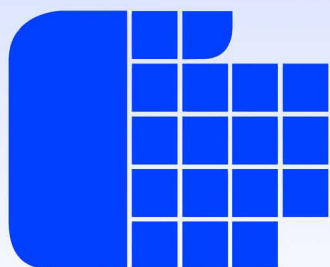


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 3 (96), май 2022 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода март и април 2022 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
КЗЛД депозира в Народното събрание отчета за дейността си през 2021 година. Резюме на отчета	3
Комисията за защита на личните данни е отличена от Съюза на юристите в България	7
КЗЛД издаде информационна брошура “Широкомащабните информационни системи на ЕС”	8
КЗЛД издаде информационна брошура “Правата на децата и младите хора при работа в дигитални платформи. Защита и укрепване на правата на децата и младите хора”	16
КЗЛД се включва активно в инициативи, свързани с правата на децата в дигитална среда	24
Заседания на Европейския комитет по защита на данните	26
ЕКЗД и ЕНОЗД приеха първо за тази година съвместно становище	27
Европейската комисия предложи правила за повишаване на киберсигурността и информационната сигурност в институциите, органите, службите и агенциите на ЕС	28
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	31
РЕШЕНИЯ НА КЗЛД	32
СТАНОВИЩА НА КЗЛД	47

СЪБИТИЯ И ИНИЦИАТИВИ

КЗЛД ДЕПОЗИРА В НАРОДНОТО СЪБРАНИЕ ОТЧЕТА ЗА ДЕЙНОСТТА СИ ПРЕЗ 2021 ГОДИНА. РЕЗЮМЕ НА ОТЧЕТА.



На 16 март 2022 г. Комисията за защита на личните данни депозира в деловодството на Народното събрание **Годишния отчет за дейността си през 2021 година**. Отчетът се състои от 172 страници, обособени в 12 основни раздела. Депозиран е съгласно чл. 7, ал. 6 от Закона за защита на личните данни и обхваща периода от 01.01.2021 г. до 31.12.2021 г.

В Годишния отчет за 2021 г. е предоставена информация за основните направления на дейността на КЗЛД в посочения период. Направен е анализ на степента на постигане на целите и приоритетите за 2021 г. и са дефинирани целите и приоритетите за 2022 г. Поставен е акцент върху надзора, осъществяван от КЗЛД в две основни насоки: разглеждане на жалби за нарушени права в областта на защитата на личните данни и осъществяване на проверки на администратори и обработващи лични данни за законосъобразност на обработването.

Към 31 декември 2021 г. в КЗЛД са постъпили общо 840 бр. жалби и 487 бр. сигнали за нарушения в областта на защитата на личните данни и искания за предприемане на контролни действия, подадени от физически и юридически лица, държавни органи и организации, както и запитвания по актуални въпроси във връзка с обработването на лични данни и изложени твърдения за нарушения на Регламент 2016/679 и ЗЗЛД. Налице е постоянна тенденция на повишаване обема и сложността на постъпващите жалби и сигнали, и извършените проверки. Прави впечатление, че подадените жалби се отличават с правна и фактическа сложност, включително с намесата на международен елемент - жалбоподатели, които не са български граждани или администратори на лични данни с основно място на установяване извън територията на Република България.

Продължава тенденцията от последните години за драстично увеличаване на жалбите срещу осъществявано видеонаблюдение - през 2021 г. техният брой расте до 196, обстоятелство, което води до засилена и натоварена контролна дейност върху обработването на лични данни на физически лица посредством изградени системи за видеонаблюдение. Други сектори на дейност на администраторите, срещу които през отчетния период най-често са постъпвали жалби от граждани, са банки и кредитни институции (64 бр.), държавни органи (57 бр.), телекомуникации (51 бр.), физически лица (51 бр.), политически субекти (46 бр.), здравеопазване (29 бр.), медии (22 бр.), трудови и осигурителни услуги (12 бр.), застраховане (9 бр.) и образование (4 бр.).

Комисията е приела решения по 420 жалби, както следва: по основателност на жалби – 257 решения (от тях за основателни са приети 142 жалби, а за неоснователни 115); по недопустимост на жалби – 49 решения (включително решение, с което КЗЛД е приела за недопустими 704 жалби, обединени в едно производство, подадени по повод нарушението на сигурността при обработване на лични данни от НАП); по нередовност на жалби и искания – 56 решения; за очевидна неоснователност – 54 решения. Оттеглените жалби са 4, с което КЗЛД на практика е била десезирана.

Анализът на съдебната практика показва много висок процент на потвърдени от съда решения на надзорния орган. През отчетния период административните съдилища, като първа инстанция, са се произнесли по 97 съдебни дела, образувани по жалби срещу решения на КЗЛД, като с 79

съдебни решения са потвърдени оспорените административни актове на КЗЛД, с 2 съдебни акта са частично отменени или изменени постановени от КЗЛД решения в санкционната част, отменени изцяло са 16 издадени от КЗЛД решения. Върховният административен съд (ВАС), като касационна инстанция, е потвърдил 41 издадени от КЗЛД индивидуални административни акта, 2 индивидуални административни акта на КЗЛД са частично отменени или изменени в санкционната част, 6 решение на КЗЛД са отменени изцяло.

От отработените през 2021 г. 468 бр. сигнала, най-много са тези, подадени срещу администратори на лични данни, предоставящи интернет услуги – 120 бр. На следващо място са сигнали за евентуално незаконосъобразно обработване от органи на държавната администрация – 42 бр., от администратори, обработващи лични данни чрез изградени системи за видеонаблюдение – 28 бр. Получени са сигнали и за незаконосъобразно обработване на лични данни в областта на здравеопазването – 27 бр., телекомуникациите – 27 бр., за целите на директния маркетинг – 21 бр., в сферата на банковото дело – 16 бр., срещу медии – 16 бр., срещу куриерски дружества – 10 бр., срещу застрахователни дружества – 7 бр., срещу сайтове за търсене и предлагане на работа – 8 бр. и сигнали, касаещи обработването на лични данни в изборния процес през 2021 г. – 10 бр. и др.

Следва да се отбележи, че постъпилите сигнали и искания през 2021 г. са многобройни и разнородни по своето естество, като преобладаващи са тези, в които се съобщава за предполагаема злоупотреба с лични данни, като често пъти се търси съдействие за разрешаване на междуличностни конфликти посредством запитвания, отправени до КЗЛД. Увеличават се сигналите и запитванията по теми, свързани със социалните мрежи, провеждане на онлайн събития, видеонаблюдение и видеозаснемане, обработване на лични данни от куриерски компании. Очертават се нови проблемни сфери, като онлайн платформите за търсене и предлагане на работа и онлайн залагания. Голям брой сигнали и запитвания касаят публично оповестени/публикувани документи с лични данни.

През 2021 г. са назначени 227 бр. проверки на място, от които са извършени 206 бр. Сред извършените проверки са тези на администратори по линия на Шенгенската информационна система (ШИС) – „Национален институт по криминалистика“, МВнР-Национален визов център, МВР-ДМОС-Бюро „СИРЕНЕ“, МВР-ДМОС-Национално звено „Европол“, МВР „Комуникационни и информационни системи“, като са наложени корективни мерки с цел повишаване на сигурността на обработваните бази данни. Значима проверка от обществен интерес през отчетния период е проверката на Агенцията по вписванията, осъществена по инициатива на Комисията след постъпил в КЗЛД одитен доклад на Сметната палата. Наложена е корективна мярка, а за констатираните нарушения е съставен акт за установяване на административно нарушение, по който председателят на КЗЛД е наложил санкция в размер на 250 000 лева. Наказателното постановление е обжалвано и в края на отчетния период се намира в съдебна фаза.

В допълнение е необходимо да се споменат и проверките относно обработване на личните данни от топлинните счетоводители и особено обемната и тежка проверка на болницата в с. Радунци, където са констатирани нарушения по отношение на повече от 65 000 медицински досиета и над 3000 трудови досиета.

Въпреки постъпилите сигнали за незаконосъобразно предоставяне на лични данни на граждани на Република България в трети държави във връзка с електронното преброяване през 2021 г., осъществено от Националния статистически институт, КЗЛД не е установила незаконосъобразни действия по обработването на данни, участващи в провежданото от НСИ „Електронно преброяване 2021“.

Въз основа на извършени проверки на място през отчетния период са съставени 5 акта за установяване на административни нарушения и са издадени 4 наказателни постановления.

За отчетния период в Комисията са получени общо 140 уведомления за нарушения на сигурността на данните. От тях, с ниско ниво на риск са преценени 10 уведомления, със средно ниво – 81 уведомления (от тях 62 на застрахователни брокери) и с високо ниво – 6 уведомления. За

14 от случаите има трансгранично обработване на данни, което е наложило КЗЛД да се конституира като засегнат орган. По останалите уведомления действията на КЗЛД са разнородни: потърсено съдействие от органите на МВР, констатирана липса на компетентност или констатация, че липсва реално нарушение на сигурността на личните данни. Анализът на нарушенията на сигурността на данните от гледна точка на техния характер показва, че дигиталните пробиви в сигурността на данните са значително по-голям процент от „обикновените“ (физическите) пробиви, като най-голям процент са случаите на инциденти, свързани с външни злонамерени атаки към системите на администраторите, представляващи различни по вид киберпрестъпления. Останалите често срещани причини за инциденти са неволни технически грешки, загуба на документи, злоупотреба със служебно положение.

По линия на надзорната дейност към края на годината са наложени следните корективни мерки: Предупреждения – 21 бр., Официални предупреждения – 27 бр., Разпореждания – 145 бр., Временно или окончателно ограничаване на обработването на лични данни – 1 бр., Глоби/имуществени санкции – 44 бр. Наложените глоби и имуществени санкции през отчетния период са общо в размер 444 150 лв., от които с решения на КЗЛД в размер на 117 150 лв. и с наказателни постановления на председателя на КЗЛД в размер на 327 000 лв.

Към края на отчетния период в процес на принудително събиране от НАП са 649 409 лв., като вече събраните суми са в размер 94 010, 08 лв. През 2021 г. доброволно са платени глоби и имуществени санкции в размер на 474 695 лв.

През изтеклата година КЗЛД е изразила 55 становища по множество въпроси от областта на защитата на личните данни, както по искания на публични органи, така и по принципни запитвания на юридически и физически лица и 11 решения, с които е разрешила предоставянето на лични данни от ЕСГРАОН на основание чл. 106, ал. 1, т. 3, предл. 3 от Закона за гражданската регистрация. В допълнение към тях, КЗЛД е изразила становища и по три преюдициални запитвания, които са предложени и приети като част от формиране на позицията на Република България пред Съда на ЕС.

През 2021 г. Комисията за защита на личните данни е извършила анализ на действащата в Република България правна уредба, имаща отношение към обработването на лични данни с цел установяване на степента на съответствие с актуализираните през 2018 г. правила за защита на личните данни. Идентифицирани са няколко конкретни области на несъответствие, които съответно: изискват актуализация на законови и подзаконови актове по същество с цел отразяване на прякото действие на Регламент (ЕС) 2016/679; налагат правно-технически промени в отделни нормативни актове; констатира липса на регламентация в национален план (в областта на здравеопазването). Резултатите от прегледа на законодателството са предоставени на вниманието на Министерския съвет за предприемане на действия по компетентност, по негова преценка, с копие до съответните публични структури, в чийто предмет на дейност е съответния нормативен акт, по отношение на който Комисията е констатирала несъответствия с правилата за защита на данните (22 бр. нормативни актове).

През отчетния период КЗЛД е извършила анализ на съвременните заплахи и предизвикателства пред защитата на личните данни в следните области: тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване; големите бази данни /Big Data/ и свързаната с тях възможност за профилиране; правата на децата и младите хора при работа в дигитални платформи.

През 2021 г. КЗЛД е предоставила множество писмени консултации – 453 бр. (вкл. становищата, посочени по-горе). Същите се отнасят до разяснения в правната уредба, по които има ясна и еднозначна регламентация и/или трайна практика на надзорния орган.

Активност е демонстрирана и по линия на участието във всички международни формати, обединяващи сродни органи по защита на данните, които са провеждали онлайн заседания или в рамките на които е обменена интензивна кореспонденция по актуални теми от сферата на защитата на личните данни. В резултат на тази активна международна дейност са изразени становища/позиции и е осъществено участие в различни международни инициативи - общо 538 бр.

По редица въпроси от обществен интерес, имащи отношение към обработването и защитата на личните данни, през отчетния период КЗЛД е осъществила ползотворно сътрудничество, вкл. в оперативен порядък, с множество държавни органи, сред които Инспекторатът към Висшия съдебен съвет, Министерството на здравеопазването, Министерството на вътрешните работи, Министерството на правосъдието, Министерството на външните работи, Министерството на регионалното развитие и благоустройството, Министерството на образованието, Министерството на транспорта, информационните технологии и съобщенията и Комисията за регулиране на съобщенията. Успешно е продължило участието на Комисията в дейността на Работна група № 5 „Конкуренция“, Работна група № 17 „Телекомуникации и информационни технологии“, Работна група № 23 „Сътрудничество в областта на вътрешните работи“ и Работна група № 33 „Сътрудничество в областта на правосъдието“ (създадени с Постановление на МС № 85 от 17 април 2007 г. за координация по въпросите на Европейския съюз).

В изпълнение на задължението за поддържане на публичен регистър на администраторите и обработващите, които са определили длъжностни лица по защита на данните, през 2021 г. КЗЛД е вписала в регистъра 358 бр. администратори/обработващи, с което общия им брой е станал 5075.

В своя отчет за 2021 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 обществен сектор за 2021 г.

Предоставена е подробна информация за институционалното взаимодействие, информационно-образователната дейност, медийната политика, административния капацитет и финансовото състояние на КЗЛД. Специален акцент е поставен върху недостига на финансови и човешки ресурси, които да гарантират адекватно, навременно и качествено изпълнение на надзорните функции на Комисията. Предвид приоритетността на този въпрос, през 2021 г. са проведени 18 конкурса и процедури за мобилност за общо 13 свободни позиции. Други три конкурса са започнати и неприключени към 31.12.2021 г.

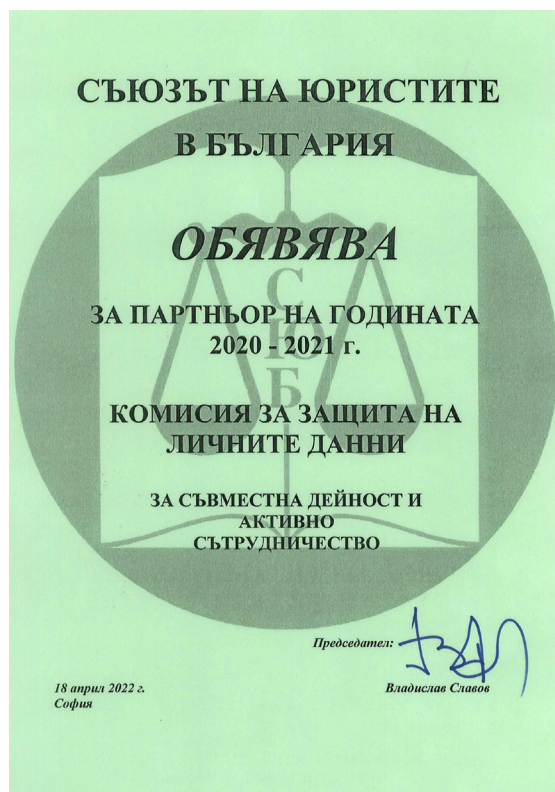
За обезпечаване на дейността на Комисията за защита на личните данни и нейната администрация през 2021 г. са извършени разходи общо в размер на 3 100 781 лв. или 99,16% от утвърдените разчети за годината.

В края на годишния си отчет КЗЛД формулира своите цели и приоритети за 2022 г. в следните направления:

1. Отбелязване на 20-та годишнина от създаването на Комисията за защита на личните данни.
2. Приемане на нова Стратегия на КЗЛД за развитие в областта на защитата на личните данни.
3. Финализиране на подзаконовата правна уредба в областта на защитата на личните данни и изпълнение на правомощия, произтичащи от националното законодателство.
4. Изводи от анализите на съвременните заплахи и предизвикателства.
5. Продължаване на усилията на КЗЛД за пълноправно членство в Шенген.

Годишният отчет на КЗЛД за 2021 г. е публикуван на институционалния сайт – **ТУК**.

КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ Е ОТЛИЧЕНА ОТ СЪЮЗА НА ЮРИСТИТЕ В БЪЛГАРИЯ



На 18 април 2022 г. в сградата на Съюза на юристите в България се проведе тържествено събрание по повод Деня на Конституцията, юриста и съдебните служители.

Събранието беше открито от Владислав Славов, председател на Съюза. Слово произнесе председателят на Конституционния съд Павлина Павлова. Приветствие към участниците отправиха министърът на правосъдието Надежда Йорданова, министърът на вътрешните работи Бойко Рашков, председателят на ВАС Георги Чолаков и омбудсманът Диана Ковачева.

Традиционните награди бяха връчени на юристи за професионална и съюзна дейност. Наградата за „Партньор на годината за 2020 и 2021 г.“ беше връчена на Комисията за защита на личните данни и получена от председателя ѝ Венцислав Караджов.

Венцислав Караджов благодари за признанието и сподели, че успешното партньорство е резултат от общи етични, морални и професионални стандарти, които двете организации споделят.



КЗЛД ИЗДАДЕ ИНФОРМАЦИОННА БРОШУРА “ШИРОКОМАЩАБНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ НА ЕС”

В Европейския съюз функционират няколко широкомащабни информационни системи, съдържащи лични данни. Надзорът върху тях се споделя между националните органи за защита на данните и ЕНОЗД, които работят заедно за постигането на високо и съгласувано ниво на защита на данните.

Пред март 2022 г. КЗЛД издаде информационна брошура, в която са представени 9 широкомащабни информационни системи на ЕС, чиято цел е подпомагане на гарантирането на сигурността в ЕС – защита на гражданите, борба с престъпността и сигурност на границите. В брошурата е предоставено кратко описание на целта на всяка система, нейният администратор на национално ниво, категориите лица, чиито лични данни се обработват, както и съответните типове лични данни. Разяснени са правата на физическите лица по отношение на личните им данни в тези системи и реда за тяхното упражняване. Посочено е, че на територията на Република България, надзорът над системите в областта на защита на личните данни се осъществява от Комисията за защита на личните данни. Предоставена е отправка към публикуваните на сайта на КЗЛД [контакти с компетентните органи](#), които администрират системите на национално ниво.

Брошурата има за цел да подпомогне практическото разбиране за различните информационни системи на Европейския съюз, както и възможностите за упражняване правата на физическите лица, субекти на данните, по смисъла на законодателството за защита на данните в ЕС.

Същата е публикувана и на сайта на КЗЛД – [ТУК](#).

В настоящия бюлетин публикуваме съдържанието на брошурата:

Широкомащабните информационни системи на ЕС са информационни системи за защитата на гражданите, борбата с престъпността и сигурността на границите. Целта им е да спомагат за поддържане на сигурността в държавите от Европейския съюз (ЕС).

В настоящия информационен материал са представени следните широкомащабни информационни системи на ЕС:

- Шенгенската информационна система от второ поколение (SIS II);
- Визовата информационна система (VIS);
- Информационната система ЕВРОДАК (EURODAC);
- Системата на Агенцията на ЕС за сътрудничество в областта на правоприлагането ЕВРОПОЛ (EUROPOL);
- Митническата информационна система (CIS);
- Системата за влизане/излизане (EES);
- Европейската система за информация за пътуванията и разрешаването им (ETIAS);
- Европейската система за информация за присъди срещу граждани на трети държави и лица без гражданство (ECRIS-TCN);
- Системата на Агенцията на ЕС за сътрудничество в областта на наказателното правосъдие (EUROJUST).

Централните компоненти на европейско ниво на представените системи се администрират от *Европейска агенция за оперативното управление на широкомащабни информационни системи* (EU-LISA). Компетентни органи на всяка държава-членка на ЕС администрират националните части на тези системи.

Всички физически лица могат да упражняват следните права по отношение на личните им данни пред националните компетентни органи, които са отговорни за функционирането на широкомащабните системи в страната:

- право на информация;
- право на достъп до собствените им лични данни;
- право на коригиране (неточни или непълни);
- право на изтриване (право „да бъдеш забравен“);
- право на ограничаване на обработването от страна администратора (когато е приложимо);
- правото на преносимост на личните данни (когато е приложимо);
- право на възражение.

Лицата, които са се възползвали от някое от правата си, получават писмен отговор от компетентния орган относно предприетите от съответното ведомство действия. Ако физическо лице счита, че правата му съобразно европейското и национално законодателство в областта на защита на личните данни не са спазени, същото може да обжалва действията на компетентния орган, пред КЗЛД или по съдебен ред.

Надзорът над процесите по обработване на лични данни на европейско ниво в тези системите се осъществява от Европейския надзорен орган по защита на данните (EDPS) в съответствие с разпоредбите на *Регламент (ЕС) 2018/1725*. Към настоящия момент надзорът се осъществява от координационните групи за надзор на SIS II, VIS, EURODAC, CIS, както и от Съвместния надзорен орган на EUROPOL. Предвижда се същият да се прехвърли към Координирания комитет за надзор.

На територията на Република България, надзорът над системите в областта на защита на личните данни се осъществява от Комисията за защита на личните данни (КЗЛД). На сайта на КЗЛД са публикувани контактите на компетентните органи, които администрират системите на национално ниво ([тук](#)).

Шенгенска информационна система от второ поколение (SIS II)

Шенгенската информационна система от второ поколение (ШИС II) е инструмент от основно значение за прилагането на разпоредбите на достиженията на правото от Шенген, включени в рамката на ЕС. ШИС II допринася за поддържането на високо ниво на сигурност, като подпомага оперативното сътрудничество между националните компетентни органи – граничната охрана, полицията, митническите органи, имиграционните органи и органите, отговарящи за предотвратяването, разкриването, разследването или наказателното преследване на престъпления или за изпълнението на наказания и органите по защита на данните. ШИС II функционира в съответствие с разпоредбите на действащите към настоящия момент *Регламент 2018/1860*, *Регламент 2018/1861* и *Регламент 2018/1862* на Европейския парламент и на Съвета.

Националната Шенгенска информационна система (НШИС) се създава, поддържа и експлоатира в МВР и е свързана с централната ШИС. Бюро „СИРЕНЕ“ в структурата на Дирекция „Международно оперативно сътрудничество“ на МВР е компетентното звено за обмен на информация във връзка със сигналите в ШИС II.

Администратор на системната на национално ниво е Министърът на вътрешните работи.

В НШИС се обработват сигнали за следните категории лица:

- Издирвани лица;
- Граждани на трети страни, за които има издаден отказ за влизане съгласно Закона за чужденците в Република България както и граждани на трети страни, за които е предприета

ограничителна мярка с цел недопускане на влизане или транзитно преминаване през територията на държавите членки;

- Безследно изчезнали лица, които е необходимо да бъдат поставени под закрила, и/или да се установи местонахождението им;
- Свидетели, лица, които са призовани, или лица, които се издирват, за да бъдат призовани да се явят пред съдебните органи във връзка с наказателно производство;
- Лица, подлежащи на дискретно наблюдение или специфичен контрол въз основа на постъпило искане от компетентните органи за защита на националната сигурност, опазване на обществения ред или съдебен орган;
- Информация за граждани на трети страни, които биха могли да бъдат свързани с терористични действия.

За лица, по отношение на които се въвеждат сигнали в НШИС, се обработват следните данни:

- фамилно и собствено име, рождено име, предишни имена и псевдоними;
- особени белези;
- място и дата на раждане;
- пол;
- снимки;
- пръстови отпечатыци;
- гражданство/а;
- дали лицето е въоръжено, склонно към насилие или избягало;
- основание за сигнала;
- орган, инициатор на сигнала;
- номер на решението, въз основа на което е въведен сигналът;
- мерки, които трябва да бъдат предприети;
- връзка с други сигнали в ШИС.

Визова информационна система (VIS)

Визовата информационна система на Европейския съюз (ВИС) представлява автоматизирана информационна система за обработване на данните от заявленията за визи, включително решенията по тях, постъпили в консулските служби на задграничните представителства на държавите – членки на ШЕНГЕН, както и за издаване на визи на граничните контролно-пропускателни пунктове на външната граница на ЕС.

Към настоящия момент Република България не е активен ползвател на ВИС. България ще получи достъп и ще може да използва и въвежда данни във ВИС след приемане на решение на Съвета на ЕС относно пълното прилагане на достиженията на правото от ШЕНГЕН в Република България.

ВИС функционира в съответствие с разпоредбите на действащия към момента *Регламент (ЕО) № 767/2008 на Европейския парламент и на Съвета от 9 юли 2008 година относно Визовата информационна система (ВИС) и обмена на данни между държави-членки относно визите за краткосрочно пребиваване.*

Националната визова информационна система (НВИС) представлява автоматизирана информационна система за съхранение и обработка на данните от заявленията за визи, както и за издаване на визи на ГКПП на българската граница. НВИС осигурява съхранение и обработка и на

данни от заявления за издаване на български документи за самоличност, постъпили в консулските служби на българските задгранични представителства.

НВИС се администрира, поддържа и експлоатира от Националния Визов Център към Дирекция „Консулски отношения“ на Министерството на външните работи и е свързана с ВИС на ЕС чрез специализиран интерфейс за връзка.

Администратор на системата на национално ниво е Министерството на външните работи.

В НВИС се съхраняват лични данни, вкл. биометрични данни (снимки и пръстови отпечатыци) на кандидатите за виза, както и информацията относно издадени, отказани, анулирани, отменени или продължени визи както и следните данни:

- фамилия, фамилия по рождение (предишна/и фамилия/и), име(на), пол, дата, място и страна на раждане;
- настоящо гражданство и гражданство по рождение;
- вид и номер на документа за задгранично пътуване, органът, който го е издал и датите на издаване и изтичане на срока на валидност;
- място и дата на подаване на заявлението за издаване на виза;
- вид виза, за която се подава заявление;
- данни на лицето, изпращащо покана и/или поемащо разноските на кандидата по време на престоя;
- главна цел на пътуването и продължителност на планирания престой;
- предполагаема дата на пристигане и заминаване;
- предполагаема граница при първо влизане или маршрут на транзитното преминаване;
- пребиваване;
- настоящо занимание и име на работодателя; за учащи: име на учебното заведение;
- за непълнолетни лица: име и фамилия на бащата и майката на кандидата.

Информационна система ЕВРОДАК (EURODAC)

Информационната система ЕВРОДАК представлява компютърна система, която управлява централна база данни за дактилоскопични отпечатыци с електронни средства за предаване на информация между държавите-членки на Европейския съюз и централната информационна система.

Основната цел на системата е да спомага за определянето на компетентната държава членка за разглеждането на подадена молба за предоставяне на международна закрила съгласно действащия Регламент (ЕС) № 604/2013 (Дъблин III), както и да се намалят т.нар. „вторични движения“ – случаи, в които гражданин на трета страна или лице без гражданство подава няколко молби за предоставяне на закрила в различни държави-членки на ЕС.

Системата функционира в съответствие с разпоредбите на действащия към момента *Регламент 603/2013 на Европейския парламент и на Съвета (Регламент ЕВРОДАК)*.

На територията на Република България системата се администрира от Националния институт по криминалистика (НИК) към МВР, а компетентните органи, които въвеждат информация в нея са Държавната агенция за бежанците при Министерския съвет и органите на МВР: НИК, Дирекция „Миграция“ и Главна дирекция „Гранична полиция“ и др.

Администратор на системата на национално ниво е Министърът на вътрешните работи.

С данните в ЕВРОДАК могат да се извършват и сравнения от правоприлагащите органи

на държавите членки и ЕВРОПОЛ за целите на правоприлагането и противодействието на организирани престъпни мрежи от трети държави, които опитват да се възползват от системата за убежище, за да въведат членове на дадена мрежа в държава – членка на ЕС, като контакт за своята престъпна дейност.

В ЕВРОДАК се обработват чувствителни лични данни, вкл. дактилоскопични отпечатаци на граждани на трети страни и лица без гражданство основно по три критерия – дали лицето е подало молба за предоставяне на международна закрила, дали лицето е задържано на граничен пункт на държава членка или е задържан във вътрешността на страната.

В зависимост от това в коя от трите категории попада чужденецът, дактилоскопните данни се съхраняват за различен период от време като към тях следва да бъде добавена и допълнителна информация – имена, пол, дата на раждане, гражданство, дата, час и място на дактилоскопиране, дата на подадена молба за предоставяне на международна закрила, дата на напускане на ЕС.

Агенция на ЕС за сътрудничество в областта на правоприлагането ЕВРОПОЛ (EUROPOL)

Европейската полицейска служба (Европол) е създадена като междуправителствен орган със седалище в Хага (Нидерландия), в съответствие с разпоредбите на действащия към момента *Регламент (ЕС) 2016/794 относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол)*.

Ролята на Европол е да подкрепя дейността на националните правоприлагащи служби и взаимното им сътрудничество за предотвратяване на тежката престъпност и тероризма, както и борба с тях. Европол способства за обмена на информация между правоприлагащите органи на държавите членки и предоставя криминален анализ с цел подпомагане на националните полицейски органи в извършването на трансгранични разследвания. Съгласно настоящите разпоредби на европейското законодателство в областта на миграцията, правоприлагането и движението на лица в ЕС, ЕВРОПОЛ има достъп до всички широкомащабни информационни системи на ЕС.

Национално звено Европол на територията на страната е в Дирекция „Международно оперативно сътрудничество“ към МВР (ДМОС), изпълняваща ангажиментите на Република България за организиране и координиране на международния обмен на оперативна информация.

Администратор на системата на национално ниво е Министърът на вътрешните работи.

В ЕВРОПОЛ се обработват лични данни свързани с дейностите по защита на националната сигурност, противодействие на престъпността, опазване на обществения ред и провеждане на наказателното производство, като имена и всякакви псевдоними и приети имена; дата и място на раждане; гражданство; пол; местопребиваване; номер на социално пребиваване и др.

Съгласно действащото законодателство Европол има достъп до данните, обработвани във всички широкомащабни информационни системи на ЕС с оглед изпълнение на задачите от компететите на службата.

Митническа информационна система (CIS)

Митническата информационна система („МИС“ или “CIS”) е централизирана платформа, която е създадена с цел предотвратяване, разследване и преследване на нарушения на законодателството в сферата митниците и земеделието.

Системата функционира в съответствие с действащия към момента *Регламент за изпълнение (ЕС) 2021/414 на Комисията от 8 март 2021 г.* МИС и FIDE се регулират от Регламент (ЕО) № 515/97 на Съвета, последно изменен с Регламент (ЕС) № 2015/1525, и Решение 2009/917/ ПВР на Съвета („Правната рамка на МИС”).

МИС на територията на Република България се администрира от Агенция „Митници“. Централизирана база данни на системата е достъпна чрез терминали във всяка държава-членка на ЕС.

Администратор на системата на национално ниво е Агенция „Митници“.

Данните, въведени в МИС, се отнасят за стоки, транспортни средства, предприятия и хора, свързани с такива нарушения. Личните данни които се обработват в МИС са: име, фамилно име, моминско име, псевдоними, дата и място на раждане, гражданство, пол и други.

Базата данни за идентификация на митническите файлове (Fichier d'Identification des Dossiers d'Enquêtes Douanières („FIDE“) се състои от протоколи за разследване, генерирани от митническите и други разследващи органи на държавите-членки на ЕС за административни цели и за целите на наказателни разследвания.

Система за влизане/излизане (EES)

С Регламент (ЕС) № 2017/2226 на Европейския парламент и на Съвета от 30 ноември 2017 г. е създадена системата за влизане/излизане с цел регистриране на данните относно влизането и излизането и данните относно отказа за влизане на граждани на трети страни, преминаващи външните граници на държавите членки.

Компетентният орган на територията на Република България, който отговаря за системата е Дирекция „Международно оперативно сътрудничество“ към МВР, като е предвидено експлоатацията на системата в цялост да започне от м. септември 2022 г.

Администратор на системата на национално ниво е Министърът на вътрешните работи.

