2023 г. ЕКЗД публикува **Ръководство за защита на данните от малкия бизнес**, чиято цел е да помогне на собствениците на малък и среден бизнес в усилията им да отговорят на изискванията за защита на личните данни. По достъпен и лесно разбираем начин се предоставя практическа информация на малките и средни предприятия (МСП) за Общия регламент относно защитата на данните. Според председателя на ЕКЗД Андреа Йелинек „В това ръководство МСП ще намерят различни инструменти и практически съвети, които да им помогнат да са в съответствие с ОРЗД. То включва конкретни примери, събрани по време на нашия 5-годишен опит с ОРЗД.“ Ръководството обхваща различни аспекти на Регламента, от основите на защитата на данните до правата на субектите на данни, нарушенията на сигурността на данните и др. То съдържа видеоклипове, инфографики, интерактивни блок-схеми и други практически материали, които да помогнат на МСП да приложат на практика защита на данните. Освен това Ръководството съдържа преглед на полезни материали, разработени за МСП от националните органи за защита на данните.

ЕВРОПЕЙСКИЯТ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ ЗАПОЧНА СВОЕТО ВТОРО КООРДИНИРАНО ПРАВОПРИЛАГАЩО ДЕЙСТВИЕ

На 15 март 2023 г. ЕКЗД излезе със съобщение за започване на своето **второ координирано действие по правоприлагане**. През цялата 2023 година 26 органа за защита на данните в Европейското икономическо пространство, включително Европейският надзорен орган по защита на данните, ще участват в инициативата, чиято цел е определянето и позицията на длъжностните лица по защита на данните. Като посредници между органите по защита на данните, физическите лица и организациите, длъжностните лица по защита на данните имат съществена роля и принос за спазването на правилата за защита на данните и насърчаването на ефективната защита на правата на субектите на данни.

За да се прецени дали те имат съответстваща на изисквана от чл. 37-39 от ОРЗД позицията в своите организации и ресурсите, необходими за изпълнение на техните задачи, участващите в координираното действие органи по защита на данните ще подхождат на национално ниво по няколко начина:

- на длъжностните лица по защита на данните ще бъдат изпратени въпросници за подпомагане на установяването на факти или въпросници за установяване дали е необходимо официално разследване;
- започване на официално разследване;
- проследяване на текущи официални разследвания.

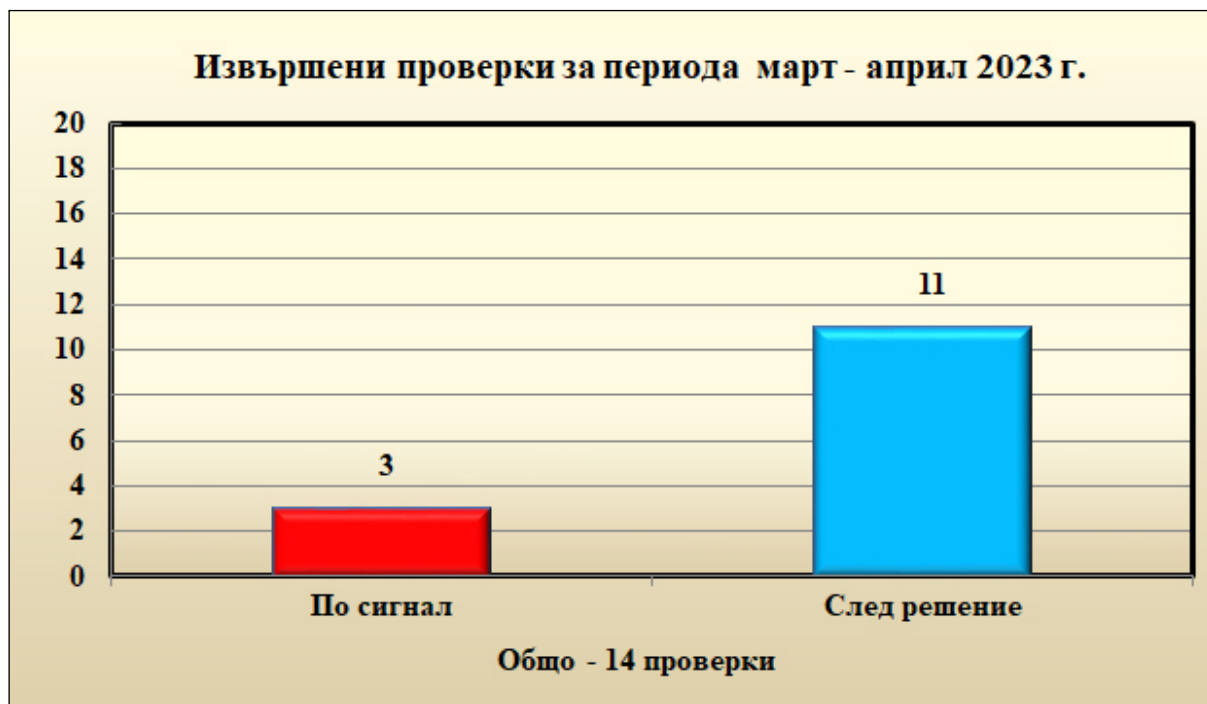
Резултатите от съвместната инициатива ще бъдат анализирани и органите по защита на данните ще вземат решение за евентуален по-нататъшен национален надзор и правоприлагащи действия. Освен това резултатите ще бъдат обобщени, генерирайки по-задълбочен поглед върху темата и позволявайки целенасочени последващи действия на ниво ЕС. ЕКЗД ще публикува доклад за резултата от този анализ, след като действията приключат.

Тази поредица от действия е втората инициатива по **Координираната рамка за прилагане (CEF)**, която има за цел да оптимизира правоприлагането и сътрудничеството между органите по защита на данните. През 2022 г. избраната тема беше **използването на облачни услуги от публичния сектор**. Доклад за резултатите от тази първа инициатива на CEF е публикуван на 18 януари 2023 г.

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАРТ - АПРИЛ 2023 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. за месеците март и април 2023 г. са извършени общо 14 проверки – 3 след постъпили в КЗЛД сигнали и 11 след решение на КЗЛД.



Разгледани са 65 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 **2 Разпореждания**, отправени са **2 Официални предупреждения** и са съставени **3 Акта за установяване на административно нарушение**.

РЕШЕНИЯ ПО ЖАЛБИ

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

РЕШЕНИЕ № ППН-01-169/2022 г. София, 16.03.2023 г.

Комисията за защита на личните данни в състав: Председател – Венцислав Караджов и членове – Цанко Цолов, Мария Матева, Веселин Целков, на редовно заседание, проведено на 12.10.2022 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни, чл. 57, § 1, б. „е” от Регламент 2016/679 и чл. 40, ал. 1 от Правилника за дейността на КЗЛД и на нейната администрация /ПДКЗЛДНА/ разгледа по основателност жалба № ППН-01-169/02.03.2022 г., подадена от В.И.

Административното производство се развива по реда на Административнопроцесуалния кодекс /АПК/ и чл. 38 от ЗЗЛД.

Комисията за защита на личните данни е сезирана с жалба № ППН-01-169/02.03.2022 г., подадена от В.И. срещу **телекомуникационен оператор (Т.О.)** за неправомерно обработване на лични данни, за да бъде създаден профил на жалбоподателя в „приложение на Т.О.“

В жалбата се посочва, че от електронно съобщение, постъпило на 17.02.2022 г. от емейл-1, е узнал, че документи, съдържащи негови лични данни /три имена, ЕГН, адрес, телефонен номер, имейл и саморъчен подпис/, са използвани за създаването на профил в „приложение на Т.О.“. Инициращият документ не е подписан от него, поради което в същия ден е поискал разяснение от мобилния оператор, като е върнал отговор на емейл-1 и емейл-2, в който уведомява администратора, че не той е подписвал заявлението и предявява искане профилът да бъде анулиран. Жалбоподателят изпраща повторно възражение до емейл-2 на 23.02.2022 г., като се свързва и с колцентъра на мобилния оператор, но казусът му не е бил разрешен.

В съответствие с чл. 26, ал. 1 от АПК страните са уведомени за образуваното административно производство, като са изискани представяне на становище и доказателства по случая.

В становището на Т.О. /писмо № ППН-01-169#5/22.06.2022 г./ се посочва, че жалбоподателят е абонат на мобилния оператор, като се представя договор за предоставяне на мобилни услуги № *****, ведно с приложение № 1 и № 2 от 02.04.2018 г. Дружеството разполага с алтернативна функционалност, в допълнение на конвенционалните опции за сключване на договор, която позволява извършване на поръчки посредством т. нар. “е-подпис на Т.О.”, представляващ поредица от действия – оторизация чрез мобилен телефон за връзка, поръчка чрез „приложение на Т.О.“, получаване на уникален идентификационен код за всяка отделна дейност. Въз основа на това към партидата на В.И. е добавена „бланка за съгласие“ относно описания механизъм за сключване на договор. Мобилният оператор не е отговорил на възражението на жалбоподателя, тъй като имейлът му е третиран като зловреден.

Администраторът посочва, че въз основа на резултатите от извършената вътрешна проверка е установено, че заявлението наистина не е подписано от В.И., предвид което са предприети мерки

същото да бъде премахнато от неговата партия, за което представят системен екран. Според процесуалния представител на Т.О. за жалбоподателя не са настъпили неблагоприятни последици, доколкото случаят не касае извършването на услуга, респективно В.И. не дължи възнаграждение.

В предоставения срок за изразяване на становище на основание чл. 34, ал. 3 от АПК жалбоподателят посочва /писма с вх. № ППН-01-169#3/07.06.2022 г. и № ППН-01-169#8/30.06.2022 г./, че не е получил отговор от Т.О., но е удовлетворен, че администраторът е признал грешката си и че функционалността е деактивирана.