Чрез записването, съхранението на данни в СВИ и осигуряването на държавите членки на достъп до тях, целите на системата са:

- да подобрява ефективността на граничните проверки, като изчислява и следи за продължителността на разрешения престой при влизането и излизането на граждани на трети страни, допуснати за краткосрочен престой;
- да спомага за установяването на самоличността на граждани на трети страни, които не отговарят или вече не отговарят на условията за влизане или за краткосрочен престой на територията на държавите членки;
- да дава възможност за установяване на самоличността и откриване на лицата, надвишили разрешения срок на престой, както и възможност на компетентните национални органи на държавите членки да предприемат подходящи мерки;
- да дава възможност за извършване на електронни проверки в СВИ за откази за влизане;
- да дава възможност за автоматизация на граничните проверки на граждани на трети страни;
- да дава на визовите органи възможност за достъп до информация относно законното използване на предишни визи;
- да информира гражданите на трети страни за срока на техния разрешен престой;
- да събира статистически данни за влизането и излизането, отказите за влизане и случаите на надвишаване на разрешения срок на престой на граждани на трети страни с цел подобряване на оценката на риска от надвишаване на разрешения срок на престой и подпомагане на разработването на основана на факти миграционна политика на Съюза;
- да води борба с измамите, свързани със самоличността, и със злоупотребата с документи за пътуване.

Личните данни, които се обработват в системата са:

- фамилно име, собствено(и) име(имена), дата на раждане, гражданство на една или повече държави, пол;
- вид и номер на документа или документите за пътуване и трибуквен код на държавата, издала документа или документите за пътуване;
- датата, на която изтича срокът на валидност на документа или документите за пътуване;
- портретна снимка;
- датата и часът на влизане;
- граничният контролно-пропускателен пункт на влизане и органът, който е разрешил влизането;
- ако е приложимо, статутът на гражданина на трета страна, който показва, че той или тя е гражданин на трета страна;
- датата и часът на излизане;
- граничният контролно-пропускателен пункт на излизане.

Европейска система за информация за пътуванията и разрешаването им (ETIAS)

С Регламент (ЕС) 2018/1240 на Европейския парламент и на Съвета от 12 септември 2018 г. се създава Европейска система за информация за пътуванията и разрешаването им (ETIAS) по отношение на граждани на трети държави, освободени от изискването за притежаване на виза при преминаване на външните граници, която позволява да се прецени дали присъствието на тези граждани на трети държави на територията на ЕС би представлявало риск за сигурността, риск от незаконна имиграция или висок епидемичен риск. За тази цел се въвеждат разрешение за пътуване, както и условия и процедури за неговото издаване или отказ.

Компетентният орган на територията на Република България, който отговаря за системата е Дирекция „Международно оперативно сътрудничество“ към МВР, като е предвидено експлоатацията на системата в цялост да започне от месец май 2023 г.

Администратор на системата на национално ниво е Министърът на вътрешните работи.

Информационната система на ETIAS се състои от национален единен интерфейс (NUI) във всяка държава членка, основан на общи технически спецификации, позволяващ свързването по сигурен начин на централната система на ETIAS с националните гранични инфраструктури и с централни звена за достъп в държавите членки.

Личните данни, съхранявани в централната система на ETIAS, не се предават и не се предоставят на трети държави, международни организации или частноправни субекти с изключение на предаването на данни на Интерпол за целите на осъществяването на автоматизираното обработване.

Европейска система за информация за присъди срещу граждани на трети държави и лица без гражданство (ECRIS-TCN)

С Регламент (ЕС) 2019/816 на Европейския парламент и на Съвета от 17 април 2019 г. се създава централизирана система за установяване на държавите членки, разполагащи с информация за присъди срещу граждани на трети държави и лица без гражданство (ECRIS-TCN), с цел допълване на Европейската информационна система за съдимост.

Компетентният орган на територията на Република България е Централното бюро за съдимост към Министерство на правосъдието, който администрира националното централно звено за достъп на ECRIS-TCN.

Администратор на системата на национално ниво е Министерството на правосъдието.

За всеки осъден гражданин на трета държава централният орган на осъждащата държава членка създава в централната система запис на данни. Записът на данни съдържа:

- фамилно име, собствени имена, псевдоними или други използвани имена;
- дата на раждане;
- място на раждане (град и държава);
- гражданство на една или повече държави;
- пол;
- идентификационен номер или вид и номер на документите за самоличност на лицето, както и името на издаващия орган;
- данни за пръстовите отпечатъци, които са били взети в съответствие с националното право в хода на наказателно производство.

Агенция на ЕС за сътрудничество в областта на наказателното правосъдие (EUROJUST)

Агенцията на ЕС за сътрудничество в областта на наказателното правосъдие (Евроюст) функционира на база на действащия *Регламент 2018/1727* от 12 декември 2019 година.

Администратор на системата на национално ниво е Прокуратурата на Република България.

Доколкото е необходимо за изпълнението на задачите ѝ, в рамките на своята компетентност и с цел изпълнение на оперативните ѝ функции, Евроюст може да обработва чрез автоматизирани средства или в структурирани, ръчно обработвани файлове лични данни с оперативно значение на лица, по отношение на които съществуват сериозни основания да се счита, че са извършили или ще извършат престъпление от компетентността ѝ или са осъдени за подобно престъпление.

В Евроюст се обработват следните лични данни:

- фамилия, фамилно име по рождение, име(на) и всички псевдоними или приети имена;
- дата и място на раждане;
- гражданство;
- пол;
- местоживееене, професия и местонахождение на съответното лице;
- номер на социално осигуряване или други официални номера, използвани в държавите членки за установяване на самоличността на лицата, свидетелства за правоуправление на моторно превозно средство, документи за самоличност, паспортни данни, идентификационни номера за митнически и данъчни цели;
- информация, която се отнася до юридически лица, ако включва информация за определени или определяеми лица, които са обект на съдебно разследване или наказателно преследване;
- данни за сметки в банки или в други финансови институции;
- описание и вид на предполагаемите престъпления, дата на извършване, наказателноправна квалификация на престъпленията и етап на разследването;
- фактите, указващи разширяване на обхвата на случая на международно равнище;
- сведения във връзка с предполагаемо членство в престъпна организация;
- телефонни номера, адреси на електронна поща, данни за трафика и данни за местоположението, както и всякакви свързани данни, необходими за идентифициране на абоната или ползвателя;
- данни за регистрацията на превозни средства;
- ДНК профили, изготвени от некодиращата част на ДНК, фотоснимки и пръстови отпечатъци.

КЗЛД ИЗДАДЕ ИНФОРМАЦИОННА БРОШУРА „ПРАВАТА НА ДЕЦАТА И МЛАДИТЕ ХОРА ПРИ РАБОТА В ДИГИТАЛНИ ПЛАТФОРМИ. ЗАЩИТА И УКРЕПВАНЕ НА ПРАВАТА НА ДЕЦАТА И МЛАДИТЕ ХОРА”

Анализът на съвременните заплахи и предизвикателства пред защитата на личните данни е елемент на реализирането на политиките за публичност и повишаване на обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработване на лични данни.

Особено значима част от практиката на КЗЛД е поетапната и систематична информационно-разяснителна дейност, специално насочена към деца и млади хора, която да положи началото на трайна тенденция за изграждане на знание и култура у тях относно важността на неприкосновеността на личния живот и защитата на личните данни.

Изпълнение на приоритетна цел за 2021 г. бе извършването на анализ на темата за правата на децата и младите хора при работа в дигитални платформи. Целта на анализа бе да предостави задълбочено основните принципни положения при обработването на лични данни на деца и защита на техните права при работа в дигитални платформи. Приложимостта на общите норми за защитата на личните данни (Регламент (ЕС) 2016/679 като *lex generalis*) се отчита в контекста на Конвенцията за правата на детето (като *lex specialis*). Анализът обхваща въпроси, насочени към всички заинтересовани страни: създателите на различни дигитални платформи, предоставящи услуги в дигитална среда за деца и млади хора; децата като субекти на данни и техните родители. За постигане на всеобхватност на анализа е отчетена не само практиката на сродни органи по защита на данните, но и на международни организации, в чиято дейност попада защитата на децата и техните права.

В края на март 2022 г. КЗЛД издаде информационно-образователна брошура, озаглавена „Правата на децата и младите хора при работа в дигитални платформи. Защита и укрепване на правата на децата и младите хора.“

Брошурата е публикувана и на институционалния сайт на КЗЛД – [ТУК](#).

В настоящия брой на бюлетина публикуваме текстът на брошурата:

Децата и младите хора, като субекти на данни, са „уязвима” категория лица в сравнение с останалите физически лица и поради тази причина се нуждаят от специална защита на техните права. Тъй като децата и младите хора днес все повече живеят живота си в дигитална среда, от изключителна важност е техните свободи и права да бъдат защитени там, така както във физическия свят. Настоящият информационен материал има за цел да подпомогне практическото прилагане на изискванията за защита на личните данни в контекста на безопасността на децата и борбата с потенциална злоупотреба при обработване на личните им данни в онлайн среда. Същият няма задължителен характер и не претендира за изчерпателност.

Като отчита приложимите международноправни документи за закрила на децата, с настоящата брошура Комисията за защита на личните данни обобщава международния опит и практика при обработването на лични данни на деца и защита на техните права при работа в дигитални платформи. Обобщените принципи и стандарти, изброени по-долу, се отнасят както до самите деца, като субекти на данни, така и до техните родители и другите участници в дигиталния свят и икономика (напр. доставчиците на онлайн услуги).

ПРИНЦИПИ

1. Най-добрият интерес на детето – всички действия, отнасящи се до деца в дигитална среда, следва да се подчиняват на принципа за най-добрия (най-висшия) интерес на детето, тъй като той е от първостепенно значение.

2. Способностите на децата за постепенно развитие – различните деца достигат различни нива на зрялост на различна възраст. За да се оцени нивото на зрялост на детето, трябва да бъдат взети предвид неговата възраст и способност за развитие (психическо, физическо и емоционално).

3. Забрана за дискриминация – децата трябва да се ползват от всички свои права без дискриминация по какъвто и да било признак.

4. Минимален стандарт за защита – доставчиците на онлайн услуги следва да осигурят и приложат минимално ниво на защита за всички свои потребители, освен ако не предприемат подход, основан на риска, за да проверят възрастта на своите потребители, така че всички принципи и стандарти да се прилагат и за всички операции по обработване на лични данни на деца.

5. Достъп до цифровата среда – частните и публичните заинтересовани страни трябва да действат отговорно и да осигурят необходимите безопасни и сигурни цифрови системи за защита на личната неприкосновеност. Разработчиците и потребителите на цифрови инструменти и услуги трябва да се придържат към действащите правила за защита на децата и младите хора.

Достъпът и използването на цифровата среда са важни за реализирането на правата и основните свободи на децата, за тяхното включване, образование, участие и за поддържане на семейните и социалните взаимоотношения. Ако децата нямат достъп до цифровата среда или когато този достъп е ограничен в резултат на лоша свързаност, способността им да упражняват в пълен обем своите човешки права може да бъде засегната.

6. Свобода на изразяване и информация – предоставянето на информация за правата на детето е особено важно. Каквито и да било ограничения на правото на децата на свобода на изразяване и информация в цифровата среда следва да бъдат в съответствие с международните и европейските конвенции по правата на човека и произтичащите от тях стандарти.

7. Ясно очертани граници на съгласието за обработване на данни – когато детето се съгласява с обработването на неговите данни, това съгласие трябва да бъде дадено свободно, конкретно, информирано и недвусмислено, чрез ясно изявление или утвърдително действие (*чл. 4, т.11 и чл. 7 от Регламент (ЕС) 2016/679*). За да бъде валидно съгласието, дадено от дете във връзка с пряко насочени към него услуги на информационното общество (напр. социални медии, блогове, интернет форуми, платформи за споделяне на видео, програми за чат, онлайн игри, приложения с игри или друго съдържание), то трябва да е навършило 14 години. За децата под тази възраст съгласието се предоставя от родителя/настойника (*чл. 25в от ЗЗЛД, чл. 8 от Регламент (ЕС) 2016/679*). Достатъчно е съгласието само на един от носителите на родителски права – съгласието на другия родител се предполага. Превантивните или консултантските услуги, предлагани директно на деца, са освободени от изискването за съгласие на родителите, тъй като децата трябва да могат да търсят съвет или подкрепа, без родителите им да знаят и това е в най-добрия интерес на детето.

8. Нулева намеса – ако даден доставчик на услуги в дигитална среда, разчита на легитимни интереси като законово основание за обработката на лични данни на деца, той трябва да гарантира, че тези законни интереси не пречат, не противоречат или не влияят неблагоприятно на нито един етап от обработването, спазвайки принципа за най-добрия интерес на детето.

9. Познаване на своята аудитория – доставчиците на онлайн услуги трябва да предприемат стъпки, за да идентифицират своите потребители и да гарантират, че услугите, насочени към, предназначени или които е вероятно да бъдат достъпни от деца, прилагат ефективно на практика специфични мерки за защита на данните, конкретно насочени за деца.

10. Предоставяне на информация във всички случаи – децата имат право да получават информация относно обработката на техните лични данни (*информацията, която администраторът дължи на децата, е посочена в чл. 13 и чл. 14 от Регламент (ЕС) 2016/679*), независимо от правното основание, на което се основава обработването. Такъв е дори случаят, когато родител е дал съгласието си от името на своето дете за обработка на неговите лични данни. Информацията трябва да бъде предоставена както при събиране на личните данни, така и по искане на субекта на данните (*чл. 12 – чл. 15 от Регламент (ЕС) 2016/679*).

11. Прозрачност, ориентирана към децата – информацията за това как администраторите използват личните данни трябва да бъде предоставена по кратък, прозрачен, разбираем и достъпен начин, като се използва ясен и прост език, който е лесен за разбиране и подходящ за възрастта на детето (чл. 12 – 14 от Регламент (ЕС) 2016/679).

12. Да оставим децата да кажат своето мнение – правото на всяко дете да бъде чуто и да се изкаже свободно по всички въпроси, които го засягат, трябва да бъде гарантирано. На изказаното от него мнение следва да се отдаде дължимото уважение, като във всички случаи се отчитат неговата възраст и зрялост.

13. Съгласието не променя детството – само защото даден администратор (доставчик на дигитални услуги) разполага с валидно съгласие от дете или от негов родител/настойник за обработване на личните му данни, не означава, че той може да се отнася към детето като към възрастен. Този администратор е длъжен да осигурява специфичната защита, която децата заслужават съгласно Регламент (ЕС) 2016/679 (*съображение 38 от Регламент (ЕС) 2016/679*).

14. Вашата платформа, Вашата отговорност – когато компания извършва проверка/верификация на възрастта и/или разчита на родителско съгласие за обработка на данните на дете, от нея се очаква да положи допълнителни усилия, за да докаже, че мерките ѝ за проверка на *възрастта* и на *родителското съгласие* са ефективни (чл. 5, пар. 2 от Регламент (ЕС) 2016/679).

15. „Не изключвайте“ децата – потребители и не подценявайте/не занижавайте техния опит – този стандарт, насочен към доставчиците на онлайн услуги, указва, че ако дадена услуга е насочена към, предназначена или има вероятност да бъде достъпена от деца, тези доставчици не могат да заобиколят задълженията си в областта на защитата на личните данни просто като изключат децата от кръга на потребителите или ги лишат от богатството на изживяването на услугата.

16. Минимално допустимата възраст на потребителите не е извинение – доставчиците на услуги онлайн не могат да се освободят от отговорностите си на администратор на лични данни по отношение потребителите – деца, като просто заявят, че деца под определена възраст не са добре дошли в съответната платформа/услуга или че не носят отговорност, ако деца я достъпят. Ако съответната услуга не е предназначена за деца под определена възраст, администраторите трябва да предприемат стъпки, за да гарантират, че механизмите им за проверка на възрастта са ефективни за предотвратяване на достъп на деца под въпросната възраст.

Методите за възрастова проверка следва да бъдат съобразени и пропорционални на идентифицираните от достъпа до услугата/обработването на данните рискове за правата и свободите на детето (*напр. доставчиците на платформи за споделяне на видео са задължени да предприемат подходящи мерки, за да гарантират, че дете няма да достъпи съдържание, което е вредно за него и/или е забранено по закон, напр. реалистично изображение на насилие, незаконни заплахи, подбуждане към бунт, агитация срещу етническа или национална група и детска порнография*). Удостоверяването на допустимата възраст трябва да става при стриктно спазване на принципа „свеждане на данните до минимум“. Не събирайте данни с цел проверка на възрастта във всички случаи, а само когато това е необходимо – с оглед естеството на услугата и идентифицираните рискове за децата!

Целта на изискването за верифициране на възрастта на потребителя е да се установи, че той е над 18 години, а не да се установи точната възраст на дете. Ако не е възможно верифицирането на

възрастта, доставчиците трябва да гарантират, че са въведени подходящи мерки за защита на данните, за да бъдат защитени децата като категория потребители, както под, така и над официалния възрастов праг на потребителите. В определени случаи е удачно администраторът да предоставя две версии на своите услуги: една, предназначена за деца и друга – за възрастни.

17. Забрана за профилиране – по принцип профилирането е вредно за децата и затова то трябва да бъде изключено по подразбиране, освен ако не е от съществено значение и условие за предоставяне на услугата или има убедителна причина да бъде включено (напр. цел гарантиране на възрастта на потребителите-деца). И в този случай обаче следва да се преценяват рисковете за правата и свободите на децата, при отчитане на техния най-добър интерес.

18. Вградете защитата! – доставчиците на онлайн услуги, които редовно обработват лични данни на деца, трябва по проектиране и по подразбиране да имат постоянно високо ниво на защита на данните, което е „вградено” в техните услуги. Още при проектирането на ИТ системи и процедури е необходимо да се вземат предвид мерки като минимизирането на данните и други аспекти на защитата на неприкосновеността с цел ефективно прилагане на чл. 25 от Регламент (ЕС) 2016/679. Защитата на данните трябва да бъде навременно интегрирана и включена в работните методи на администратора.

19. Неприкосновеност и защита на личните данни – децата имат право на личен и семеен живот в дигиталната среда, което включва защита на личните им данни и зачитане на неприкосновеността на тяхната кореспонденция и лична комуникация. Съответните заинтересовани страни, по-специално тези, които обработват лични данни, но също и връстници на детето, родители или полагащи грижи, и възпитатели, следва да са запознати и да зачитат правото на детето на неприкосновеност и защита на данните.

- **Споделяне на лични данни с трети лица** – споделянето на лични данни с трети страни може да бъде разрешено в някои случаи, а в други не. Приложимите правила в конкретен случай зависят от целта, за която първоначално са били събрани данните.

- **Данни за геолокация** – това, което е в най-добрия интерес на детето, може да варира в зависимост от ситуацията, но като основно правило не трябва да се използват данни, уточняващи местоположението на децата и младите хора. Данните за геолокация (данни за местоположение) могат да дадат информация относно географското положение на мобилен телефон или таблет в даден момент. Те правят възможно формирането на заключения относно личния живот на тези, към които се отнасят данните, като навиците им, това къде живеят, местата, които посещават, техните движения, дейности и социални взаимоотношения. Затова данните за местоположението се считат за много чувствителни по отношение на неприкосновеността на личността. Като цяло, рисковете от нарушаване на тази неприкосновеност се увеличават с количеството достъпни данни и степента на тяхната прецизност, тъй като позволяват по-подробно картографиране на съответното засегнато лице, за което се отнасят.

20. Защита на децата от вредно медийно влияние – УНИЦЕФ разглежда рисковете онлайн (т.нар. дигитални опасности), като ги класифицира в три категории: съдържание, контакт, поведение.

- *Рискове по отношение на съдържанието*: когато детето е изложено на неподходящо съдържание; такова съдържание включва сексуални, порнографски изображения или такива с насилие; някои форми на реклама; материали с расистко, дискриминационно съдържание или съдържание с езика на омразата (hate speech); интернет сайтове, които проповядват нездравословно или опасно поведение, като самонараняване, самоубийство или различни хранителни разстройства (анорексия, булимия и др.);

- *Рискове, свързани с контакт*: когато детето участва в рискова комуникация (напр. с възрастен, който търси неподходящ контакт с детето или за използването му за сексуални цели, или при контакт с възрастни, които се опитват да радикализират детето или да го убедят да участва в нездравословно или опасно поведение);

– *Рискове на поведението*: когато поведението на детето способства за възникване на някой от другите рискове – рисково съдържание или рисков контакт (напр. детето пише или създава материали за други деца, като използва език на омразата, като подбужда към расизъм, публикува или разпространява образи със сексуално съдържание, вкл. на материали, които децата сами са създали).

- **Мерки за защита на децата от вредно медийно влияние** – в законодателството и саморегулирането. Подходящи инструменти за защита на децата от вредно медийно влияние са и кодексите за поведение, използвани например за борба с омразата в интернет, както и доброволни споразумения със заинтересованите страни от бизнеса, като етични правила относно необходимостта от специално внимание в маркетинговите комуникации, насочени към деца и млади хора.

- **Различни нива на зрялост** – когато се решава кое съдържание е вредно, се взема предвид емоционалната и интелектуална зрялост на децата, която се развива непрекъснато.

- **По-уязвими от другите** – някои деца са изложени на по-голям риск от засягане от вредно медийно влияние. Деца с невропсихични увреждания обикновено използват медиите по-често от средното.

- **„Рискът от излагане на децата също е фактор, който трябва да се има предвид при създаването на дигитална среда, в която има деца.”** – децата с интелектуални затруднения също съобщават в по-голяма степен, че някой е бил злобен с тях в интернет.

- **Право на изтриване, вкл. във връзка с борбата със заплахите и омразата** – изтриването трябва да бъде извършено незабавно, ако детето го поиска и е навършило възрастта, необходима за контрол на собствените данни, дори ако първоначално съгласието е било предоставено от неговия родител/настойник.

- **Онлайн инструменти** – всички механизми, използвани за подпомагане на лицата да упражняват лесно правата си, когато са активни онлайн. Децата и младите хора имат свои собствени права, които се считат за достойни за специална защита.

- **Побутване (nudging)** – цифровото побутване е термин, който често се използва, за да опише как уебсайтът може да насочва избора на потребителите чрез „дизайна на изживяването”. Технологиите за проектиране като такава обикновено не е проблем, проблемът е как се използва тя. Побутването може да се използва по начини, които са напълно съвместими с принципите за защита на данните и с правата на децата и младите хора, когато се използва за насочване на потребителите към алтернативата, която им осигурява най-силна защита на неприкосновеността.

- **(Интернет) Свързани играчки** – на потребителите трябва да бъде предоставена ясна информация, че продуктът обработва лични данни (напр. глас, физическа активност и др.), преди закупуването на продукта, респ. преди инсталирането му. Това може да се направи както върху опаковката на физическия продукт, така и в инструкциите за употреба, например с помощта на икона, показваща, че продуктът е свързан с интернет и обработва личните данни на потребителя. Потенциалните купувачи трябва да могат да четат политиката за поверителност на продукта, условията за използване и друга подходяща и адаптирана информация онлайн, без първо да се налага да купуват. Когато става въпрос за играчки за деца, още по-важно е информацията да е проста и ясна.

21. Изводи и препоръки:

21.1. Към разработчиците и доставчиците на цифрови услуги с цел осигуряване на безопасна и полезна цифрова среда за децата:

- Изследванията в дигитална среда да се предприемат отговорно в съответствие с принципите за защита на данните, които включват защита на неприкосновеността на децата, минимизиране на данните и ограничаване на целта;

- Да прилагат, като принцип за защита на етапа на проектирането, подход за безопасност на децата при проектирането или при предоставянето на съответните дигитални услуги;

– Да създадат гаранции и да вземат предпазни мерки по отношение на неприкосновеността на децата, защитата на техните данните и търговското използване на тези данни; и

– Да демонстрират и доказват отчетност. Тежестта на доказване винаги се носи от администратора на лични данни (*чл. 5, пар. 2 от Регламент (ЕС) 2016/679*).

21.2. Към родителите:

– Да се насърчават децата да упражняват правата си – децата могат да упражняват собствените си права в областта на защитата на личните данни директно, при условие че това може да се разглежда като „рутинно действие” и особено, ако е в най-добрия интерес на детето. Поради това децата трябва да могат да упражняват собствените си права в тази област по отношение на социални мрежи, игри и платформи за споделяне на видео. Те трябва да разберат какви са механизмите и съответните процедури за подаване на жалби и средствата за защита, ако сметат, че правата им са нарушени. Информацията за това трябва да бъде адаптирана съобразно възрастта на децата (напр. прости диаграми, илюстрации, графики или движещи се картинки), в допълнение към писмената информация, за да стане тя по-интересна и достъпна. Способността на децата да действат автономно не отменя правото на родителите да упражняват същите права от името на своите деца и да предоставят подкрепа по време на целия процес.

– Да се насърчи упражняването на родителски контрол, който зачита неприкосновеността и най-добрия интерес на детето. Инструментите за родителски контрол се отнасят до различни цифрови решения, които дават на родителите или настойниците възможността да ограничат или контролират това, което децата и младите хора могат да правят онлайн (вкл. споделянето на лични данни). Тези инструменти са важни, тъй като могат да се използват за подкрепа на възрастните при защитата и насърчаването на най-добрия интерес на детето.

Въпреки че става въпрос за взаимоотношения в личната сфера и за семейни отношения е силно препоръчително родителският контрол да отговаря на правилата за защита на данните, и по-специално на:

- принципът на пропорционалност, като се вземат предвид интересите, възрастта и степента на зрялост на детето и избягване на използването на натрапчиви функции като постоянно проследяване;
- принципът на прозрачност спрямо детето чрез ясно обяснение кои родителски контроли се използват;
- принципът на сигурност на данните на детето, за да се гарантира, че трети страни нямат достъп до информация за детето (напр. данни за геолокация на детето).

Прилагането на инструменти за родителски контрол трябва да зачита изискването децата да не бъдат контролирани или подлагани на произволни или незаконни посегателства върху личния и семейния им живот.

– Информиране на детето – ако администраторът предлага инструменти за родителски контрол, трябва да се предостави на детето информация, подходяща за възрастта, за тези инструменти. Това може да стане чрез символи или икони, показващи на детето кога се извършва наблюдението.

СЪВЕТИ КЪМ АДМИНИСТРАТОРИ

За да обработва лични данни на деца администраторът трябва да разполага с правно основание за това, а самото обработване следва да се подчинява на принципите по чл. 5 от Регламент (ЕС) 2016/679. С цел осигуряване на специална защита на децата онлайн, Комисията за защита на личните данни отправя следните съвети и препоръки към администраторите – създатели на дигитални платформи и доставчици на дигитални услуги, които се ползват от деца:

1. При всички решения онлайн винаги трябва да се ръководите от най-висшия интерес на детето!

2. Избягвайте да се позовавате на своя легитимен интерес като основание за обработване на данни на деца! Може да прибегнете до това правно основание, само ако Вашият легитимен интерес съвпада с най-добрия интерес на детето!

3. Ако искате да използвате личните данни на деца и младежи за маркетингови цели (напр. банери, рекламни слотове на видео споделяне на платформи или игри), винаги трябва да отчитате съвпада ли Вашето правно основание с най-добрия интерес на детето. Детето трябва да може да разбере кое е реклама и кое не - рекламата не трябва да бъде проектирана под формата на игра и не трябва да бъде вградена в онлайн игри, така че детето да не може да различи рекламата от играта.

4. За да се позовете на съгласието на децата като основание за обработване на техни данни, трябва да сте сигурни, че то отговаря на изискванията за съгласие на деца (чл. 4, т. 11, чл. 7 и чл. 8 от Регламент (ЕС) 2016/679), като едновременно с това:

- искането за съгласие е ясно формулирано и отделно от други условия за ползване на услугата онлайн;

- не поставяте изискване към потребителите, че даването на съгласие за обработване на данните им е предпоставка/условие за получаване на услугата;

- разполагате с технически решения, които гарантират, че ако съгласието бъде оттеглено, личните данни могат да бъдат незабавно изтрети след оттеглянето му;

- осигурите отделно съгласие за всеки отделен случай на обработка на лични данни (обработване за различни цели).

5. Използвайте като изходна позиция за Вашите услуги (позиция по подразбиране) „повишена поверителност” или „висока неприкосновеност”:

- употребата на личните данни на деца трябва да е ограничена само до това, което е от съществено значение за предоставяне на основната услуга онлайн (напр. създаването на акаунт и използването на сайт за онлайн игри), като всички допълнителни функции (напр. геолокацията) трябва да са деактивирани по подразбиране;

- личните данни на децата могат да са видими или достъпни за други потребители на услугата, само ако детето промени настройките си, за да позволи видимост и достъпност.

6. Разработваният/предлаганият от Вас интерфейс трябва да бъде изграден на принципа на „активния положителен избор” (напр. отметка в квадратче). Мълчанието или бездействието на потребителя онлайн не представляват активен избор. Незаконно е използването на:

- предварително маркирани квадратчета (съгласие по подразбиране);

- технически решения, при които лицето трябва да маркира самò, че не дава съгласието си;

- технически решения от типа „ако не изберете опция, приемаме, че сте съгласни”;

- неясно или общо (за различни цели и услуги) съгласие.

7. Не използвайте подвеждащ и манипулативен дизайн! Настройките за поверителност трябва да се променят лесно, а някои опции, като геолокация, трябва да бъдат деактивирани по подразбиране.

8. Проектирайте и използвайте дизайн на дължимата за дигиталната услуга информация, който и най-малките по възраст потребители (при различни възрастови категории деца) могат да разберат. Децата трябва да могат да разберат за какво се съгласяват. Отговорността да докажете това е Ваша!

9. Предложете онлайн инструменти за изтегляне, изтриване, ограничаване или коригиране на лични данни или за подаване на жалба, за да се ориентират децата по-лесно как да упражняват своите права.

10. Ако обработването на лични данни на деца от Ваша страна е във връзка с пряко предлагане на услуги на информационното общество, то Вие задължително трябва да извършите оценка на въздействието върху защитата на данните, независимо от оценката на риска, която сте извършили преди това (чл. 35, пар. 4 от Регламент (ЕС) 2016/679; <https://www.cdpd.bg/?p=element&aid=1186>).

11. Правете периодичен преглед на предоставяните от Вас дигитални услуги и свързаната с тях оценка на въздействието върху защитата на данните, за да отчитате своевременно развитието на информационните технологии и практики!

12. Когато се проектират (интернет) свързани играчки е необходимо да се вземе предвид следното:

- да се направят лесни стандартните настройки за поверителност;
- да се избягва пасивното събиране на лични данни, а ясно да се посочва и показва кога устройството събира такива данни. Това може да стане под формата на „светване“, когато устройството записва изображения и звук или по друг начин събира лични данни;
- трябва да е лесно да се изключи режимът „събиране на данни“ от устройството, например чрез поставяне на бутон „офлайн“ директно върху устройството или чрез предоставяне на онлайн функции за това. Би трябвало да е възможно да се използват играчката или устройството във възможно най-голяма степен, без да се налага свързване с интернет;
- да се даде възможност за създаване на различни потребителски профили, които могат да бъдат адаптирани към възрастта на потребителя.

СЪВЕТИ КЪМ РОДИТЕЛИ

Предоставените по-долу съвети и препоръки към родителите имат за цел да ги подпомогнат в подкрепата, която трябва да оказват на децата си в дигиталната среда, при зачитане на неприкосновеността на личния живот и най-добрите интереси на детето:

1. Достъпът на Вашето дете до услуги онлайн е свързан с обработването на негови лични данни. Какви точно лични данни се събират и съхраняват от доставчиците на дигитални услуги зависи от естеството на предоставяната онлайн услуга и нейните цели. Важно е да знаете, че личните данни включват не само имена и адреси – това е цялата информация, която може да бъде свързана конкретно с Вашето дете, напр. ЕГН, електронен идентификатор, данни по личен документ, подпис, данни за местонахождение (геолокация) и др.

2. Вашето дете (субект на данни) има права в областта на защитата на личните данни, произтичащи от прякото приложение на Регламент (ЕС) 2016/679. В зависимост от своята възраст и степен на зрялост, то може да ги упражнява самостоятелно или чрез Вас.

3. Вслушайте се и вземете предвид изказаното от детето мнение (съобразно неговата възраст и зрялост) във връзка с обработването на личните му данни в онлайн среда! Правото на всяко дете да бъде чуто и да се изкаже свободно по всички въпроси, които го засягат, трябва да бъде гарантирано.

4. Доставчиците на онлайн услуги (администратори на лични данни) трябва да предоставят адаптирана информация за обработването на лични данни на децата и за техните права по начин, който отчита техните възрастовите различия и степен на зрялост. Помагайте на своите деца да осмислят и осъзнаят тази информация в пълнота, разяснявайте им по подходящ начин съответните законови ограничения (напр. филтриране на съдържание) и механизмите, които администраторите са предвидили за защита, включително как и до кого да подадат жалба, да докладват за злоупотреба или да поискат помощ и съвет!

5. Детето Ви може само да дава съгласие за обработването на негови лични данни при пряко достъпване на услуги на информационното общество, ако е навършило 14 год. възраст. За деца под

тази възраст, Вие сте тези, които трябва да изразите съгласие, ако съответната дигитална услуга се извършва въз основа на съгласие като правно основание по чл. 4, т. 11 от Регламент (ЕС) 2016/679. Дори в този случай Вашето дете има право да получи дължимата от администратора информация за обработването, независимо, че съгласието не се дава лично от него.