На основание чл. 38, ал. 1 от ПДКЗЛДНА Комисията се е произнесла с Решение по редовността и допустимостта на жалбата на закрито заседание, проведено на 20.07.2022 г., а жалбата, като редовна и допустима, е взето решение да бъде разгледана по същество на 12.10.2022 г. В административното производство са конституирани страните В.И. – жалбоподател и Т.О. с ЕИК ***** – ответник. Страните са редовно уведомени за насроченото открито заседание за разглеждане на жалбата по същество.

В допълнителни становища на ответника /писма с вх. № ППН-01-169#13/17.08.2022 г. и № ППН-01-169#15/06.10.2022 г./ се посочва, че за твърдяното нарушение е узнато в хода на настоящото административно производство, като незабавно е извършена проверка и са предприети действия за преустановяване на нежеланите действия. Според администратора не е налице нарушаване сигурността на личните данни в Т.О. Разяснява се, че допълнителната функционалност се активира след идентификация на лицето във физическия магазин на Т.О. и подписване на документ за съгласие. В конкретния случай е установено, че подписът на бланката не е положен от жалбоподателя, тъй като служителят във физическия магазин не е спазил правилата за идентификация на физическото лице.

На проведеното открито заседание на КЗЛД, жалбоподателят не се явява и не се представлява. Ответникът, представляван от юрисконсулт Я.З., оспорва жалбата. Представя доказателства, както следва: Инструкция № 1 за идентификация на лицата в Т.О.; Инструкция № 10 – преглед на жалби за злоупотреба с лични данни; Инструкция за идентификация на физическо лице с приложение; работа с чувствителна информация на Т.О.; протокол за проверка за спазване на правилата за работа с лични данни и друга чувствителна информация. Изразява мнение, че от представените доказателства е видно, че дружеството е взело всички възможни мерки. Потвърждава изразената позиция, че въз основа на извършената проверка е установено, че В.И. не е полагал подпис върху заявлението, респективно не е предоставил съгласие по смисъла на Регламента за обработване на лични данни за целите на функционалността „приложение на Т.О.“. Същата представлява алтернативен метод, с който лицето би могло да встъпва във или да прекратява договорни отношения с дружеството.

На въпрос на Комисията как е създаден въпросният профил при положение, че субектът на данни физически не се е явил в търговски обект на Т.О., а според собствените изисквания на администратора физическото лице следва безспорно да бъде идентифицирано, юрисконсулт Я.З. посочва, че не може да каже по какъв начин това се е случило, но поради това, че събитието е от м. февруари т. г. не се съхраняват видеозаписите от магазина. На въпрос на Комисията какви действия е предприел администраторът, така че да не се случва инцидент със сигурността на личните данни от такова естество, юрисконсулт Я.З. посочва, че администраторът се старее да минимизира шанса от злоупотреби, но не е възможно това да се подsigури на 100%. На въпрос на Комисията какви възможности дава т. нар. “е-подпис на Т.О.” юрисконсулт Я.З. посочва, че това е алтернативен метод, с който биха могли да се сключват, изменят или прекратяват договори, като същият може да се активира само за съществуващи клиенти на Т.О. Посочва, че след като е установено нарушението на лични данни, са предприети допълнителни мерки.

На въпрос на Комисията дали при прекратяване или създаване на нов договор има някакви последващи действия за валидация юрисконсулт Я.З. посочва, че след подаване на заявка за сключване, промяна или прекратяване на договора, същият се визуализира като текст в приложението и абонатът може да изрази съгласието си чрез натискане на бутон /а не с полагане на саморъчен или електронен подпис/. Доколкото мобилният оператор е разписал процедура, че при сключване на нов договор и заявяване на нови услуги, както и при закупуване на устройства, се изпраща

текстово съобщение с разписани условия, то субектът на данни би следвало да бъде уведомен за евентуално договорно правоотношение или за липсата на такова. На въпрос на Комисията как лицето е разбрало, че въпросната функционалност е активирана и дали получава хартиено копие от съответната документация, процесуалният представител на ответника посочва, че по процедура следва да се получи копие от документа, но в настоящия случай субектът на данни не е получил такова. Юрисконсулт Я.З., поддържайки предходните становища на администратора, посочва, че в конкретния случай не става въпрос за предоставяне на някаква нова услуга, въз основа на която да се генерират приходи за администратора или да се създадат нови правоотношения между страните, а се касае за алтернативен начин за изразяване на волеизявления в рамките на съществуващото правоотношение между страните. Личните данни на жалбоподателя са обработвани във връзка с действащото правоотношение между страните – договор за ползване на мобилни услуги, който жалбоподателят изпълнява надлежно и страните нямат претенции помежду си във връзка с изпълнението. В конкретното заявление не фигурират лични данни, по-различни от тези, които са обработвани на договорно основание. По никакъв начин чрез този метод не се е стигнало до сключването на договор, до предоставянето на услуга или до закупуването на устройства, нито са се променяли параметрите на съществуващата услуга. Според Я.З. не са настъпили вреди, нито са осъществени злонамерени действия по повод създадения метод на подписване. При проверката се е оказало, че заявката за създаване на профил не е подписана от жалбоподателя, след което алтернативната функционалност е заличена от профила на абоната. Счита, че от предоставените правила и процедури е видно, че мобилният оператор е предприел множество мерки, с които се старае да сведе до минимум както възможността за злоупотреби, така и повторност на подобни хипотези. По тези причини апелира Комисията да възприеме тезата, че не е налице нарушение, а при условията на евентуалност – че същото не е съществено.

В отговор на уточняващ въпрос на председателя на Комисията в какъв срок В.И. е подал жалба до администратора и по-конкретно дали това е сторено в двумесечния срок за съхраняване на кадрите от видеонаблюдението в търговския обект, юрисконсулт Я.З. посочва, че при проверката се е установило, че възражението до администратора от 23.02.2022 г. срещу уведомлението от 17.02.2022 г. е попаднало в папка „нежелана поща“ и поради това не е било разглеждано, както и че според него администраторът не е бил сезиран с жалба. В отговор на уточняващ въпрос дали във вътрешните правила на администратора има изискване, ако се подаде жалба в срока на съхранение на видеокадрите, същите да бъдат запазени до приключване на разглеждания спор, юрисконсулт Я.З. посочва, че ако има жалба кадрите се запазват, стига към момента на подаването на жалбата и разглеждането ѝ този запис да бъде наличен, като практиката сочи, че жалбите се разглеждат ежемесечно.

Комисията обръща внимание на процесуалния представител на ответника, че защитната му теза, че личните данни на жалбоподателя са обработени на основание договора му с мобилния оператор, е невярна. В случая личните данни на В.И. не са обработени за целите, за които са събрани. Те са събрани на основание чл. 6, § 1, б. „б“ от Регламента, т.е. за целите на сключване на договор, като впоследствие са обработени за цел, различна от първоначалната – за създаването на допълнителна функционалност, чрез която могат да се правят алтернативни волеизявления от името на физическото лице, които биха могли да създадат съответните права и задължения за субекта на данни, дори и по независещи от него причини, както и без същият да е изразил съгласие по смисъла на Регламента. Юрисконсулт Я.З. посочва, че според него няма как да се стигне до сключване на договор, защото дори и да е активирана функционалността „приложение на Т.О.“, лицето трябва да влезе в профила си, като въведе паролата си. Когато се заяви подписване, промяна или прекратяване на такъв договор, се изпраща повторно SMS с код, който служи за верификация.

При така установеното от фактическа страна, от правна страна жалбата е допустима и основателна.

С Регламент 2016/679 и Закона за защита на личните данни се определят правилата за защита на физическите лица във връзка с обработването на личните им данни, както и правилата по отношение

на свободното движение на лични данни, така че да бъдат защитени основни права и свободи на физическите лица и по-конкретно правото им на защита на лични данни.

Предмет на жалбата е твърдение за неправомерно обработване на лични данни чрез употребата им за цел, различна от тази за която са били първоначално събрани, а именно – съставяне на заявка и активиране на онлайн функционалността „приложение на Т.О.“, респективно създаването на т.нар. “е-подпис на Т.О.“, който не е равносителен на електронен подпис по смисъла на Закона за електронния документ и електронните удостоверителни услуги, но активирането му би могло да доведе до правни последици за субекта на данни.

Отвратната страна Т.О. е юридическо лице – администратор на лични данни по смисъла на чл. 4, т. 7 от Регламента и е обработвал личните данни на жалбоподателя чрез съвкупност от операции като съхранение и употреба за цели, различни от тези, които може да обоснове като легитимни, което представлява нарушение на чл. 5, §1, б. „б“ от Регламента.

По отношение на твърденията на субекта на данни, че мобилният оператор не е върнал отговор на запитването му, следва да се отбележи, че жалбоподателят не е предявил искане за упражняване на права по смисъла на чл. 12 и сл. от Регламента, а е изпратил запитване в свободен текст, въз основа на което за администратора не е възникнало задължение за предоставяне на отговор. Комисията също не е сезирана с жалба за непредоставяне на отговор – в искането на субекта на данни е отбелязано, че същият не е получил отговор от администратора, но предмет на жалбата е неправомерно обработване на лични данни.

В случай че беше надлежно сезиран, администраторът не би могъл да се позовава на това, че имейлът на жалбоподателя е третиран като зловердна поща. Администраторът е длъжен да осигури надежден и сигурен канал за комуникация с клиентите си. От обстоятелство, че имейлът на В.И. евентуално е идентифициран като зловердна поща следва извод, че не са предприети подходящи организационни и технически мерки, доколкото имейлът е получен именно от електронния адрес, с който жалбоподателят е идентифициран от Т.О. Непо повече – администраторът е имал други данни за кореспонденция със субекта на данни като телефонен номер и физически адрес, поради което е имал възможност да се свърже с лицето и да извърши насрещна проверка на информацията, която твърди, че представлява зловердна поща, но не го е сторил.

Между страните не се спори, че между тях е налице договорно правоотношение и че на това основание мобилният оператор първоначално е обработвал личните данни на лицето. В хода на съществуващото договорно правоотношение администраторът е продължил да обработва личните данни на субекта, като съществено е изменил заложената в договора цел – данните му /три имена, ЕГН, адрес, електронен адрес, телефонен номер и подпис/ са достъпни от служител в магазин на Т.О., след което са разпространени и използвани за генерирането на „Заявление-декларация за електронна идентификация и подписване на договори с електронен подпис“. Между страните няма спор, че заявлението не е подписано от жалбоподателя, респективно, че същият не е предоставил съгласие¹ по смисъла на Регламента за използване на личните му данни за целите на допълнителната функционалност.

Администраторът на лични данни и ответник в настоящото производство се позовава на грешка, като признава, че субектът на данни не е бил надлежно идентифициран, както и че въпросната функционалност е била деактивирана на 15.06.2022 г. в хода на извършена вътрешна проверка след подаване на жалбата /така напр. Приложение № 2 към становище на Т.О. с вх. № ППН-01-169#5/22.06.2022 г./ Доколкото между страните няма спор, че жалбоподателят не е

¹ „Съгласие“ по смисъла на съображение 32 от Регламента означава „свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни ... мълчанието, предварително отметнатите полета или липсата на действие не следва да представляват съгласие. Съгласието следва да обхваща всички дейности по обработване, извършени за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие. Ако съгласието на субекта на данни трябва да се даде след искане по електронен път, искането трябва да е ясно, сбито и да не нарушава излишно използването на услугата, за която се предвижда.“

подписал процесното заявление, както и поради това, че не са налице доказателства в обратната посока, следва извод, че личните му данни са използвани неправомерно за целите на създаване на допълнителната функционалност "е-подпис на Т.О.". Същата, независимо, че не е равносилна на електронен подпис по смисъла на ЗЕДЕП, представлява механизъм за изразяване на волеизявления, въз основа на който администраторът на лични данни счита, че биха могли да възникнат, да се изменят или да се прекратят договорни правоотношения със субекта на данни. Въпросът дали този алтернативен метод на изразяване на волеизявления, верифицирането на които не се извършва нито чрез полагане на саморъчен подпис, нито чрез употреба на електронен подпис, е годен да породи гражданскоправни последици, не е предмет на произнасяне на Комисията.

Предвид гореизложеното, действията на администратора по обработване на лични данни са извършени в нарушение на принципа за „ограничение на целите“, регламентиран в чл. 5, параграф 1, буква „б“ от Регламент 2016/679.

Администраторът е извършил проверка по случая и е установил, че не жалбоподателят е положил подпис върху заявлението и не той е предявил искане за активиране на онлайн функционалността на Т.О., като това е станало поради неспазване правилата за идентификация на субекта на данни във физическия магазин на мобилния оператор /така напр. Инструкция за идентифициране на клиенти в магазин на Т.О./. Същото представлява нарушение на принципа на чл. 5, §1, б. „е“ от Регламента, поради това, че личните данни са обработени по начин, който не гарантира подходящо ниво на сигурност, включително защита срещу неразрешено обработване, което е сторено от служителя в магазина на администратора, а не от субекта на данни.

Личните данни, предмет на неправомерно обработване /три имена, ЕГН, адрес, електронен адрес, телефонен номер, подпис/, са такива, с които администраторът разполага на друго основание – това по чл. 6, §1, б. „б“ от Регламента. В случая не се обработват специални категории лични данни по смисъла на чл. 9 от Регламента.

В хода на административното производство и в проведеното открито заседание за разглеждане на жалбата по същество се установи, че администраторът е нарушил собствените си правила за идентификация на физическите лица. Администраторът е узнал от възражението на субекта на данни още в същия ден, че В.И. не е подписвал декларацията, с която се иска активиране на допълнителната функционалност "е-подпис на Т.О.", но не е предприел действия. Видно е, че възражението на субекта на данни и искането за анулиране на създадената функционалност е постъпило до официалните имейли за кореспонденция с Т.О. още в същия ден /17.02.2022 г./. Администраторът не би могъл да се позовава на евентуални съмнения относно самоличността на лицето, от което изхожда искането, доколкото същият този администратор е могъл да извърши безспорна идентификация на субекта на данни преди да откаже да разгледа искането му. Доколкото към онзи момент не е бил изтекъл срокът за съхранение на записите от видеонаблюдението, администраторът е следвало, след като се увери в самоличността на субекта на данни, да предприеме съответните мерки по извършване на проверка по жалбата.

Видно от представените в откритото заседание доказателства администраторът разполага с вътрешни правила и процедури за защита на личните данни, но от предприетите действия по случая става ясно, че не е осъществен системен контрол. Извършената проверка е могла да се реализира на много по-ранен етап, в който администраторът е разполагал с възможността на провери видеокамерите в търговския обект, така че да може да удостовери, че В.И. не е бил вътре, респективно – че не е подписал заявката за активиране на допълнителната функционалност.

Независимо, че жалбоподателят незабавно е уведомил администратора за нежеланието си личните му данни да бъдат използвани за целите на алтернативния метод за комуникация с мобилния оператор чрез „приложението на Т.О.“, последният не е предприел необходимите действия за преустановяване на нарушението. Нарушението се дължи освен на липсата на съответните организационни и технически мерки, също така и на неосказването на достатъчен контрол върху дейността на служителите в магазина на Т.О., което не е позволило на администратора да обработи своевременно информацията и да извърши необходимите действия в разумен срок.

Несвоевременната проверка, която администраторът е извършил, всъщност е довела до неефективност на предприетите мерки. Същите не водят до превенция, каквито са изискванията на Регламента, поради което Комисията счита, че за да има превантивен и възпиращ ефект наложената мярка, следва на администратора да бъде наложена имуществена санкция. На същия администратор многократно са налагани корективни мерки, които да подобрят организационните и техническите условия при него. В настоящия случай е установено, че въведените правила не се спазват от служителите, което води до извод за извършено нарушение по чл. 5, §1, б. „е“ и чл. 24, §1 и §2 от Регламента, именно защото въвеждането на организационни и технически мерки включва и контролът по тяхното изпълнение.

Администраторът признава грешката си, като освен това става ясно, че мерките за безспорна идентификация на физическите лица, въведени от администратора, са се оказали неподходящи. Дори и да беше вярно обратното, по тяхното спазване не е упражнен необходимият контрол.

В отношенията между мобилния оператор и субекта на данни действията, извършени във функционалността „приложение на Т.О.“, имат силата на електронна идентификация и от тях биха могли да възникнат неблагоприятни правни последици за субекта на данни. Самият администратор не извършва последваща идентификация и верификация на евентуално извършените действия / натискането на бутон след „преглед“ на договора не представлява действие по идентификация на субекта на данни/. Независимо от това, следва да се отбележи, че не са възникнали неблагоприятни последици за субекта на данни, но не защото администраторът е предприел подходящи мерки, позволяващи безспорна идентификация на субекта на данни, а поради това, че В.И. не е встъпил в договорни правоотношения с администратора.

Комисията разполага с правомощия по целесъобразност, въз основа на които преценява кое от корективните правомощия по чл. 58, § 2 от Регламент 2016/679 да упражни. Нарушението, изразяващо се в обработване на лични данни за цели, несъвместими с първоначално създадените – неспазване на принципа на чл. 5 § 1, б. „б“ от Регламента, е преустановено с деактивирането на създадената функционалност “е-подпис на Т.О.” на 15.06.2022 г., поради което не биха могли да намерят приложение корективните правомощия на Комисията с предупредителен или преустановителен характер, а би следвало да се наложи административно наказание имуществена санкция по чл. 58, § 2, б. „и“ от Регламента.

При налагането на имуществена санкция надзорният орган е ограничен от съответните лимити по чл. 83, § 5, б. „а“, вр. с чл. 5, § 1, б. „б“ и б. „е“ от Регламента. В настоящия случай ефективна, пропорционална и възпираща мярка би била имуществена санкция в размер, близък до минималния – администраторът е поправил грешката си, субектът на данни не е претърпял вреди, а нарушението е преустановено в сравнително кратки срокове. Нарушението представлява обработване на лични данни на един субект на данни чрез съхранение и употреба за цели, различни от тези, за които личните данни са били първоначално събрани от администратора, като същото е продължило през относително кратък период от време /по малко от 4 месеца или от 17.02.2022 г. до 15.06.2022 г./ Личните данни на физическото лице не са се разпространили до лица, извън служителите на администратора. Независимо, че нарушението не е съпроводено с вреди за субекта на данни, това се дължи не на предприетите мерки от администратора, а на случайно събитие. От нарушението са могли да възникнат имуществени вреди за физическото лице. Чрез разкриването на профил в приложението биха могли да възникнат частноправни последици и не е вярно твърдението, че единствено съответният абонат може да ползва функционалността, доколкото Т.О. не извършва последваща идентификация на физическото лице, освен че в разглеждания случай не е извършил и предварителна такава.

Смекчаващо отговорността обстоятелство е, че администраторът е преустановил нарушението по собствена инициатива в хода на настоящото административно производство. Отегчаващо обстоятелство е, че администраторът не е предприел действия по възражението на субекта на данни, доколкото същият няма разписани ефективни механизми за последващ контрол или поне не е доказал наличието и спазването на такива.

Степента на отговорност на администратора следва да се категоризира като относителна висока, имайки предвид, че въведените от същия технически и организационни мерки, както и оказания контрол върху тях не са достатъчни, за да бъде избегнато или преустановено нарушението, предвид това, че поради липсата на подходящи организационни и технически мерки, и неупражняването на достатъчен контрол личните данни на лицето са били достъпни от служител в магазин на Т.О., същият ги е обработил за цели, несъвместими със законосъобразното обработване на лични данни и това е останало без съответните последствия.