6. Доставчиците на онлайн услуги трябва да положат разумни усилия, като вземат предвид наличните технологии, за да проверят дали даденото съгласие от дете наистина е в съответствие със закона. Затова те могат да прилагат мерки за верификация на възрастта, които трябва да са ефективни, надеждни и пропорционални.

7. Вие не можете и не трябва да давате съгласие, ако обработването на данните на Вашето дете е за превантивни или консултантски услуги, предлагани директно на деца, вкл. онлайн. Целта на тези услуги е да защитят най-добрия интерес на детето – Вие не сте участник в този процес.

8. Повишавайте своята информираност относно дигиталните опасности и разяснявайте на децата си кои са рисковете в онлайн средата, особено в контекста на споделянето на лична информация и данни.

9. Ако купувате интернет свързани играчки, винаги се интересувайте по какъв начин те събират данни. Тези играчки се поддържат от функции, предоставени чрез цифрова връзка. Те могат да записват глас (напр. плюшено мече, с което детето говори и споделя информация), данни относно физическата активност (напр. лентите за активност, които регистрират информация относно тази активност и предават такива данни на сървъри, където се компилират, съхраняват и използват за показване като отчети за активността в приложение).

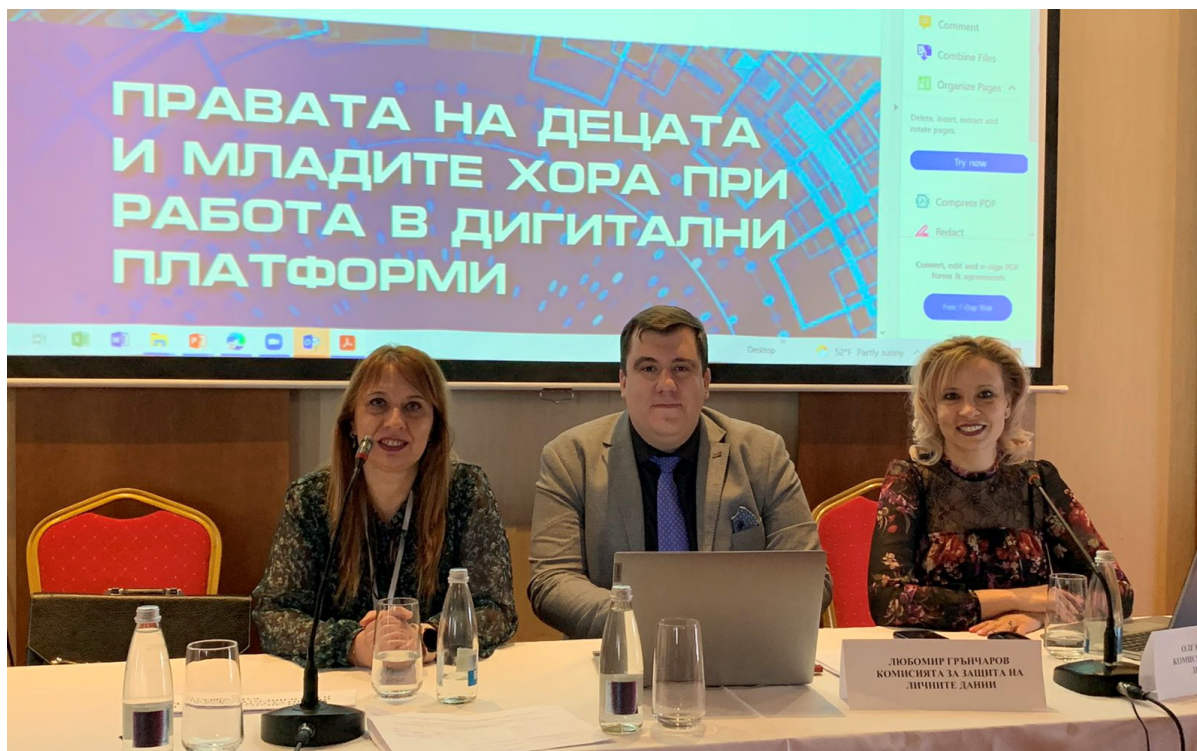
10. Насърчавайте детето си само да упражнява правата си в областта на защитата на личните данни, ако възрастта и зрелостта му позволява това (напр. по отношение на социални мрежи, игри и платформи за споделяне на видео). Това не отменя Вашето право да упражнявате същите права от негово име и да му предоставяте подкрепа, когато то само упражнява правата си.

11. При достъпа на Вашето дете до дигитални услуги, свързани с обработване на лични данни, упражнявайте родителски контрол по начин, който зачита неприкосновеността и най-добрите интереси на детето. Инструментите за родителски контрол могат да се използват, само ако детето е в състояние да разбере, че е наблюдавано, как и кога – зачитайте правото на личен живот на детето!

КЗЛД СЕ ВКЛЮЧВА АКТИВНО В ИНИЦИАТИВИ, СВЪРЗАНИ С ПРАВАТА НА ДЕЦАТА В ДИГИТАЛНА СРЕДА

През месеците март и април 2022 г., по покана на председателя на Държаван агенция за закрила на детето (ДАЗД) д-р Елеонора Лилова, представители на КЗЛД участваха в две мероприятия посветени на закрилата на децата – **семинар** на тема „Правата на децата в цифрова среда и практики по превенция на насилието” и **заседание** на Съвета на децата, който е консултативен орган към председателя на ДАЗД.

Състояният се в периода 21-23 март 2022 г. семинар на тема „**Правата на децата в цифрова среда и практики по превенция на насилието**“ бе организиран от ДАЗД и Регионално управление на образованието – София-град, с подкрепата на Министерство на образованието и науката. Семинарът бе посветен на повишаване на административния капацитет на професионалистите от образователните институции в сферата на защита на личността на децата в дигиталното пространство и действията им случаи на кибертормоз и атаки в интернет, както и запознаване с чуждестранни практики и обмяна на опит. Участие в работата на семинара взеха представители на Министерство на образованието и



науката, отдел Киберпрестъпност към Главна Дирекция „Борба с организираната престъпност“ - МВР, Комисията за защита на личните данни, УНИЦЕФ България, Национален център за безопасен интернет, Софийски университет „Св.Св. Климент Охридски“, Агенцията за защита на детето в киберпространството на Израел и др.

Представителите на КЗЛД - Любомир Грънчаров и Олга Александрова, експерти в дирекция „Правно-нормативна и международна дейност, взеха участие по темата „Деца и защитата на личните данни“. Те представиха новия информационно-разяснителен материал на КЗЛД (брошура), посветен на „Правата на децата и младите хора при работа в дигитални платформи“. Съдържанието на брошурата е публикувано в настоящия бюлетин, както на сайта на КЗЛД - [ТУК](#).

В периода 31.03-02.04.2022 г. представителите на КЗЛД Любомир Грънчаров и Олга Александрова взеха участие в **заседанието на Съвета на децата**, който е консултативен орган към председателя на ДАЗД и от 2003 г. работи в изпълнение на основните принципи на Конвенцията на ООН за правата на детето и Закона за закрила на детето, като основната му цел е да насърчи детското участие в процеса на изработване на политики за децата и вземане на решения. Представителите на КЗЛД обсъдиха с членовете на Съвета на децата какво всъщност са личните данни и колко важно е да бъдат предоставяни с повишено внимание. От своя страна децата поеха ангажимент да помогнат със съвети за изготвянето на информационни материали които да са на достъпен език за децата и по интересен начин да обясняват всичко за личните данните.

Участието на експерти на КЗЛД в тези мероприятия е принос към практиката за съвместна работа на различни държавни институции. Включването в инициативи, свързани с правата на децата, доброто патньосрство и общите усилия, са предпоставка за защита на българските деца от опасностите, които крие необятното виртуално пространство.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



European Data Protection Board



На състоялото се в средата на март 2022 г. заседание ЕКЗД прие в окончателен вариант **Насоки 02/2022 относно член 60 от ОРЗД**. Изготвянето на такива насоки е част от **стратегията и работната програма на ЕКЗД за периода 2021–2022 г.** за подпомагане на ефективното правоприлагане и ефикасното сътрудничество между националните надзорни органи. Насоките предоставят подробно описание на сътрудничеството

между надзорните органи по линия на ОРЗД и имат за цел допълнително да се подобри последователното прилагане на правните разпоредби, свързани с механизма за обслужване на едно гише. Насоките помагат на надзорните органи да тълкуват и прилагат своите национални процедури по такъв начин, че те да съответстват и да се вписват в сътрудничеството в рамките на механизма за обслужване на едно гише.

На същото заседание бяха приети **Насоки 03/2022 относно тъмните модели в интерфейсите на платформите на социалните медии**. Същите бяха обект на публична консултация до 2 май 2022 г. Насоките предлагат практически препоръки на проектантите и потребителите на платформи на социалните медии относно това, как да оценяват и избягват т.нар. „тъмни модели“ в интерфейсите на социалните медии, които нарушават изискванията на ОРЗД. Тъмните модели са интерфейси и услуги за потребителите, прилагани в платформите на социалните медии, които карат потребителите да вземат непредвидени, нежелателни и потенциално вредни решения относно обработването на личните им данни. Това оказва влияние върху поведението и способността на ползвателите да защитават ефективно своите лични данни. В насоките се дават конкретни примери за тъмни модели, представят се най-добри практики за различни случаи на употреба и се съдържат конкретни препоръки за проектантите на потребителски интерфейси, които улесняват ефективното прилагане на ОРЗД.

ЕКЗД прие **инструментариум относно основните гаранции за защита на данните при сътрудничеството между надзорните органи на ЕИП и трети държави**. Това допринася за едно от ключовите действия на **стратегията и работната програма на ЕКЗД за периода 2021–2022 г.** и има за цел да улесни взаимодействието между членовете на ЕКЗД и надзорните органи на трети държави. Инструментариумът може да се използва както за административни договорености, разработени в рамките на ЕКЗД от самите надзорни органи, така и за международни споразумения, договорени от Европейската комисия. Инструментариумът обхваща основни теми, като например приложимите права на субектите на данни, спазването на принципите за защита на данните и съдебната защита.

Европейският комитет по защита на данните прие съвместно становище с Европейския надзорен орган по защита на данните (ЕНОЗД) относно предложенията за удължаване на срока на действие на цифровия COVID сертификат.

На състоялото се през април 2022 г. заседание Комитетът прие изявление относно обявяването на нова трансатлантическа рамка за защита на личните данни. ЕКЗД приветства като първа положителна стъпка в правилната посока поетите от САЩ ангажименти за предприемане на „безпрецедентни“ мерки за защита на неприкосновеността на личния живот и личните данни на лицата в Европейското икономическо пространство (ЕИП) при предаването на техните данни на САЩ. В изявлението на ЕКЗД се отбелязва, че това съобщение не представлява правна рамка, въз основа на която износителите на данни от ЕИП могат да предават данни на САЩ. Те трябва да продължат да предприемат необходимите действия, за да се съобразят със съдебната практика на Съда на Европейския съюз, и по-специално с неговото решение Schrems II от 16 юли 2020 г. ЕКЗД заявява, че ще следи внимателно как това политическо споразумение се превръща в конкретни правни предложения. След като получи всички съпътстващи документи от Европейската комисия, Комитетът ще оцени подобренията, които новата

рамка може да донесе в светлината на правото на ЕС, съдебната практика на Съда на ЕС и предишните му (на Комитета) препоръки. По-специално, ЕКЗД ще анализира дали събирането на лични данни за целите на националната сигурност е ограничено до строго необходимото и пропорционалното. Освен това ще проучи как обявеният независим механизъм за правна защита защитава правото на лицата от ЕИП на ефективна правна защита и на справедлив съдебен процес. По-конкретно, ЕКЗД ще проучи дали всеки нов орган, част от този механизъм, има достъп до съответната информация, включително лични данни, когато упражнява своята мисия, и дали може да приема решения, обвързващи разузнавателните служби. Ще бъде разгледано дали съществува съдебна защита срещу решенията или бездействието на този орган. ЕКЗД заявява, че остава ангажиран да играе конструктивна роля в гарантиране на сигурността на трансатлантическо предаване на лични данни, което е от полза за лицата и организациите от ЕИП.

На същото заседание ЕКЗД прие писмо, в което изразява загриженост относно последните законодателни промени в Белгия, насочени към реформиране на закона за създаване на Белгийския надзорен орган, тъй като те могат да окажат отрицателно въздействие върху неговите стабилност и независимото функциониране. Комитетът подчертава, че независимият надзор, за който се опасява, че ще бъде засегнат от предложените реформи, е от съществено значение за основното право на защита на данните и по тази причина е защитен от Хартата и Договора за ЕС. Той също така е крайъгълен камък на ефективното прилагане на ОРЗД и на ефективното сътрудничество между надзорните органи.

В края на състоялото се през април заседание ЕКЗД реши да поиска статут на наблюдател в рамките на Пролетната конференция на европейските органи за защита на данните, която предоставя платформа за диалог на органите за защита на данните от цяла Европа, включително и от държави извън ЕИП. Това искане е част от Стратегията на Комитета за периода 2021-2023 г. за засилване на ангажираността с международната общност и за улесняване на сътрудничеството между членовете на Комитета и органите за защита на данните на трети държави.

ЕКЗД И ЕНОЗД ПРИЕХА ПЪРВО ЗА ТАЗИ ГОДИНА СЪВМЕСТНО СТАНОВИЩЕ

На 14 март 2022 г. ЕКЗД и ЕНОЗД приеха **съвместно становище относно предложенията на Европейската комисия за удължаване на срока на действащите регламенти за Цифровия COVID сертификат на ЕС** с 12 месеца и за изменение на определени разпоредби, като например разширяване на видовете тестове за COVID, които да се признават при пътуванията в рамките на ЕС, и поясняване, че сертификатите за ваксинация следва да съдържат броя на дозите, сложени на притежателя на сертификата, независимо от държавата членка, в която те са сложени. В своето становище ЕКЗД и ЕНОЗД посочват, че разбират необходимостта от удължаване на срока на прилагане на Регламента за Цифровия COVID сертификат на ЕС, тъй като не може да се предвиди дали пандемията ще продължи. В съответствие с **предходното съвместно становище относно първоначалните регламенти за COVID сертификата** се припомня, че спазването на правилата за защита на данните не представлява пречка за борбата с пандемията от COVID-19. Относно настоящото предложение ЕКЗД и ЕНОЗД отбелязват, че то не изменя съществено съществуващите разпоредби на регламентите, що се отнася до обработването на лични данни.



ЕКЗД и ЕНОЗД изразяват съжаление, че Европейската комисия не е извършила оценка на въздействието. Комисията следва да приложи към настоящото предложение доклад относно въздействието върху улесняването на свободното движение, основните права и недискриминацията. Регламентът за Цифровия COVID сертификат на ЕС предвижда задължение за Комисия да представи такъв доклад на Европейския парламент и на Съвета. Научните доказателства и въведените допълнителни мерки следва да бъдат редовно оценявани, за да се гарантира спазването на общите принципи на ефективност, необходимост и пропорционалност.

Според председателката на ЕКЗД Андреа Йелинек *„Тези предложения са от особено значение поради голямото им въздействие върху защитата на правата и свободите на лицата. Всяко ограничение на свободното движение на лицата в рамките на ЕС с цел ограничаване на разпространението на COVID-19, включително изискването за представяне на Цифрови COVID сертификати на ЕС, следва да бъде премахнато веднага щом епидемиологичната обстановка го позволи.“*

Според Европейския надзорен орган по защита на данните Войчех Виевиоровски *„Трябва непрекъснато да преценяваме кои мерки остават ефективни, необходими и пропорционални в борбата с пандемията от COVID-19. Принципите за защита на данните следва да се прилагат и интегрират постоянно, като се отчитат надлежно развитието на епидемиологичната обстановка и въздействието върху основните права.“*

В становището ЕКЗД и ЕНОЗД заявяват, че промяната на определени полета за данни изглежда ограничена до строго необходимото и не поражда особени опасения от гледна точка на защита на данните. Двата надзорни органа припомнят предишното си становище, според което всяка промяна в полетата за данни може да изисква повторна оценка на рисковете за основните права и че чрез приемането на делегирани актове следва да се добавят само по-подробни полета за данни, попадащи във вече определените категории данни. В съвместното становище ЕКЗД и ЕНОЗД заявяват, че ще продължат да обръщат специално внимание на развитието на пандемията от COVID-19, и по-специално на използването на личните данни след края на пандемията.