Администраторът не е предприел необходимите мерки за преустановяване на нарушението след като още в същия ден и впоследствие на 23.02.2022 г. субектът на данни е представил обратна комуникация на Т.О. /независимо, че същата не представлява искане за упражнява на права по Регламента/, че никога не подписвал документите, както и че не му е известно как личните му данни са попаднали в искането за използване на “е-подпис на Т.О.“. Нарушението не е преустановено, което говори, че администраторът няма подходящо разписани вътрешни механизми за превенция и за контрол по отстраняване на нарушения на сигурността на данните. Администраторът е осигурил съдействие на надзорния орган, за да бъде отстранено нарушението, като все пак е смекчил евентуалните неблагоприятни последици от него по отношение на субекта на данни, деактивирайки функционалността. В настоящата хипотеза администраторът не е реализирал преки или косвени финансови ползи, нито е избегнал загуби вследствие на нарушението /това не е станало поради предприетите мерки от администратора, а поради това, че функционалността не е била ползвана от физическото лице/.

Администраторът на лични данни Т.О. има предишни нарушения, свързани със сигурността на личните данни, нееднократно действията му са били обект на санкция от Комисията, която в редица свои решения е разяснявала приложението и смисъла на Регламента за защита на личните данни /така напр. в Решение № ППН-01-130/2019 г. администраторът е санкциониран за несъобразяване с условията за предоставяне на съгласие от субекта на данни, а в Решение № ППН-01-313/2019 г. на администратора е наложена санкция за неспазване на подходящи организационни и технически мерки/.

Предвид гореизложеното и на основание чл. 38, ал. 3 от ЗЗЛД Комисията за защита на личните данни

РЕШИ:

1. Обявява Жалба № ППН-01-169/02.03.2022 г. на В.И. срещу Т.О. с ЕИК **** за основателна за нарушение на чл. 24, §1 и §2, вр. с чл. 5, § 1, б. „б“ и б. „е“ от Регламент (ЕС) 2016/679.

2. На основание чл. 58, § 2, б. „и“ и чл. 83, § 5, б. „а“ от Регламент (ЕС) 2016/679 за нарушение на чл. 5, § 1, б. „б“ и б. „е“ от Регламента налага на администратора телекомуникационен оператор с ЕИК ***** административно наказание имуществена санкция в размер на 2000 /две хиляди/ лв.

Имуществената санкцията следва да бъде изплатена в 14-дневен срок, считано от влизане в сила на настоящото Решение по следната банкова сметка на КЗЛД в БНБ:

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Титуляр: Комисия за защита на личните данни, БУЛСТАТ 130961721,

в противен случай ще бъдат предприети мерки по принудително изпълнение.

Настоящото решение може да бъде обжалвано в 14-дневен срок от връчването му чрез Комисията за защита на личните данни пред Административен съд София – град.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № ПНМД-01-20/2023 г. гр. София, 16.03.2023 г.

ОТНОСНО: *Искане за изразяване на становище по въпроси, свързани със създаването и поддържането на регистър на лицата по чл. 10в, ал. 3 от Закона за хазарта (ЗХ), осигуряване на достъп до данните в регистъра на служители, определени от организаторите на хазартните игри (ОХИ), както и предприетите от НАП организационни и технически мерки за защита на данните, съдържащи се в регистъра*

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 15.03.2023 г., разгледа писмо с вх. № ПНМД-01-20/10.03.2023 г. от изпълнителния директор на Националната агенция за приходите. В писмото се посочва, че по силата на законови промени в ЗХ (изм. и доп. ДВ. бр. 69 от 4 Август 2020 г.), на Националната агенция за приходите (Агенцията, НАП) е възложено да създаде и поддържа Регистър на лица, които смятат, че имат проблем с хазарта и/или чието социално положение и/или равнище на доходи може да ги направи по-податливи към участие в хазартни игри и развиване на хазартна зависимост. Целта е да се намалят или избегнат потенциални негативни икономически, социални и личностни последици за уязвими лица и техните близки. Регистърът е предвидено да съдържа имена по документ за самоличност, единен граждански номер (ЕГН) или личен номер на чужденец (ЛНЧ), дата на вписване и период на вписване, ако такъв е посочен, като по силата на чл. 10г, ал. 4 от ЗХ същият не може да бъде по-кратък от две години. Вписването се извършва въз основа на писмено искане по образец, подадено от лицето или негов представител до изпълнителния директор на НАП. В чл. 10г, ал. 5 от ЗХ е регламентиран редът и начинът на заличаване от регистъра.

Малко след влизане в сила на посочените по-горе изменения и допълнения на ЗХ, влезе в сила нова нормативна промяна в ЗХ, внесена с § 91, ал. 2 от Преходните и Заключителни разпоредби към Закона за изменение и допълнение на Закона за данък върху добавената стойност (ЗИД на ЗДДС), обн., ДВ бр. 104 от 08.12.2020 г., в сила от 01.01.2021 г., въвеждаща мораториум за прилагане на изискванията на чл. 10г и чл. 10д от ЗХ за период от 24 месеца, считано от влизане в сила на закона. С въведената нормативна промяна се отлага прилагането на изискванията на чл. 10г и чл. 10д от ЗХ за периода от 12.12.2020 г. до 12.12.2022 г. включително.

В искането се посочва, че регистърът съдържа лични данни от категорията на имена по документ за самоличност и идентификатор на лицата. С оглед на контекста, в който данните ще бъдат обработвани, въз основа на същите могат да бъдат направени индиректно предположения за актуално или бъдещо здравословно състояние на субектите. Към момента липсва легална дефиниция на понятията „уязвимост“ и „хазартна зависимост“. Съгласно публикувана информация на официалната интернет страница на Министерство на здравеопазването, посочените понятия са свързани с поведенческа зависимост, определени патологични разстройства, зад които нерядко се крият психологически причини, като например „скрита депресия“. В този контекст, разглежданите категории данни могат да бъдат индиректно съотнесени към специалните категории лични данни по смисъла на чл. 9, пар. 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 Април 2016 г. относно защита 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 защита на данните (ОРЗД) и по-конкретно – въз основа на обработването на лични данни на вписаните в регистъра лица, съобразно конкретния контекст, могат да бъдат направени предположения за актуалното или бъдещото здравословно състояние на субектите на данните и специфични личностни особености, включително е възможно при недобросъвестно обработване на данните да бъдат оценени определени лични аспекти на субектите, свързани с икономическото им състояние, лични предпочитания, интереси, надеждност, поведение, включително да бъде нарушено правото на неприкосновеност на личния живот и достойнство на лицата, да настъпят сериозни неимуществени вреди за същите като например: дискриминация, изолация на субектите от определени социални общности, накарняване на тяхната репутация и др. В тази връзка НАП, в качеството си на първичен администратор на данните в регистъра, предприема редица действия по планиране и въвеждане на организационни и технически мерки за защита на посочените данни, част от които са, както следва:

1. Преди започване на дейностите по обработване е извършена Оценка на въздействието върху защитата на данните (ОВЗД), която се актуализира периодично, и в чиито рамки са идентифицирани възможни рискове за субектите на данни и планирани/предприети мерки за тяхното минимизиране, като не е отчетен висок остатъчен риск за лицата;

2. Прозрачност и информираност на субектите на данни и ОХИ – Агенцията периодично публикува актуална информация на официалната си интернет страница, съдържаща разбираеми разяснения относно функционирането на регистъра, реда и начина за вписване на лицата в същия, правата на субектите на лични данни, реда и начина за подаване на жалби и сигнали пред администратора НАП или Комисията за защита на личните данни при съмнения за нарушения при обработването на лични данни, задължения и отговорности на ОХИ, реда и начина за достъпване на данните и др. От НАП отбелязват, че с оглед постигане на пълна информираност на ОХИ за въведените мерки за защита на данните в регистъра, реда и начина за достъпване на данните и др., с представители на съответния бранш са организирани и проведени няколко срещи с разяснителен характер. В допълнение, проведена е и широка информационна кампания чрез средствата за масово осведомяване посредством специално разработени за целта разяснителни клипове;

3. Процесът по събиране на данни за лицата посредством подадени от тях или техни представители искания до НАП за вписването им в регистъра, по-нататъшното записване, структуриране и съхранение на данните в регистъра от страна на НАП, е обособено като самостоятелна дейност по обработване на лични данни, като същата е вписана по надлежния ред в Регистъра на дейностите по обработване, за които НАП отговаря, съгласно чл. 30, т. 1 от ОРЗД;

4. Планирани и предприети са мерки по недопускане вписването на лица, които не са изразили волята си за това, тъй като подобно обработване на данни би могло да се категоризира, като незаконосъобразно и съществува риск от ограничаване на права на конкретните физически лица (недопускането им до участие в хазартни игри), риск от уронване на престижа и доброто им име, др.;

5. Със заповед на изпълнителния директор на НАП е утвърден образец на искане за вписване и образец на искане за заличаване от регистъра, включително е определен ограничен кръг от длъжностни лица от НАП с право на достъп до данните в регистъра;

6. Предприети са подходящи организационни и технически мерки за защита на данните в процеса на тяхното съхранение на хартиен носител (входирани искания за вписване или заличаване от регистъра) и в електронната база данни на Агенцията, които детайлно са описани в извършената ОВЗД и в изготвените и утвърдени Технически изисквания за разработване на електронна услуга за достъп до регистъра по чл. 10 г, ал. 1 от ЗХ;

7. Обсъден е въпросът за определяне на срокове за съхранение на данните в регистъра, в т.ч. след изтичане на срока за вписване на лицата или след подадени искания за заличаване от регистъра, когато е изтекъл нормативно определеният минимум за вписване в регистъра от 2 години;

8. Други.