ЕВРОПЕЙСКАТА КОМИСИЯ ПРЕДЛОЖИ ПРАВИЛА ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА И ИНФОРМАЦИОННАТА СИГУРНОСТ В ИНСТИТУЦИИТЕ, ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА ЕС

На 22 март 2022 г. Европейската комисия предложи нови правила за установяване на общи мерки за киберсигурност и информационна сигурност в институциите, органите, службите и агенциите на ЕС: **„Предложение за Регламент за определяне на мерки за високо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза“** и **„Предложение за Регламент относно информационната сигурност в институциите, органите, службите и агенциите на Съюза“**

Целта на предложенията е да се укрепи устойчивостта и капацитета за реагиране срещу киберзаплахи и киберинциденти, както и да се гарантира устойчива и сигурна публична администрация на ЕС в условията на засилване на злонамерените действия в киберпространството в световен мащаб. Възприемането на съвместен подход към киберсигурността и информационната сигурност е крайно наложителен в контекста на пандемията от COVID-19 и нарастващите геополитически предизвикателства. Определянето на общи приоритети и рамки допълнително ще засили междуинституционалното сътрудничество и ще укрепи сигурността на ЕС.

Според комисаря по въпросите на бюджета и администрацията Йоханес Хан тези две предложения *„представяват крайъгълен камък в областта на киберсигурността и информационната сигурност“*

в ЕС. Те се основават на засилено сътрудничество и взаимна подкрепа между институциите, органите, службите и агенциите на ЕС, както и на координирана готовност и реакция.“

В прессъобщение Европейската комисия заявява:

„С предложения **Регламент относно киберсигурността** ще се въведе рамка за ръководство, управление и контрол на риска в областта на киберсигурността. Това ще доведе до създаването на нов междуинституционален съвет по киберсигурност, ще повиши капацитета в областта на киберсигурността и ще стимулира редовните оценки на зрелостта и по-добрата киберхигиена. Също така ще бъде разширен мандатът на екипа за незабавно реагиране при компютърни инциденти за институциите, органите, службите и агенциите на ЕС (CERT-EU) като център за обмен на разузнавателна информация за заплахи и координиране на реакцията при инциденти, централен консултативен орган и доставчик на услуги.

Основни елементи на предложението за регламент относно киберсигурността са:

- Укрепване на мандата на CERT-EU и предоставяне на ресурсите, необходими за неговото изпълнение.
- Изискване към институциите, органите, службите и агенциите на ЕС да:
 - разполагат с рамка за ръководство, управление и контрол на риска в областта на киберсигурността;
 - прилагат базов набор от мерки за киберсигурност, насочен към преодоляване на установените рискове;
 - извършват редовни оценки на зрелостта;
 - въведат план за подобряване на своята киберсигурност, одобрен от ръководството на субекта;
 - обменят със CERT-EU без ненужно забавяне информация относно инциденти.
- Създаване на нов междуинституционален съвет по киберсигурност, който да ръководи и наблюдава прилагането на регламента и да направлява CERT-EU.
- Преименуване на CERT-EU от „Екип за незабавно реагиране при компютърни инциденти“ на „Център за киберсигурност“ в съответствие с развитието в държавите членки и в световен мащаб, като при това краткото име „CERT-EU“ се запазва с цел по-лесно разпознаване.

Предложеният **Регламент относно информационната сигурност** ще създаде минимален набор от правила и стандарти за информационна сигурност за всички институции, органи, служби и агенции на ЕС, за да се гарантира засилена и последователна защита срещу променящите се заплахи за тяхната информация. Тези нови правила ще осигурят стабилна основа за сигурен обмен на информация между институциите, органите, службите и агенциите на ЕС и с държавите членки въз основа на стандартизирани практики и мерки за защита на информационните потоци.

Основни елементи на предложението за регламент относно информационната сигурност:

- Създаване на ефективно управление за насърчаване на сътрудничеството между всички институции, органи, служби и агенции на ЕС, а именно междуинституционална координационна група за информационна сигурност;
- Установяване на общ подход към категоризацията на информацията въз основа на нивото на поверителност;
- Модернизиране на политиките за информационна сигурност така, че да се включат изцяло цифровата трансформация и дистанционната работа;
- Рационализиране на настоящите практики и постигане на по-голяма съвместимост между съответните системи и устройства.“

Предложеният **Регламент относно киберсигурността** ще осигури съгласуваност с политиките на ЕС в областта на киберсигурността, в пълно съответствие с действащото европейско законодателство:

- Директивата относно сигурността на мрежите и информационните системи (Директивата за МИС) и бъдещата Директива относно мерки за високо общо ниво на киберсигурност в Съюза („МИС 2“), които Комисията предложи през декември 2020 г.;

- Акта за киберсигурността;
- Препоръката на Комисията за изграждането на съвместно киберзвено;
- Препоръката на Комисията относно координираната реакция при мащабни инциденти и кризи в областта на киберсигурността.

Предложеният **Регламент относно информационната сигурност** има за цел да повиши защитата на информацията чрез рационализиране на различните правни рамки на институциите, органите, службите и агенциите на Съюза в тази област. Предложението е в съответствие със:

- Стратегията на ЕС за Съюза на сигурност, която включва всеобхватен ангажимент на ЕС за допълване на усилията на държавите членки във всички области на сигурността;

- основната характеристика на Стратегическата програма за периода 2019-2024 г., приета от Европейския съвет през юни 2019 г. — да защитава нашите общества от непрекъснато променящите се заплахи, насочени към информацията, с която работят с институциите, органите и агенциите на ЕС;

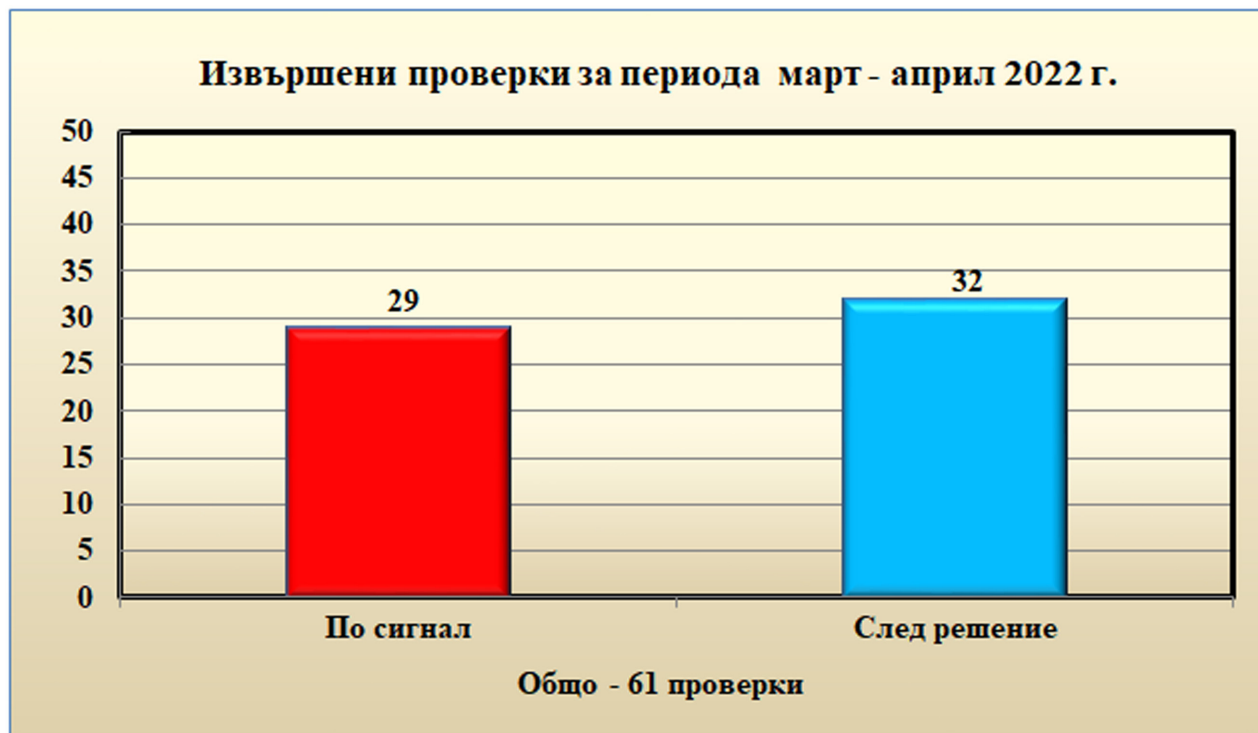
- Заключениеята от заседанието на Съвета по общи въпроси от декември 2019 г., в които институциите, органите и агенциите на ЕС се призовават да разработят и приложат с подкрепата на държавите членки всеобхватен набор от мерки за гарантиране на своята сигурност.



КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАРТ - АПРИЛ 2022 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците март и април 2022 г. са извършени общо 61 проверки – 29 след постъпили в КЗЛД сигнали и 32 след решение на КЗЛД.



Разгледани са 35 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 периода КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са издадени 16 Разпореждания и са отправени 3 Предупреждения и 4 Официални предупреждения.

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-01-324/2021 г. София, 07.04.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: Цанко Цолов, Мария Матева и Веселин Целков на заседание, проведено на 26.01.2022 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента, ОРЗД), разгледа по същество жалба № ППН-01-324/14.04.2021 г.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Комисията за защита на личните данни е сезирана с жалба, подадена от С.И., с изложени твърдения за неправомерно обработване – употреба и разпространение на личните му данни от С.Ш., чрез вписването им в адресирана до него поканата, поставена на „видно място“ – „на общото табло“.

Към жалба е приложено копие на поканата, същата с дата 12.04.2021 г., от С.Ш. - управител на етажната собственост, находяща се в *****, до С.И.

С оглед застъпените в административния процес принципи на равенство на страните и истинност, г-жа С.Ш. е информирана за образуването по случая административно производство, указана ѝ е възможността да ангажира писмено становище по изложените в жалбата твърдения и да представи относими по случая доказателства.

В отговор е депозиран отговор с рег. № ППН-01-324#5/17.09.2021 г., с приложени към него относими доказателства – заверено копие на процесната поканата и Информационни права на субектите на лични данни, без дата на изготвяне, приемане, влизане в сила.

Госпожа С.Ш. оспорва жалбата. Информира, че е управител на етажна собственост находяща се в ***** и допълва, че срещу месечно възнаграждение жалбоподателят изпълнява „на пълен работен ден функциите на портиер“ в етажната собственост (ЕС). Твърди, че взаимоотношенията между жалбоподателя и ЕС не са били регламентирани съгласно изискванията на Кодекса на труда, поради което на 12.04.2021 г., в присъствието на свидетели, е връчила на г-н С.И. процесната поканата за сключване на трудов договор за изпълняване на длъжността „портиер“. Допълва, че г-н С.И. е отказал да подпише, че е получил поканата, обстоятелство което е удостоверено с подписите на свидетелите В.И. и Й.П. Госпожа С.Ш. отрича да е разпространявала личните данни на жалбоподателя чрез поставяне на поканата на общото табло в хода на жилищната сграда или по друг начин, а твърденията на г-н С.И., в тази насока, квалифицира като клевета.

Комисията за защита на личните данни е независим държавен орган, който осъществява защита на лицата при обработването на личните им данни и при осъществяване на достъпа до тези данни, както и контрол по спазването на ЗЗЛД и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

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

Подадената от г-н С.И. жалба ППН-01-324/14.04.2021 г. съдържа задължително изискуемите реквизити: данни за жалбоподателя, естеството на искането, дата и подпис, посочена е пасивно легитимираната страна, с оглед което жалбата е редовна.

Жалбата е подадена от физическо лице с правен интерес срещу надлежна страна – физическо лице, администратор на лични данни – С.Ш., в качеството ѝ на домоуправител на етажна собственост. Сезиран е компетентен да се произнесе орган – КЗЛД, която съгласно правомощията си по чл. 10, ал. 1 от ЗЗЛД във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679, разглежда жалби подадени от субект на данни срещу актове и действия на администраторите на лични данни, с които се нарушават правата на физическите лица свързани с обработване на личните данни, като не е налице изключенията по чл. 2, § 2, буква „в“ и чл. 55, § 3 от Регламент (ЕС) 2016/679 предвид обстоятелството, че случая не касае дейности по обработване извършвани от физическо лице в хода на чисто лични или домашни занимания и/или дейности извършвани от съдилищата при изпълнение на съдебните им функции. Не са налице отрицателните предпоставки по чл. 27, ал. 2 от АПК.

По изложените съобщения на проведено на 17.11.2021 г. заседание на комисията жалбата е приета за допустима и като страни в производство са конституирани: жалбоподател – С.И. и ответна страна – С.Ш., в качеството ѝ на домоуправител на етажна собственост находяща се в *****. Насрочено е открито заседание за разглеждане на жалбата по същество на 26.01.2022 г. от 13:00 часа, за което страните са редовно уведомени и им е указано разпределянето на доказателствената тежест в процеса, като жалбоподателя е информиран, че следва, не по-късно от дата на заседанието, да ангажира доказателства в подкрепа на твърденията си, предвид обстоятелството, че същите са оспорени от ответната страна.

На проведено на 26.01.2022 г. открито заседание на КЗЛД, жалбата е разгледана по същество.

Жалбоподателят С.И. – редовно уведомен, се явява лично.

Ответната страна С.Ш. в качеството на домоуправител на етажна собственост, находяща се в ***** – редовно уведомена, се явява лично. Води и свидетел.

Страните отказват да сключат споразумение.

Жалбоподателят поддържа жалбата, не сочи нови доказателства, искания по доказателствата няма. Заявява, че поканата му е връчена, но той отказал да я приеме, в резултат на което е поставена на табло в входа на ЕС.

Ответната страна г-жа С.Ш. оспорва жалбата. Твърди, че поканата е връчена лично на жалбоподателя в присъствието на свидетели. Отрича да е поставяла поканата на таблото в входа на ЕС. Моли комисията да допусне до разпит свидетел, за установяване на съдържанието на приложена по преписката покана, в частта касаеща връчването ѝ на жалбоподателя. Уточнява, че свидетелят, който води, е присъствал лично при връчване на поканата и има непосредствени възприятия относно спорния по преписката въпрос, като с подписа си под поканата е удостоверил начина на връчването ѝ на г-н С.И.

Комисията оставя без уважение искането на ответницата за събиране на гласни доказателства, доколкото с тях се цели да се докаже съдържанието на частен свидетелстващ документ – покана, неоспорен от жалбоподателя.

Предвид събраните по преписката доказателства и направените от страните заявления, комисията намира случая за изяснен от фактическа страна. В ход по същество жалбоподателят поддържа жалбата. Моли комисията да я уважи и да санкционира действията на администратора. Ответникът поддържа становище за неоснователност на жалбата и моли комисията да я отхвърли.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в административното производство, съгласно чл. 7 от АПК, изискващ наличието на установени действителни факти и предвид събраните доказателства и наведените твърдения, комисията приема, че разгледана по същество жалба № ППН-01-324/14.04.2021 г. е неоснователна.

Предмет на жалбата са твърденията за неправомерно обработване – употреба на личните данни на жалбоподателя в обем от три имена, ЕГН и адрес, съдържащи се в адресирана до него поканата от С.Ш., и разпространението им до неограничен кръг от лица посредством поставяне на поканата на видно и общодостъпно място – на „общото табло“.

Страните не спорят, че жалбоподателят е изпълнявал функциите на портиер в етажната собственост, находяща се в *****, домоуправител на която е ответната страна - С.Ш., без отношенията между страните да са регламентирани съобразно Кодекса на труда. Не е спорно наличието на писмена поканата от г-жа С.Ш., в качеството ѝ на домоуправител, адресирана до жалбоподателя, за сключване на трудов договор между ЕС и г-н С.И. във връзка с изпълняваната от него длъжност. В поканата, видно от съдържанието ѝ, се съдържат три имена, ЕГН и адрес на жалбоподателя, като следва да се отбележи, че същата е от 12.04.2021 г. към която дата е безспорно, че жалбоподателят е изпълнявал длъжността на портиер в ЕС.

Събраните по преписката свидетелстват, че на 12.04.2021 г. поканата е връчена на г-н С.И., обстоятелство което е удостоверено с подписите на свидетелите В.И. и Й.П., присъствали при връчването ѝ, удостоверели че г-н С.И. е отказал да се подпише, че е получил екземпляр от поканата. Доказателства в обрана насока не са ангажирани, а доказателствената сила на документа не е оспорена от жалбоподателя.