По-нататък в писмото на НАП се посочва, че с оглед постигане на баланс между спазване на законовото задължение, което се прилага спрямо НАП да уведомява организаторите на хазартни игри за лицата, вписаните в регистъра, съгласно чл. 10д, ал. 1 от ЗХ, от една страна, недопускане реализирането на имуществени или неимуществени вреди на лицата, както и с оглед изпълнение на нормативното изискване в чл. 10д, ал. 2 от ЗХ достъп до данните в регистъра да имат само определени от ОХИ техни служители от друга страна, НАП е реализирала възможност за извършване на справка от ОХИ относно наличието на вписано в регистъра лице под формата на електронна услуга, достъпна с КЕП в Портала за електронни услуги на НАП (U2S-интерфейс потребител-система) и/или приложен програмен интерфейс във вид на уеб-сървис (S2S-интерфейс система-система). Достъпът до услугата е ограничен до всички юридически лица с издаден активен лиценз за организиране на хазартни игри и упълномощените от тях служители. За целите на предоставяне на достъп до услугата се правят автоматизирани проверки дали юридическото лице – ОХИ е със статус „регистриран“, има поне един запис със статус „активен“ за лиценз по ЗХ и дали упълномощеното лице е с активно заявление за достъп до тази услуга. Проверката се изпълнява при всяко достъпване на услугата и в случай, че ОХИ вече няма активен лиценз или не е със статус „регистриран“ или няма активно заявление за достъп до електронните услуги на НАП, тогава достъпът до услугата не се разрешава. По отношение на уеб-сървисът, наред с някои от посочените по-горе изисквания за електронната услуга, се извършва и проверка дали използваният токен (софтуерен ключ) за достъп е активен, като е дефиниран процес по заявяване, издаване и предоставяне на упълномощени представители на ОХИ на токен, на място в ЦУ на НАП с подписване на приемо-предавателен протокол.

От НАП уточняват, че при извършваната проверка на въведения идентификатор, в случай, че същият е вписан в регистъра (пълно съвпадение на идентификатор), се визуализира съобщение, че лице с идентификатор 11111**** и имена Х. Y. Z (Х – инициал на собствено име, Y – инициал на презиме, Z – инициал на фамилия) към дата (системната дата) е вписано в Регистъра по чл. 10г от ЗХ. Визуализирането на данни за инициал на собствено, бащино и фамилно име на вписаното в регистъра лице ще предостави възможност на организаторите за самоконтрол относно достоверността на въведения идентификатор (че справката е коректно извършена по отношение на конкретно лице, заявило участие в хазартни игри), но същевременно минимизира риска за проверявания субект в случай на нарушение на сигурността на личните му данни. В случаите, в които за проверяваното лице посредством въведен негов идентификатор няма данни същото да е вписано в регистъра, пред оторизирания потребител на справката се визуализира единствено частично замаскиран идентификатор, но не и инициали на имената по документ за самоличност.

В искането се допълва, че в Техническите изисквания детайлно са разгледани въпроси, свързани с опазването на информацията и осигуряване на мрежова и информационна сигурност.

Във връзка с въведените от НАП организационни и технически мерки за защита на данните в регистъра, в Агенцията постъпват запитвания и предложения от ОХИ, които предполагат различно тълкуване на чл. 10д, ал. 1 от ЗХ. Според част от изразените мнения, задължението за НАП да „уведомява организаторите на хазартни игри за лицата, включени в регистъра по чл. 10г, ал. 1“ следва да се тълкува като осигуряване на своевременен достъп до пълния списък с вписани в регистъра лица. Пред НАП е повдигнат въпросът относно възможността Агенцията да изпраща по електронен път данни за вписаните лица на електронните адреси на предварително определени от ОХИ служители. Позицията на НАП е, че по този начин ще бъдат нарушени принципите, прокламирани в чл. 5, т. 1 от ОРЗД и преди всичко принципа на „свеждане на данните до минимум“, тъй като по този начин всеки един ОХИ ще обработва данни на вписани в регистъра субекти, част от които потенциално няма да са заявили участие в хазартни игри, респективно няма да е налице възникнала конкретна цел, за която данните да бъдат обработвани. В случая, целите на обработване следва да се отъждествяват с конкретно заявено участие до хазартна игра от конкретно физическо лице. Като аргумент за целесъобразността от изпращане на пълния списък с вписани в регистъра лица, който да е наличен при определения от ОХИ служители, е изтъкната хипотезата за възможни евентуални възникнали технически проблеми,

водещи до възпрепятстване на комуникацията между системите на ОХИ и внедрените услуги от НАП за проверка на лицата в регистъра. От НАП считат, че посоченият аргумент е неоснователен с оглед на факта, че данните за вписаните в регистъра лица не са константна величина и се променят ежедневно. Агенцията е на мнение, че подобен подход би възпрепятствал администрацията да осигури своевременно актуализиране на данните, ще изиска непропорционално разходване на времеви и човешки ресурс, а така също няма да е възможно да се осигури от страна на ОХИ своевременно изтриване на данни или тяхното коригиране при установена неточност.

На 16.01.2023 г. в ЦУ на НАП постъпва по електронен път писмо (Приложение №1) от „Сдружение на организаторите на хазартни игри и дейности в България“ (СОХИДБ), ЕИК 206074080, с което са изложени допълнителни аргументи, целящи да бъдат омаловажени предприетите от НАП организационни и технически мерки за достъп до данните в регистъра и тяхната защита, като са предложени алтернативни начини за предаване на данните от регистъра. Предложението на СОХИДБ е свързано с използването на техническо решение от типа „хеш функция“ - на Агенцията е предложено при предоставяне на информацията към ОХИ да преобразува личните данни на лицата включени в Регистъра в изходен низ, т.е. да ги хешира и в този преобразуван вид, да ги предоставя за проверка на организаторите на хазартни игри. В допълнение е посочено, че функцията е еднопосочна, като не позволява възстановяване на изходните данни от хеш стойностите, т.е. организаторите на хазартни игри няма да имат практическа възможност да извлекат личните данни на лицето от предоставената им хеш стойност. ОХИ ще имат задължението да използват идентично техническо решение (софтуер) изпълняващо хеш функция, което при въвеждане на личните данни на потенциалния клиент да получават хеш стойност. В случай, че получената хеш стойност е идентична с хеш стойността, която е предоставена от НАП, то това означава, че лицето е включено в Регистъра и същото няма да бъде допуснато до организираната игра. И обратното, липсата на съвпадение означава, че лицето не е включено в Регистъра и може да бъде допуснато до игра.

Във връзка с отправеното предложение за хеширане на данните от регистъра НАП подчертава, че подобен технически подход единствено би защитил данните при тяхното предаване от НАП на ОХИ, но би бил отново в разрез с принципите, прокламирани в чл. 5, т. 1 от ОРЗД. В допълнение от НАП излагат мотиви, че при хеширането на ЕГН-тата в регистъра, създаден и поддържан от НАП, във връзка с неговото изпращане към всички ОХИ, съществува хипотеза, при която ОХИ биха били в състояние да хешират всички ЕГН-та, съдържащи се в алтернативни бази данни (на всяко ЕГН ще съответства точно определен хеш) и да проверяват всички лица от тях, относно това дали са вписани в регистъра, независимо дали проверяваните към даден момент лица са заявили конкретното си желание за участие в хазартна игра или не, респективно могат да бъдат проверявани и субекти, които не са клиенти на съответния ОХИ към определен момент.

В изпратеното на 16.01.2023 г. писмо до НАП, СОХИДБ допълнително посочват, че при извършване на справки в регистъра на уязвимите лица посредством електронната услуга или S2S-интерфейса „система-система“, от страна на ОХИ, ще е налице процес по обработване на голям брой идентификатори на заявили участие в хазартни игри физически лица. Тъй като за извършване на съответните справки е необходимо идентификаторите да бъдат въведени във формата за търсене на съответната услуга, то по този начин, според изложеното становище от ОХИ, това би довело до незаконосъобразно обработване на голям брой идентификатори на физически лица, тъй като „ноторно известно е, че по-голямата част от посетителите на игралните зали и казината не са включени в регистъра на уязвимите лица“. ОХИ допълват, че „така чувствителни лични данни (за това, че посещават игрални зали и казина) за неограничен кръг лица биха били споделени с администрацията и евентуални пропуски в сигурността биха довели до това да стане достояние на обществеността обстоятелството, че дадено лице посещава игрални зали и казина“.

От Агенцията смятат, че изложените аргументи от страна на ОХИ са неоснователни, тъй като на първо място, задължението на ОХИ да идентифицират своите клиенти, в това число да администрат база данни за имена и идентификаторите на лицата, е тяхно законово задължение. Следва да се има

предвид, че съгласно чл. 74, ал. 1 от ЗХ всички посетители в игралното казино се вписват в специален регистър по образец, утвърден от изпълнителния директор на НАП. Регистърът се води на хартиен и електронен носител. Наред със задълженията на ОХИ в качеството им на субекти по смисъла на Закона за мерките срещу изпирането на пари и Закона за мерките срещу финансирането на тероризма, са в пряка връзка със законово вменените контролни правомощия на Агенцията, респективно да осъществява мониторинг върху ОХИ относно спазване от тяхна страна на законовото задължение за проверка на лица, заявили желание за участие в организирани хазартни игри, относно фигурирането им в регистъра. С други думи, алтернативните и предложени от ОХИ начини за предоставяне на данни от регистъра или осигуряване на достъп до същия не биха осигурили възможност за контролния орган НАП да удостовери в пълнота дали в действителност се извършват проверки на лицата. НАП допълва, че посочената категория данни не представлява „чувствителни лични данни“, както СОХИДБ сочат в своето писмо, още повече не представлява и защитена от закона информация извън рамката на законодателството за защита на личните данни. Агенцията е на мнение, че подобно обработване на лични данни от нейна страна би било напълно законосъобразно при условията, регламентирани в чл. 6, пар. 1, б. „д“ от ОРЗД, а именно – при осъществяване на официални правомощия, които са предоставени на Агенцията. На следващо място следва изрично да се подчертае, че в качеството си на първичен администратор на личните данни на физическите лица, които са заявили желанието си да бъдат вписани в регистъра по чл. 10 г, ал. 1 от ЗХ, НАП следва самостоятелно да определи критериите за достъп до данните в регистъра при съблюдаване на действащото законодателство в областта на защитата на личните данни. Именно в този контекст са и мотивите към предложението за изменение и допълнение на ЗИД на ЗДДС, с което се налага мораториумът, вх. №054-04-249/13.11.2020 г. по описа на Народното събрание на Република България (Приложение № 2), а именно: *„От една страна НАП следва да създаде този регистър и да предостави достъп до него на Организаторите, като обаче определи реда и начина за това, при това като едновременно се осигури неговата цялост и сигурност (...) осигурява се опазване на личните данни на субектите в него при съблюдаване на законодателството в областта. Следва да бъде предвиден и ред за установяване спазването на това изискване от Организаторите, защото не бива да се разчита нито само на тяхното добросъвестно поведение, нито на това на участниците (...). Създаването от Организаторите на системи за идентификация на лица, които са включени в регистъра, особено при участието им в хазартна игра, предлагана по наземен път, изисква допълнителна инвестиция в подходящ за целта Софтуер, което следва да се предвиди, осигури и реализира от икономическите оператори“* (вж. стр. 27-29 от Приложение №2). От изложените мотиви е видно, че именно НАП е правоимащата страна да определи реда и начина за достъп до регистъра, същият се достъпва, а не администрира от ОХИ, не се разкрива в неговата цялост и се администрира именно от страна на Агенцията, като достъп до данните в него би следвало да се осигури на определените от изпълнителния директор на НАП длъжностни лица и на служителите, определени от ОХИ по повод на възникнала конкретна цел, като разкритите данни задължително да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които същите ще се обработват.

Във връзка с гореизложеното, от НАП молят КЗЛД да изрази становище по отношение на следния въпрос:

Отчитайки изискванията на чл. 10д, ал. 1 и ал. 2 от ЗХ, както и принципите за обработване на лични данни, прогласени с чл. 5 от ОРЗД, допустимо ли е НАП да предоставя на ОХИ предварителен, пълен и неограничен достъп до данните в целия регистър или НАП следва да осигури единствено възможност за проверка на конкретно физическо лице, заявило желание за конкретно участие в хазартни игри при конкретен ОХИ?

ПРИЛОЖЕНИЕ:

1. Писмо от „Сдружение на организаторите на хазартни игри и дейности в България“ (СОХИДБ) – електронен формат, съдържа 4 стр.

2. Мотиви към предложението за изменение и допълнение на ЗИД на ЗДДС, вх. №054-04-249/13.11.2020 г. по описа на Народното събрание на Република България – ксерокопие, съдържа 30 стр.

Правен анализ:

По силата на чл. 10 г, ал. 1 от ЗХ Националната агенция за приходите създава и поддържа регистър на лицата, които по тяхно желание искат да не бъдат допускани до участие в хазартни игри, вкл. онлайн такива, организирани от ОХИ. Регистърът съдържа следната информация:

1. имена по документ за самоличност;
2. единен граждански номер (ЕГН) или личен номер на чужденец (ЛНЧ);
3. период на вписване, ако такъв е посочен;
4. дата на вписване.

Видно от правната регламентация на регистъра, може да се направи обосновано заключение, че същият представлява и „регистър с лични данни“ по смисъла на чл. 4, т. 6) от ОРЗД, а именно - *структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип*. Този факт обуславя приложимостта на ОРЗД, доколкото чрез регистъра се обработват лични данни (арг. чл. 2 от ОРЗД).

За да е законосъобразно обработването на лични данни е необходимо наличието на поне едно от основанията, посочени в чл. 6, пар. 1 и/или чл. 9, пар. 2 от ОРЗД, както и спазването на прогласените с чл. 5 от ОРЗД принципи за обработване на лични данни.

В съответствие с принципите личните данни следва да са:

- обработвани **законосъобразно, добросъвестно и по прозрачен начин** по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);
- събирани за **конкретни, изрично указани и легитимни цели** и не се обработват по-нататък по начин, несъвместим с тези цели; ... („ограничение на целите“);
- **подходящи, свързани със и ограничени до необходимото** във връзка с целите, за които се обработват („свеждане на данните до минимум“);
- **точни** и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);
- съхранявани във форма, която да позволява идентифицирането на субекта на данните **за период, не по-дълъг от необходимото за целите**, за които се обработват личните данни; ... („ограничение на съхранението“);
- обработвани по начин, който **гарантира подходящо ниво на сигурност** на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

Наред с това администраторът носи отговорност и трябва да докаже спазването на посочените по-горе принципи (т. нар. „отчетност“).

ЗХ предоставя правните основания за обработването на личните данни, съдържащи се в регистъра по чл. 10г от закона както за НАП, така и за ОХИ. НАП обработва данните по повод упражняване на своите законоустановени правомощия (по чл. 6, пар. 1, б д), пр. 2 от ОРЗД), а ОХИ ги обработват за целите на спазването на свое нормативно задължение (по чл. 6, пар. 1, б. в) от ОРЗД). В съответствие с принципа за прозрачност при обработването на лични данни администраторите –

съответно НАП и ОХИ, имат задължение да предоставят информация на субектите на данни (лицата, заявили участие в хазартни игри), предвидена в чл. 13 и спазвайки условията на чл. 12 от ОРЗД.

Един от реквизитите на тази информация е и срокът, за който ще се съхраняват личните данни. По правило той трябва да е подходящ и не по-дълъг от необходимото за постигане на целите, за които се обработват. НАП и ОХИ трябва да предвидят подходящ срок за съхранение на данните и след заличаването им от регистъра. Той следва да е обусловен от преклузивните срокове за упражняване на правата на субектите на данни, произтичащи както от ОРЗД, така и от друго специално секторно законодателство.

НАП и ОХИ обработват личните данни за различни цели, които произтичат от ЗХ. Следва да се има предвид обаче, че администратор на лични данни в регистъра по чл. 10г от ЗХ е НАП. При спазване на ЗХ и нормативните изисквания за защита на личните данни ОХИ трябва да имат само достъп до данните от въпросния регистър, администриран от НАП. Систематично тълкуване на правните норми на чл. 10д, ал. 1 и ал. 2 от ЗХ показва, че ОХИ имат право да бъдат уведомявани от НАП единствено за конкретно физическо лице, заявило желание за конкретно участие в хазартни игри при конкретен ОХИ. Това произтича от общите принципи на законодателството за защита на личните данни. Предварителният, пълен и неограничен достъп до данните в целия регистър би представлявал сериозно нарушение на принципите за защита на личните данни, поради потенциалната възможност от обработване на данните на трети лица, различни от конкретно явилите се при съответното ОХИ и заявили участие за конкретни хазартни игри. Нарушението на принципите за обработване на лични данни и липсата на правно основание са скрепени с по-високите санкции, въведени с чл. 83, пар. 5, б. а) от Регламент (ЕС) 2016/679.

Получаването и поддържането на паралелни регистри при ОХИ, от една страна, не отговаря на целите, регламентирани със ЗХ (недопускане на конкретни лица, вписани в регистъра, до конкретни хазартни игри при конкретен ОХИ в конкретен момент), а от друга – би представлявало обработване на лични данни от ОХИ без правно основание.

Нещо повече, поддържането на паралелни регистри при ОХИ, не гарантира по никакъв начин, че същите са точни и актуални към конкретния момент, в който даденото лице заявява участие в хазартни игри, като това води до нарушение както на ЗХ, така и на принципа за точност на данните и принципа за отчетност – задължение, произтичащо от законодателството за защита на данните.

Отчитайки установените в ЗХ условия за достъп до данните в регистъра и факта, че НАП администрира същия, то именно единствено Агенцията има правомощието и носи отговорността да определи техническите и организационни мерки за защита на данните, в частност на фактическия достъп до него. Това се обуславя също така и от задължението на администратора - НАП да извърши оценката на риска и съответно оценката на въздействието върху защитата на данните, обработвани в регистъра.

Принципно положение в законодателството за защита на данните е, че исканията за разкриване на данни, освен че трябва да са съобразени с целите на обработването, следва винаги да бъдат обосновани и да засягат само отделни случаи и не трябва да се отнасят до целия регистър с лични данни или да водят до свързване на регистри на лични данни. Това разбиране намира израз и в трайната практика на КЗЛД по въпросите за достъп до регистри, създавани и поддържани от публичните органи. Така например, КЗЛД има правомощие да разрешава предоставянето на данни от ЕСГРАОН на български и чуждестранни юридически лица по реда на чл. 106, ал. 1, т. 3, пр. 3 от Закона за гражданската регистрация. Предоставянето на такива данни се осъществява по искания на юридическите лица на справка за конкретно лице, за което е възникнала необходимост. Според практиката на КЗЛД пълен и неограничен достъп до регистри, поддържани от публични органи е недопустим.

По отношение на повдигнатите въпроси относно проверяването на голям брой лица в регистъра по чл. 10г от ЗХ и получаването в НАП на техните лични данни, трябва да се има предвид, че това е

предвидено и е допустимо от законодателството. В този смисъл, освен право, НАП има и задължение да обработва въпросните лични данни, както за целите на ЗХ, така и за други законови цели, свързани с данъчното облагане и мерките срещу изпирането на пари.

По аналогия с въведените от НАП мерки за защита на личните данни, ОХИ също трябва да предприемат подходящи и адекватни действия по привеждане на обработването на лични данни в съответствие с изискванията, произтичащи от законодателството за защита на данните.

В допълнение и за пълнота на изложението, следва да се има предвид, че нарушенията на законодателството за защита на личните данни могат да бъдат докладвани и по реда на новоприетия Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (ЗЗЛПСПОИН).