Съдържащите се в поканата информация за жалбоподателя в обем от три имена, ЕГН и адрес имат качеството на лични данни, предвид обстоятелството, че посредством тях лицето може да бъде еднозначно индивидуализирано. В тази връзка е безспорно, че действията по употреба на личните данни на жалбоподателя за изготвяне на поканата и поставяне на поканата на общодостъпно място, следва да се квалифицират като обработване – употреба, респективно разпространение, на лични данни по смисъла на чл. 4, т. 2 от ОРЗД и като такива следва да отговарят на изискванията на ОРЗД и ЗЗЛД.

Употреба на лични данни на жалбоподателя за целите на изготвена до него поканата за оформяне в писмена форма на трудов договор между страните е законосъобразно. Същото се осъществява в хипотезата на чл. 6, § 1, буква „в“ от ОРЗД – обработването е необходимо за спазване на законово задължение спрямо администратора произтичащо от Кодекса на труда, предвид качеството му на работодател на г-н С.И. и трудовоправните отношения между тях с оглед изпълняваната от г-н С.И., срещу заплащане, длъжност на портиер в ЕС, представлявана от г-жа С.Ш. В тази връзка и предвид твърденията на жалбоподателя, че данните му са използвани за съставяне на поканата без негово съгласие, следва да се отбележи, че съгласието е само едно от основанията за законосъобразно обработване на лични данни разписани в чл. 6, § 1, букви от „а“ – „е“ от ОРЗД. Независимо от факта, че то е посочено на първо място, всички правни основания са алтернативни и равнопоставени и не са подредени в йерархична зависимост, като наличието на което и да е от тях прави обработването законосъобразно, при условие, че са спазени и другите изисквания на регламента.

По преписката липсват доказателства за твърдяното от жалбоподателя разпространение на личните му данни до неограничен кръг от лица, чрез поставяне на поканата на видно и общодостъпно място – на „общото табло“ от г-жа С.Ш. Същите са оспорени от ответната страна, а въпреки дадените

на жалбоподателя конкретни указания за разпределяне на доказателствената тежест в процеса, г-н С.И. не ангажира доказателства в подкрепа на твърденията си. В тази връзка, с оглед разпределяне на доказателствената тежест в процеса, при направено оспорване от ответника и поради липса на процесуална активност от страна на жалбоподателя жалбата, в частта ѝ касаеща твърдения за разпространение на личните данни, следва да бъде оставена без уважение, като недоказана, доколкото съгласно принципа на истинност по чл. 7 от АПК административните актове се основават на действително установени факти по случая. За пълнота следва да се отбележи, че бездействие на жалбоподателя не може да бъде компенсирано от служебното начало, доколкото съгласно чл. 36, ал. 2 от АПК страните следва да оказват съдействие на органа при събиране на доказателства, като са длъжни да предоставят доказателствата, от които черпят права, и които се намират при тях и не се намират при административния орган, както е в настоящия случай.

Водима от горното и на основание чл. 38, ал. 3 от Закона за защита на личните данни, Комисията за защита на личните данни,

РЕШИ:

Обявява жалба ППН-01-324/14.04.2021 г., подадена от С.И. срещу С.Ш. за неоснователна и недоказана.

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

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ

№ ППН-02-483/2021 г.

София, 07.04.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: в състав: Председател: Венцислав Караджов и членове: Мария Матева и Веселин Целков на заседание, проведено на 16.03.2022 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни, респективно чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента/ОРЗД), постави за разглеждане жалба № ППН-02-483/08.10.2021 г.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Комисията за защита на личните данни е сезирана с жалба заведена с вх. № ППН-02-483/08.10.2021 г. съдържаща твърдения за неправомерно обработване лични данни на жалбоподателя в изборния процес, чрез включването им в списък на лицата подкрепящи регистрацията на политическа партия „Български национален съюз“ за участие в проведените на 14.11.2021 г. избори за президент и вицепрезидент на Република България и народно събрание.

Към жалбата не са приложени доказателства, не се посочени имена на жалбоподателя.

Жалбата е подадена по електронен път от имейл адрес ***** и не носи подпис на подателя, нито имената на лицето сезирало комисията. В тази връзка в изпълнение на разпоредбата на чл. 30, ал. 1 от Административно-процесуалния кодекс (АПК) и разпоредбата на чл. 28, ал. 2 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация, до жалбоподателя е изпратено писмо № ППН-02-483-#1/17.11.2021 г. с указания, че жалбата не съдържа нормативно определените реквизити, с оглед което същата е нередовна и следва да бъде потвърдена в 3-дневен срок от получаване на съобщението за това. В допълнение подателят е информиран, че следва да посочи трите си имена, адрес за кореспонденция и постоянен адрес, а също и единния си граждански номер, с оглед предмета на жалбата и да приложи доказателства в подкрепа на твърденията си, в това число резултатите от сочената проверка на сайта на ЦИК. Уточнено е, че при неизпълнение на дадените указания в срок, образуваното производство ще бъде прекратено.

На 29.11.2021 г. писмото е изпратено на електронния адрес от който е подадена жалбата – *****, но получаването му не е потвърдено от адресата. В тази връзка и доколкото в жалбата не е посочен друг адрес за кореспонденция с подателя или телефон за връзка с него, указанията са съобщени по реда на чл. 18а, ал. 10 от АПК, чрез публикувано на 28.02.2022 г. на сайта на КЗЛД съобщение, което по аргумент от цитираната разпоредба се счита за връчено след изтичане на 7-дневен срок от публикуването му, т.е. на 08.03.2022 г. В законоустановеният 3-дневен срок и до настоящият момент не са предприети действия за потвърждаване на жалбата, респективно за изпълнение на дадените от КЗЛД указания.

Комисията за защита на личните данни е независим държавен орган, който осъществява защита на лицата при обработването на личните им данни и при осъществяване на достъпа до тези данни, както и контрол по спазването на ЗЗЛД и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г.

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

В чл. 28, ал. 1 от ПДКЗЛДНА са посочени задължителните реквизити, които следва да съдържа искането, с което е сезирана КЗЛД. Данните за искателя: имена, адрес за кореспонденция и постоянен адрес, както и подпис са задължителни реквизити на искането, като следва да се отбележи, че съгласно чл. 30, ал. 1 от АПК когато писменото искане не е подписано и при съмнение, че изхожда от посочения в него гражданин, административния орган следва да изиска неговото потвърждение със собственоръчен или електронен подпис в тридневен срок от получаване на съобщението за това. Законодателят е указал, че при непотвърждение в срока производството следва да се прекрати.

Жалба № ППН-02-483/08.10.2021 г. е подадена по електронен път и не е подписана с квалифициран електронен подпис, следователно не съдържа всички нормативно определени и задължителни реквизити, като липсват и данни безспорно индивидуализиращи подателя на искането – негови три имена, а и ЕГН с оглед предмета на жалбата.

Предвид констатираните нередовности на искането, жалбоподателят е уведомен, че следва да потвърди жалбата, като я подпишете надлежно със собственоръчен или квалифициран електронен подпис и я подадете в КЗЛД, като в допълнение посочи трите си имена, адрес за кореспонденция и постоянен адрес, а също и единния си граждански номер, с оглед предмета на жалбата.

Дадените от комисията указания не са изпълнени, в указания законоустановен срок, а и до настоящия момент. Жалбата не е потвърдена, което по аргумент от чл. 38 а от ЗЗЛД и чл. 29, ал. 1, т. 1 от ПДКЗЛДНА е пречка за разглеждането ѝ от КЗЛД. Налице са предпоставките по чл. 56, ал. 2 от АПК, във връзка с чл. 30, ал. 1 и 2 от АПК и чл. 38а от ЗЗЛД за прекратяване на производството доколкото жалбата не съдържа данни за жалбоподателя и не е подписана, а след дадени от органа указания за отстраняване на недостатъците в искането, не е потвърдена.

Водима от горното и на основание чл. 56, ал. 2, във връзка с чл. 30, ал. 1 от АПК и чл. 38 а от ЗЗЛД, чл. 28, ал. 3 и чл. 29, ал. 1, т. 1 от ПДКЗЛДНА, Комисията за защита на личните данни,

РЕШИ:

Остава без разглеждане жалба № ППН-02-483/08.10.2021 г. като нередовна и прекратява образуваното административно производство.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ

№ ППН-01-585/2021 г.

София, 07.04.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: Председател: Венцислав Караджов и членове: Цанко Цолов и Мария Матева на заседание, проведено на 23.02.2022 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни, респективно чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента/ОРЗД), постави за разглеждане по същество жалби № ППН-01-585/30.07.2021 г., ППН-01-586/30.07.2021 г. и ППН-01-589/02.08.2021 г., подадени съответно от Р.Т., Х.Т. и К.С.

Административното производство е по реда на чл. 38 от Закона за защита на личните данни (ЗЗЛД).

Комисията за защита на личните данни е сезирана с жалби подадени от Р.Т., Х.Т. и К.С. с изложени идентични твърдения, а именно за неправомерно обработване на личните им данни – три имена и единен граждански номер, чрез публикувани на сайта на сдружение „Българска републиканска федерация по кинология“, в рубрика „Новини“, Указания от съдия по вписванията, относно ИОС, 04.07.2021 г., в които същите се съдържат. В допълнение г-жа К.С. твърди, че указанията на съда са публикувани и на Фейсбук страницата на сдружението, обстоятелство което установила на 29.07.2021 г.

Жалбоподателите твърдят, че личните им данни са публикувани без тяхно знание и съгласие от Г.Х., Р.Х. и синът им Н.Х., които са администратори на сайта. Допълват, че са информирали семейство Х. за допуснатото нарушение, с искане личните им данни да бъдат заличени от публикуваните на сайта и във Фейсбук профила на сдружението указания. Молят комисията да извърши проверка по случая.

Към жалбите са приложени доказателства – екранна разпечатка на „Указания № 20210710215619/13.07.2021 г., по повод заявление № 20210710215619/10.07.2021 г. от А.Т. на осн. чл. 22, ал. 5 от ЗТРЮЛНЦ съдържащи три имена и ЕГН на жалбоподателите.

С оглед изясняване на случая от фактическа страна и на основание чл. 36, ал. 1 от АПК за служебно събиране на доказателства са направени екранни разпечатки, обективирани в Протокол ППН-01-585#1/09.08.2021 г., на публикувани на сайта <https://brfk.bg>, в раздел „Новини“, Указания от съдия по вписванията относно ИОС 04.07.2021 г. Констатирано е, че към дата на справка – 09.08.2021 г. в публикуваните указания се съдържат три имена, но не и единни граждански номера на физическите лица, сезирали КЗЛД.

Предвид публикуваната на сайта <https://brfk.bg> информация и уточнението, че същото е официален сайт на сдружение „Българска републиканска федерация по кинология“, от сдружението са изискани относими доказателства, в това число заверено копие на вътрешни правила и/или Политика за защита на личните данни относно обработването на лични данни от сдружението, предприети технически и организационни мерки за защита на личните данни, инструкция, заповед или друг акт за обучение на служителите на сдружението, в частност на тези които публикуват информация на сайта, а също и информация и резултати от извършена по случая вътрешна проверка, ако такава е възложена. Копие от жалбите са изпратени на сдружението за запознаване, с указания относно правната възможност за изразяване на писмено становище по изложените твърдения.

На проведено на 13.10.2021 г. заседание на комисията жалбите са приети за редовни - съдържат задължително изискуемите реквизити, а именно: налице са данни за жалбоподателите, естеството на искането, дата и подписи, посочени са пасивно легитимирани страни – лицата срещу които са подадени жалбите. Жалбите имат за предмет - неправомерно обработване – разпространение на личните данни на жалбоподателите – три имена и единен граждански номер, чрез публикувани на сайта на сдружение „Българска републиканска федерация по кинология“, в рубрика „Новини“, Указания от съдия по вписванията, в които същите се съдържат, публикувани и на Фейсбук страницата на сдружението.

Жалбите са подадени в срока по чл. 38 от ЗЗЛД от физически лица с правен интерес срещу пасивно легитимирани физически лица, за които се твърди, че са администратори на лични данни по смисъл чл. 4, ал. 7 Регламент ЕС 2016/679. Предвид обаче съдържанието на публикувана на сайта информация и документи комисията конституира служебно, като ответна страна в производството, сдружение „Българска републиканска федерация по кинология“, в качеството му на администратор на лични данни. Сезиран компетентен да се произнесе орган – КЗЛД, която съгласно правомощията си по чл. 10, ал. 1 от ЗЗЛД във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679, разглежда жалби срещу актове и действия на администраторите на лични данни, с които се нарушават правата на субекти на данни свързани с обработване на личните данни, като не са налице изключенията по чл. 2, § 2, буква „в“ и чл. 55, § 3 от Регламента предвид обстоятелството, че случая не касае дейности по обработване извършвани от физическо лице в хода на чисто лични или домашни занимания и/или дейности извършвани от съдилищата при изпълнение на съдебните им функции.

По изложените съображения и предвид липсата на отрицателните предпоставки по чл. 27, ал. 2 от АПК, жалбите са приети за допустими и са обединени за разглеждане в едно административно производство, с оглед обстоятелството, че правата и задълженията на страните произтичат от еднакво фактическо състояние, подадени са срещу едни и същи лица и са от компетентността на един и същ административен орган – КЗЛД. Като страни в производство са конституирани: жалбоподатели – Р.Т., Х.Т. и К.С. и ответни страни - Г.Х., Р.Х. и Н.Х., пасивно легитимирани, и сдружение „Българска републиканска федерация по кинология“ – служебно конституирана страна.

Насрочено е открито заседание за разглеждане на жалбите по същество на 08.12.2021 г., същото, поради нередовно уведомяване на страните в производството, отложено за 23.02.2021 г. от 13:00 часа.

С оглед изясняване на случая от фактическа страна от ответниците са изискани относими доказателства и информация, доколкото липсва информация и доказателства за дата на която указанията, съдържащи единните граждански номера на жалбоподателите, са публикувани на сайта на сдружението и Фейсбук страницата му.

В отговор, председателят на сдружението не оспорва изложените от жалбоподателите твърдения, дори напротив в становища ППН-01-586#6/03.12.2021 г. и ППН-01-586#6/03.12.2021 г., с идентично съдържание, признава, че указанията са публикувани във вида в който са получени от сдружението, като в последствие са заличени единните граждански номера на жалбоподателите. Не конкретизира обаче кога, като дата, са публикувани указанията със и без ЕГН на жалбоподателите.

Предвид изложените от председателя на сдружението - Г.Х. твърдения, че данните са възложени за публикуване на Р.Х. – бивш координатор, в период в който не е била служител на сдружението, от г-н Х. са изискани заверено копие на договор или друг акт уреждащ отношенията между тях по възлагане за обработване/публикуване на лични данни на сайта на сдружението, получените от съда указания и разписани технически и организационни мерки за защита на личните данни, правила, инструкции, заповед или друг акт, уреждащ реда за публикуване на документи съдържащи лични данни на сайта на сдружението и Фейсбук страницата му.

В отговор с придружително писмо ППН-01-589#4/27.01.2022 г. председателят на сдружението прилага копие на план за обучение, без дата, политика за защита на личните данни, приета на 01.02.2019 г. и указания № 20210710215619/13.07.2021 г. по описа на Агенция по вписванията. Приложена е и молба от жалбоподателката К.С., адресирана до КЗЛД, за оттегляне на жалбата. Във връзка с последната г-н Х. информира, че на 01.12.2021 г. г-жа К.С. му се обадила, за да му се извини „за причиненото неудобство от подадените жалби“.

По същество на спора г-н Х. сочи, че указанията съдържащи лични данни - ЕГН са били достъпни на сайта на сдружението 20 минути, но счита, че от последното не са произтекли никакви вреди за жалбоподателите, още повече, че указанията са достъпни и публикувани в Агенция по вписванията „месеци наред“. Твърди, че Н.Х. няма отношение към публикуваните указания, а действията на г-жа Р.Х. по публикуване на информацията на сайта на сдружението са с цел информираност на членовете на сдружението и общността на кинолозите, поради изнесени неверни и клеветнически твърдения. Не взема отношение по твърденията за публикуване на указанията и на Фейсбук страницата на сдружението.