Настоящият правен анализ е базиран изцяло на трайната практика на КЗЛД, свързана с обработването на лични данни, на съдебната практика по жалби със сходен предмет, както и на насоките и становищата на Европейския комитет по защита на данни (ЕКЗД) в тази посока. Изразеното становище има единствено, принципен, консултативен характер за администратора/обработващия лични данни при прилагане на относимите правни норми, без да поражда права и/или задължения за заинтересованите страни, тъй като се базира само на посочените в искането обстоятелства. То не ограничава КЗЛД да разгледа всяка жалба или сигнал, свързани с предмета му. Съгласно Регламент (ЕС) 2016/679 администраторът на лични данни сам или съвместно с друг администратор определя правилата и процедурите за обработване на данни, които трябва да съответстват на законодателството за защита на личните данни. Той трябва да е в състояние да докаже това. За предприетите от администратора, съвместните администратори или обработващия действия по обработване на данните, се прилагат както правилата на отчетност, прозрачност и добросъвестност, така и разпоредбите, отнасящи се до ангажиране на административнонаказателна отговорност по отношение на законосъобразността на осъществяваните от него/тях дейности по обработване на лични 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:

В изпълнение на изискванията на чл. 10д, ал. 1 и ал. 2 от Закона за хазарта, както и на принципите за обработване на лични данни, прогласени с чл. 5 от Регламент (ЕС) 2016/679, НАП следва да предоставя на ОХИ единствено възможност за проверка на данните на конкретно физическо лице, заявило желание за конкретно участие в хазартни игри при конкретен ОХИ.

Предоставянето на ОХИ на предварителен, пълен и неограничен достъп до данните в целия регистър, поддържан от НАП, противоречи на принципите за обработване на лични данни.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

МОДЕЛИРАНЕ НА ВЗАИМОДЕЙСТВИЯТА В СИСТЕМАТА ЗА ЗАЩИТА НА ЛИЦАТА, ПОСДАВАЩИ СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАЩИ ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ



ПРОФ. Д.Т.Н. ВЕСЕЛИН ЦЕЛКОВ

член на Комисията за защита на личните данни

Ключови думи: защита на лицата подаващи сигнали за нарушения, моделиране на системи, функционални взаимодействия, синхронизация и контрол.

ВЪВЕДЕНИЕ

Изграждането на Системата за защита на лицата подаващи сигнали за нарушения (СЗЛПСН) е в съответствие с правната рамка на Република България (Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, ДВ. бр.11 от 2 февруари 2023г. [1]) и Директива 2019/1937 (т.нар. *Whistleblower Directive*) [2].

Основната цел на СЗЛПСН е да осигури „**защитата на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, станала им известна при или по повод изпълнение на трудовите или служебните им задължения или в друг работен контекст**“ [1].

За основа на разглежданията в този доклад е представения [4] многослоен модел на Системата за защита на лицата подаващи сигнали за нарушения, както следва:

- Слой 1: Информация за нарушения;
- Слой 2: Лица на които се предоставя защита;
- Слой 3: Задължени субекти;
- Слой 4: Институции, органи, служби и агенции на ЕС;
- Слой 5: Европейска комисия.

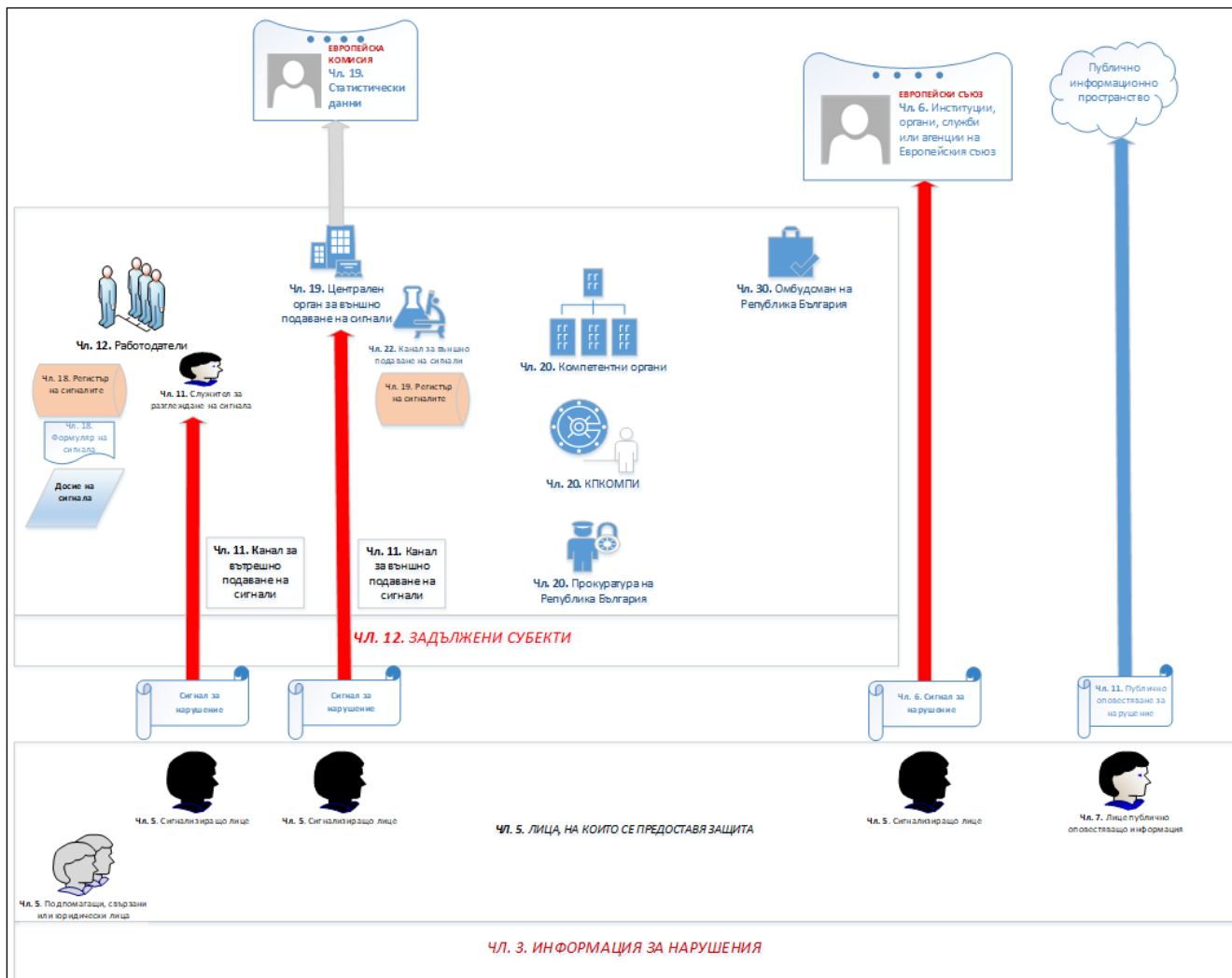
Дефинирани са структурните елементи на модела и типовете взаимодействия. Представени са модели на взаимодействията с най-голям обхват и значимост.

МНОГОСЛОЕН МОДЕЛ НА СИСТЕМАТА ЗА ЗАЩИТА

Структурните елементи на модела на системата за защита са:

- Информация за нарушения;
- Лица, на които се предоставя защита;

- Лица подаващи сигнал (сигнализиращо лице);
- Лица публично оповестяващи информация;
- Подпомагащи и свързани лица;
- Юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст;
- Задължени субекти, в това число:
 - Работодатели в публичния и частния сектор;
 - Централен орган за външно подаване на сигнали (ЦОВПС);
 - Компетентни органи;
 - Прокуратура на Република България;
 - Комисията за противодействие на корупцията и за отнемане на незаконно придобитото имущество (КПКОНПИ)
 - Омбудсман на Република България;
- Институции, органи, служби и агенции на ЕС;
- Европейска комисия.



Фигура 1. Модел на Системата за защита на лицата подаващи сигнали или публично оповестяващи информация за нарушения

Информация за нарушения

Информацията за нарушения обхваща сигнали или публично оповестяване на информация за:

- Нарушения на българското законодателство или на посочените в приложението към закона актове на Европейския съюз;
- Нарушения, които засягат финансовите интереси на Европейския съюз по смисъла на чл. 325 от Договора за функционирането на Европейския съюз [3];
- Нарушения на правилата на вътрешния пазар по смисъла на чл. 26, параграф 2 от Договора за функционирането на Европейския съюз, включително правилата на Европейския съюз и българското законодателство относно конкуренцията и държавните помощи;
- Нарушения, свързани с трансгранични данъчни схеми, чиято цел е да се получи данъчно предимство, което противоречи на предмета или на целта на приложимото право в областта на корпоративното данъчно облагане;
- Извършено престъпление от общ характер, за което лице по чл. 5 е узнало във връзка с извършване на своята работа или при изпълнение на служебните си задължения [1].

Задължени субекти

Задължени субекти

Основните функции на всички задължени субекти са:

- Изграждат Канал за вътрешно подаване на сигнали;
- Определят служител за разглеждане на сигнали;
- Комуникират с лицата подали сигнали;
- Комуникират с лицата засегнати от сигнали;
- Поддържат Регистър на подадените сигнали;
- Комуникират с ЦОВПС.

Централен орган за външно подаване на сигнали

Централният орган за външно подаване на сигнали изпълнява:

- Изгражда Канал за външно подаване на сигнали (КВПС);
- Проверява сигналите и ги изпраща по компетентност;
- Поддържа Регистър на сигналите;
- Разглежда публично оповестена информация като сигнал, ако за това има информация в ЦОВПС;
- Точка за контакт с институциите, органите, службите и агенциите на ЕС;
- Предава на Европейската комисия обобщени статистически данни;
- Дава методически указания, извършва обучение и контрол.

Компетентните органи

Компетентните органи са:

1. Комисията за защита на конкуренцията;
2. Комисията за финансов надзор;
3. председателя на Държавната агенция за метрологичен и технически надзор;
4. министъра на транспорта и съобщенията;
5. министъра на околната среда и водите;
6. председателя на Агенцията за ядрено регулиране;
7. Българската агенция за безопасност на храните;

8. главния държавен здравен инспектор по смисъла на Закона за здравето;
9. Комисията за защита на потребителите;
10. Националният екип за реагиране при инциденти с компютърната сигурност;
11. министъра на финансите;
12. изпълнителния директор на Националната агенция за приходите;
13. изпълнителния директор на Изпълнителна агенция „Главна инспекция по труда“;
14. областни управители.

Компетентните органи в рамките на техните правомощия:

- Извършват проверки по сигналите за нарушения;
- Информират ЦОВПС за резултатите от проверката;
- Изпълняват указанията на ЦОВПС.

Омбудсман на Република България

Омбудсманът на Република България:

- Осъществява външен одит на ЦОВПС;
- Извършва проверка на КВПС;
- Приема и разглежда жалби срещу ЦОВПС.

Канали за подаване на сигнали

Видове канали за подаване на данни

Каналите за подаване на данни биват:

- Канал за вътрешно подаване на сигнали;
- Канал за външно подаване на сигнали;
- Публичното оповестяване на информация се разглежда като Канал за външно подаване на сигнали.

Изисквания към Каналите за подаване на данни

Каналите за подаване на данни осигуряват:

- Поверителност, цялостност и наличност на информацията;
- Трайно архивиране;
- Одит и актуализация на правилата за функциониране.

Сигнал за нарушения

Формуляр на сигнала

За регистрирането на сигнала се използва формуляр, който съдържа най-малко следните данни:

1. трите имена, адрес и телефон на подателя, както и електронен адрес, ако има такъв;
2. имената на лицето, срещу което се подава сигналът, и неговата месторабота, ако сигналът се подава срещу конкретни лица и те са известни;
3. конкретни данни за нарушение или за реална опасност такова да бъде извършено, място и период на извършване на нарушението, ако такова е извършено, описание на деянието или обстановката и други обстоятелства, доколкото такива са известни на сигнализиращото лице;
4. дата на подаване на сигнала;
5. подпис, електронен подпис или друга идентификация на подателя.

Регистър на сигналите

За отчетност и контрол се създава и поддържа регистър на сигналите за нарушения, който не е публичен. Регистърът съдържа информация за:

1. лицето, което е приело сигнала;
2. датата на подаване на сигнала;
3. засегнатото лице, ако такава информация се съдържа в сигнала;
4. обобщени данни за твърдяното нарушение, като място и период на извършване на нарушението, описание на деянието и други обстоятелства, при които е било извършено;
5. връзката на подадения сигнал с други сигнали след установяването и в процеса на обработване на сигнала;
6. информация, която е предоставена като обратна връзка на лицето, подало сигнала, и датата на предоставянето и;
7. предприетите последващи действия;
8. резултатите от проверката по сигнала;
9. периода на съхраняване на сигнала.

Синхронизация на информацията за сигналите

За синхронизация на информацията за сигнала, формуляра на сигнала и начина на водене на регистъра, ЦОВПС:

- Издава Уникален Идентификационен Номер (УИН) за всеки получен сигнал;
- Утвърждава образец на Формуляра на сигнала;
- Определя с Наредба, реда и начина за воденето на Регистъра на сигналите;
- Издава указания за структурата и съдържанието на Досието на сигнала и начините извършване на проверката по сигнала.

ЗАЩИТА НА ЛИЦАТА ПОДАВАЩИ СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАЩИ ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ

Мерките за поверителност и защита на лицата обхващат:

- Защита на информацията;
- Защита на самоличността на сигнализиращите лица;
- Забрана за ответни действия спрямо сигнализиращите лица;
- Задължителни предписания за преустановяване на увреждащите действия;
- Право на обезщетение за претърпените имуществени и неимуществени вреди;
- Освобождаване от отговорност.

МОДЕЛ НА ВЗАИМОДЕЙСТВИЯТА В СИСТЕМАТА ЗА ЗАЩИТА НА ЛИЦАТА ПОДАВАЩИ СИГНАЛИ ЗА НАРУШЕНИЯ

На формализиране и анализ подлежат взаимодействията:

- Служител за разглеждане на сигнала – лице подаващо сигнала;
- Служител за разглеждане на сигнала – подпомагащи и свързани лица;
- Служител за разглеждане на сигнала – юридически лица, свързани с лицето подаващо сигнала;
- Служител за разглеждане на сигнала – засегнато лице;
- Служител за разглеждане на сигнала – ЦОВПС;
- ЦОВПС – КВПС;

- ЦОВПС – компетентни органи;
- ЦОВПС – КПКМПИ;
- ЦОВПС – Прокуратура на Република България;
- ЦОВПС – Европейска комисия;
- ЦОВПС - Институции, органи, служби и агенции на ЕС;
- ЦОВПС - Лица, на които се предоставя защита:
 - ЦОВПС - Лица подаващи сигнал (сигнализиращо лице);
 - ЦОВПС - Лица публично оповестяващи информация;
 - ЦОВПС - Подпомагащи и свързани лица;
 - ЦОВПС - Юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст;
- Омбудсман на Република България – ЦОВПС.

Ще бъдат разгледани взаимодействията с най-голям обхват и предизвикващи обществен интерес а именно:

- Служител за разглеждане на сигнала – лице подаващо сигнала;
- Служител за разглеждане на сигнала – засегнато лице.

Моделиране на взаимодействието „Служител за разглеждане на сигнала – лице подаващо сигнала“. Действия.

СЛУЖИТЕЛ ЗА РАЗГЛЕЖДАНЕ НА СИГНАЛА (СРС)	ЛИЦЕ ПОДАВАЩО СИГНА (СЛ)
СРС поддържа Регистър на сигналите	
	СЛ – подава сигнал до СРС Възможни са начините: • Писмено (попълнен формуляр); • По електронна поща (попълнен формуляр); • Устно. Възможно е предоставяне и допълнителни материали
СРС – приема сигнала • Получава УИН от ЦОВПС • Потвърждава приемането в 7 дневен срок	
• Ако сигналът е устен – СРС попълва формуляр	СЛ – може да подпише формуляра (по желание)
• Ако има пропуски – СРС дава 7 дневен срок за отстраняването им • Ако пропуските не са отстранени – сигналът се връща на СР	СЛ – отстранява пропуските • Ако – да – продължава • Ако – не – получава върнатите материали

СРС проверява сигнала за достоверност • Не се разглеждат сигнали не попадащи в предметното поле на закона или не са правдоподобни; • При неверни или заблуждаващи твърдения, сигналът се връща на СЛ за поправка и отговорността за убеждаване	СЛ има възможност за: • Поправи твърденията; • Оттегли сигнала.
СРС предоставят на СЛ информация за Външния канал за подаване на сигнали и Европейските институции • Ако сигналът е срещу работодателя, насочва СЛ към канала за външно подаване на сигнали.	СЛ получава информацията • СЛ подава сигнала по външния канал за подаване на сигнали
СРС поддържат връзка със СЛ	СЛ предоставя изискваните материали
СРС изготвя индивидуален доклад по сигнала: • Кратка информация по сигнала; • Предприетите действия; • Окончателните резултати от проверката.	
СРС предоставя обратна информация на СЛ за предприетите действия в срок не по-дълъг от три месеца от потвърждаването на получаването на сигнала	СЛ получава информацията за предприетите действия
СРС при необходимост: • Препращат сигнала до ЦОВПС; • Предварително уведомява СЛ за препращането на сигнала.	СЛ получава предварителното уведомление за препращането на сигнала до ЦОВПС.

Моделиране на взаимодействието „Служител за разглеждане на сигнала – засегнато лице“.
Действия.

СЛУЖИТЕЛ ЗА РАЗГЛЕЖДАНЕ НА СИГНАЛА (СРС)	ЗАСЕГНАТО ЛИЦЕ (ЗЛ)
СРС поддържа Регистър на сигналите	
СРС уведомява ЗЛ (осигурява анонимност на сигнала)	На ЗЛ се дава възможност за: • Устни обяснения; • Писмени обяснения; • Предоставяне на доказателства.
СРС: • Изслушва ЗЛ; • Приема писмените обяснения; • Събира и оценя предоставените от ЗЛ доказателства.	

СРС: • Предоставят на ЗЛ всички събрани доказателства по сигнала; • Дава се възможност на ЗЛ да предостави възражения по тях в 7 дневен срок	ЗЛ: • Получава от СРС всички събрани доказателства по сигнала; • Има възможност да предостави възражения по тях в 7 дневен срок
СРС дава възможност на ЗЛ да представи и посочи нови доказателства	ЗЛ има възможност да предостави и посочи нови доказателства
СРС изготвя индивидуален доклад по сигнала: • Кратка информация по сигнала; • Предприетите действия; • Окончателните резултати от проверката.	
СРС - при потвърден сигнал, организира последващи действия	
СРС при необходимост: • Препращат сигнала до ЦОВПС.	

Моделирането на останалите взаимодействия в Системата са в процес на разработване и прецизиране.

ЗАКЛЮЧЕНИЕ

Предложените модели на взаимодействията в Системата за защита на лицата подаващи сигнали за нарушения системата могат да послужат като теоретична основа за изграждането и функционирането на Системата. Те са основата за моделиране и синхронизиране на взаимодействията между структурните звена на Модела.

В доклада е отразено личното виждане и опитът на автора като член на Комисията за защита на личните данни, Централен орган за външно подаване на сигнали. Доклада съдържа и част от изследванията направени от автора в Университета по библиотекознание и информационни технологии.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, ДВ. бр.11 от 2 февруари 2023г.
2. Директива 2019/1937 (т.нар. Whistleblower Directive)
3. Договор за функционирането на Европейския съюз от 13 декември 2007 година
4. Tselkov, V., Model of the Whistleblower Protection6Systems, International Scientific Conference "TECHNICS. TECHNOLOGIES. EDUCATION. SAFETY", ISSN 2535-0315 (Print), ISSN 2535-0323 (Online)

Комисия за защита на личните данни

Председател: Венцислав Караджов

Членове: Цанко Цолов

Мария Матева

Веселин Целков

Информационен бюлетин № 3 (102) 2023 г.

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

Уеб сайт на КЗЛД: www.cpdp.bg

Разпространява се в електронен вид

ISSN 2367-7759