Предвид представената от ответника молба за оттегляне на жалба ППН-01-589/02.08.2021 г., до К.С., сочена като подател на молбата, са изпратени указания да информира КЗЛД поддържа ли искането за десезиране на комисията. Получен е потвърдителен отговор от г-жа К.С., предвид което настоящето решение по същество на спора не касае подадената от нея жалба, доколкото последната е оттеглена, след провеждане на откритото заседание, като по повод същата е постановен отделен индивидуален административен акт на комисията.

На проведено на 23.02.2022 г. заседание на комисията, жалбите са разгледани по същество.

Страните – редовно уведомени, не се явяват, не се представлява.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в административното производство, изискващ наличието на установени действителни факти и предвид събраните доказателства и наведените твърдения, комисията приема, че разгледани по същество жалби ППН-01-585/30.07.2021 г. и ППН-01-586/30.07.2021 г. са основателни.

Предмет на жалбите са твърдения за неправомерно обработване – разпространение на личните данни на жалбоподателите – три имена и единен граждански номер, чрез публикувани на сайта на сдружение „Българска републиканска федерация по кинология“, в рубрика „Новини“, Указания № 20210710215619/13.07.2021 г. от длъжностно лице по вписванията, в които същите се съдържат.

Страните не спорят, че на 29.07.2021 г. на официалната страница на сдружение „Българска републиканска федерация по кинология“, в рубрика „Новини“ са публикувани указания № 20210710215619/13.07.2021 г. по описа на Агенция по вписванията, адресирани до сдружението за допускане на вписване в ТРРЮЛНЦ по партидата на сдружението на обстоятелства относно представляващия сдружението и органите на управление, в случая Управителен съвет, неговия поименен състав и мандат. В указанията са съдържат лични данни за жалбоподателите в обем три имена, ЕГН и заемана длъжност в сдружението, доколкото същите са част от органа на управление на сдружението, Х.Т. – заместник-председател на Управителния съвет, а г-жа Р.Т. – член на Управителния съвет.

Не е спорно, че указанията са публикувани на сайта на сдружението без в тях да са заличени единните граждански номера на жалбоподателите. В следствие данните са заличени, като видно от направена на 09.08.2021 г. служебна справка, относно съдържанието на публикуваните на сайта указания, обективизирана в Протокол ППН-01-585#1/09.08.2021 г., е констатирано, че в достъпните на сайта указания се съдържат три имена, но не и единни граждански номера на физическите лица, сезирали КЗЛД.

Безспорно администратор на сайта, респективно администратор на лични данни по отношение на публикуваните на сайта на сдружението данни, е сдружение „Българска републиканска федерация по кинология“, предвид което задължение на последното е да обработва данните съобразно изискванията на ОРЗД и ЗЗЛД, в това число съобразно принципите по чл. 5 от ОРЗД, в частност принципите на законосъобразност и на „свеждане на данните до минимум“ – чл. 5, § 1, буква „а“ и „в“ от ОРЗД, още повече че достъпа до сайта е неограничен и свободен. Не се събраха доказателства отношение към публикуването на данни на сайта да имат пасивнолегитимирани страни Н.Х. и Г.Х., в лично качество. По отношение на Р.Х. и предвид изложените от председателя на сдружението твърдения, че тя е публикувала данните на сайта на сдружението, следва да се отбележи, че независимо дали лицето е служител на администратора или е обработващ, в каквото качество е била тя като външен координатор, регламентът въвежда за администратора – сдружението, същите задължения: а именно данните да се обработват законосъобразно и в съответствие с принципите по чл. 5 от ОРЗД, данните да се обработват само по указания на администратора и при контрол от негова страна. Поради това и с оглед прилагане нормите на Регламента е без значение дали лицето е външен обработващ или е служител на администратора - отговорността и в двата случая е за администратора, като възражението на последния, че информацията е качена неправилно от външно за дружеството лице не може да бъде споделена от комисията, като обстоятелство изключващо отговорността на администратора.

Действията на администратора на лични данни, сдружение „Българска републиканска федерация по кинология“, по публикуване на сайта указания, без в тях да са заличени ЕГН на жалбоподателите, са незаконосъобразни - извършени без наличие на нито едно от условията за законосъобразност на обработването, доколкото е безспорно, че същото е извършено без знание и съгласие на жалбоподателите. Обработването не е необходимо за изпълнение на договор, по които субекта на данни е страна, не е необходимо за спазване на законово задължение, което се прилага спрямо администратора, не е необходимо за защита на жизненоважни интереси на субекта на данни или на друго физическо лице или за изпълнение на задача от обществен интерес, не е налице и легитимен интерес на администратора преимуществен пред интереса на лицата чиито данни са публикувани. Доколкото администраторът на лични данни не е орган на власт е неприложима и хипотезата за обработване на личните данни при упражняване на официални правомощия. В тази връзка за пълнота следва да се отбележи, че за Агенция по вписванията е налице основание за публикуване на акта – указанията по партида на сдружението в изпълнение на задълженията ѝ произтичащи от ЗТРРЮЛНЦ. Такова законово задължение за публикуване на акта обаче не е предвидено за сдружението, адресат на указанията, предвид което направената от сдружението съпоставка между действията на сдружението и Агенция по вписванията е несъстоятелна, доколкото се касае за различни администратори на лични данни, подчинени на различна правна регулация, в случая специална по отношение на Агенция по вписванията касателно нормативно установени задължения относно дейността ѝ.

При публикуване на указанията на сайта на сдружението, без заличени ЕГН на жалбоподателите, е допуснато и нарушение на принципа на „свеждане на данните до минимум“. Съгласно последния обработваните, в случая публикувани, от администратора лични данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват. Доколкото целта на сдружението е информиране на неговите членове за подлежащите на вписване обстоятелства относно състава на органите на управление на сдружението, за постигане на последното е необходимо и достатъчно посочване на трите имена на лицето и заеманата от него и вписан в регистъра към Агенция по вписванията длъжност, като посочването и на ЕГН на лицата е прекомерно.

Предвид констатираното нарушение и доколкото нарушението е първо за администратора и са предприети мерки за прекратяването му, още преди информиране на сдружението за образуването пред КЗЛД административно производство, комисията счита за пропорционално упражняването на корективно правомощие по чл. 58, § 2, буква „б“ от ОРЗД – официално предупреждение. Намира, че с оглед установената фактическа обстановка и събраните по преписката доказателства, мерките по чл. 58, § 2, буква „а“, „в“, „г“, „д“, „е“, „ж“ и „й“ от Регламент ЕС 2016/679 са неприложими, а налагането на санкция - непропорционално на допуснатото нарушение, неговата продължителност и предприетите от администратора последващи действия. Съобразявайки целта на наказанието, което следва да има възпираща и предупредителна функция, естеството и тежестта на нарушението, обществените отношения които засяга, категориите засегнати лични данни, комисията счита, че упражненото корективно правомощие безспорно отговаря на търсените от КЗЛД и Регламент 2016/679 ефективност и възпиращ ефект, като в същото време не нарушава принципа на пропорционалност и изискването за съразмерност.

Водима от горното и на основание чл. 38, ал. 3 от КЗЛД, Комисията за защита на личните данни,

РЕШИ:

1. Обявява жалби № ППН-01-585/30.07.2021 г. и ППН-01-586/30.07.2021 г. за основателни.

2. На основание чл. 58, § 2, буква „б“ от ОРЗД отправя официално предупреждение до сдружение „Българска републиканска федерация по кинология“, в качеството му на администратора на лични данни, за допуснато нарушение на чл. 5, § 1, буква „а“ „в“ от ОРЗД относно публикувани на сайта <https://brfk.bg> указания № 20210710215619/13.07.2021 г. по описа на Агенция по вписванията, съдържащи единни граждански номера на лицата сезирали КЗЛД.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

РЕШЕНИЕ

№ ППН-01-1011#36/2019 г.

София, 07.04.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на заседание, проведено на 15.12.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни, респективно чл. 57, § 1, буква „а“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента/ОРЗД), разгледа събраните доказателства относно изпълнение на постановено от комисията Решение ППН-01-1011#36/2019 от 01.03.2021 г.

Комисията за защита на личните данни е сезирана с жалба ППН-01-1011#36/07.10.2019 г., подадена от Р.Б., Е.С. и Г.А., с предмет незаконосъобразно обработване на лични данни посредством видеонаблюдение осъществявано от П.Д. в съсобствен имот с адрес ****.

Жалбоподателите информират, че във връзка с подадена през 2018 г. от тях жалба срещу М.Д., с идентичен предмет, комисията е постановила решение ППН-01-1011/18.07.2019 г. за основателност на жалбата и е издала на администратора на лични данни М.Д. разпореждане да преустанови видеонаблюдението на обществени места, имотите на жалбоподателите и прилежащото към тях съсобствено дворно място, като демонтира камерите. Твърдят, че разпореждането е изпълнено фиктивно, тъй като камерите са демонтирани и монтирани на имот собственост на П.Д., майка на М.Д., като към датата на сезиране на КЗЛД видеонаблюдението се осъществява от П.Д. Твърдят, че видеонаблюдението се осъществява без тяхно съгласие, а в обхвата му попада съсобственото дворно място.

С оглед изясняване на случая от фактическа страна е извършена проверка по предмета на жалба, резултатите от която са обективирани в Констативен акт ППН-02-428/16.10.2020 г. с приложения към него Констативен протокол от 27.08.2020 г., графични изображения от обекта и системата за видеонаблюдение и попълнен въпросник.

Констатирано е, че на посочения в жалбата адрес: **** се намира урегулиран поземлен имот (УПИ), в който са построени 5 (пет) броя сгради в режим на съсобственост. П.Д. е собственик на едноетажна жилищна сграда - къща, която отдава под наем за нощувки. Жалбоподателите са собственици на сгради, както и част от дворното място в същия поземлен имот. Една от сградите в имота е собственост на Сдружение на еврейската общност „Обе Шалом” - Русе.

След извършен оглед е констатирано, че видеокамерите са с пространствено разположение и обхват на заснемане, както следва: Първата видеокамера е монтирана на метална врата отделяща 1/3 идеална част от парцела, собственост на Д., насочена е и заснема пътека в общото дворно пространство между имота на Д. и сграда в УПИ-то, собственост на Сдружение „Обе Шалом”, която пътека П.Д. и жалбоподателите използват, за да достигнат до имотите си. Камерата заснема също входа към поземления имот, използван от всички собственици, прилежаща част от улица „Видин” и тротоара. Втората и третата видеокамери са монтирани на фасадата на къщата на Д., насочени са и заснемат част от дворното място в нейния имот и част от общата пътека, описана по-горе. Четвъртата видеокамера е монтирана на фасадата на къщата, насочена е и заснема част от дворното място на П.Д., част от пътеката в общото дворно място, както и част от къщата, обитавана от жалбоподателя Р.Б. Видеокамерите са с резолюция, позволяваща идентификация на физически лица. На видно място на прозорец на къщата на Д., откъм пътеката в общото дворно място, има поставена информационна табела за видеонаблюдението. Не са представени документи (правила, процедури), регламентиращи обработването на лични данни чрез изградената система за видеонаблюдение.

Безспорно установено е, че ответниците осъществяват видеонаблюдение посредством изградена в имота на П.Д. система за видеонаблюдение, състояща се от 4 (четири) броя куполни камери за видеонаблюдение, видеорекордер - снабден с твърд диск, както и други вложени компоненти (кабели, зарядни устройства, ел. кутии, конектори и др. Извършва се запис с видеокадри на твърдия диск в рекордера, като записите се съхраняват за срок от около 1 (един) месец, след което автоматично се изтриват по реда на тяхното постъпване. Локален достъп до системата се осъществява от П.Д. и нейната дъщеря М.Д. Отдалечен достъп до изходящия образ от видеокамерите в реално време и записите с видеокадри на твърдия диск в рекордера се осъществява от М.Д. посредством специализиран софтуер, инсталиран на неин мобилен телефон. Достъпът се осъществява след въвеждане на атрибути за идентификация - потребителско име и парола, известни единствено на дъщерята на П.Д. - М.Д.

По преписката липсват доказателства за възлагане, а и твърдения, за възлагане на обработването на лични данни чрез системата за видеонаблюдение от администратор на обработващ, поради което и предвид констатираната фактическа обстановка П.Д. и М.Д. е приела, че имат качеството на администратори на лични данни, доколкото сами определят целите и средствата за обработване на лични данни чрез системата за видеонаблюдение и имат достъп до същата.

По отношение на ответницата П.Д. и предвид целта на осъществявано видеонаблюдение, обхвата и техническите характеристики на камерите комисията е приела, че се касае за видеонаблюдение извършвано в нарушение на принципите на законосъобразност и „свеждане на данните до минимум” разписани в чл. 5, § 1, буква „а” и „в” от Регламент ЕС 2016/679, с оглед обстоятелството, че се заснемат имоти които не са собственост на администратора П.Д. и обществени места – част от прилежаща улица и тротоар.

По отношение на ответницата М.Д. и предвид целта на осъществявано видеонаблюдение и неговия обхват, комисията е приела извода за видеонаблюдение извършвано в нарушение на принципите на законосъобразност разписан в чл. 5, § 1, буква „а” от ОРЗД, с оглед обстоятелството, че се заснемат имоти които не са собственост на администратора М.Д. и обществени места – част от прилежаща улица и тротоар, предвид което за М.Д. липсва условия за законосъобразност на обработването по смисъла на чл. 6, § 1 от ОРЗД по аргументи идентични с изложените относно П.Д. Изводът е мотивиран от анализ на представените по преписката доказателства и твърденията на страните, от които се установи, че ответницата М.Д. няма собственост в УПИ-то, липсват доказателства за наличието на вещни права върху имота, поради и което осъществяването от нея видеонаблюдение е без правно основание, обстоятелство което е констатирано и с решение ППН-01-1011/18.07.2019 г. на КЗЛД, същото известно на М.Д.

Предвид характера и вида на констатираните нарушения и обстоятелството, че същите не са преустановени, а също и че засегнатите лични данни не са чувствителни по смисъла на закона и няма данни за настъпили вреди от обработването, комисията е приела за целесъобразно, пропорционално и ефективно налагането на корективна мярка по чл. 58, § 2, буква „г” от Регламент ЕС 2016/679 и на двата администратора П.Д. и М.Д., като е приела, че същата ще постигне целта на закона - ще преустанови нарушението и ще възстанови установения правов ред по отношение на обработването на личните данни. Доколкото констатираното нарушение обаче е второ за М.Д., в допълнение на корективната мярка по чл. 58, § 2, буква „г” от ОРЗД комисията е наложила и глоба на М.Д. в размер на 1 000 лв. (хиляда лева).

Мотивирано от горното комисията е постановила решение ППН-01-1011#36/2019 01.03.2021 г. със следния диспозитив:

1. Обявява жалба № ППН-01-1011#36/07.10.2019 г. за основателна.

2. За нарушение на чл. 5, § 1, буква „а” и „в” от Регламент ЕС 2016/679 и на основание чл. 58, § 2, буква „г” от Регламента издава разпореждане на П.Д. да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като преустанови видеонаблюдението и демонтира камерите, в едномесечен от влизането на решението в сила, след което да уведоми комисията за изпълнението като представи съответните доказателства.

3. За нарушение на чл. 5, § 1, буква „а” от Регламент ЕС 2016/679 и на основание чл. 58, § 2, буква „г” от Регламента издава разпореждане на М.Д. да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като преустанови видеонаблюдението, в едномесечен от влизането на решението в сила, след което да уведоми комисията за изпълнението като представи съответните доказателства.

4. На основание чл. 83, § 5, буква „а” и чл. 58, § 2, буква „и” от ОРЗД налага на М.Д. глоба в размер на 1 000 лв. (хиляда лева) за нарушение на чл. 5, § 1, буква „а” от Регламент.

Решението е съобщено на страните в административното производство, не е обжалвано и е влязло в законна сила на 16.06.2021 г. По отношение на М.Д. са предприети действия за принудително събиране на наложената глоба в размер на 1 000 лв. чрез органите на НАП – образувано е изпълнително дело, няма данни глобата да е заплатена.

Доказателства за изпълнението на издаденото от КЗЛД разпореждане за демонтиране на камерите и преустановяване на видеонаблюдението не са представени в указания в решението срок. С писмо ППН-01-1011#55/24.06.2021 г. в КЗЛД е постъпило заявление от жалбоподателя Р.Б., с приложени към него доказателства - снимки на местоположението на камерите, в което се съдържат твърдения за неизпълнение на издаденото разпореждане.

Предвид горното с решение от проведено на 15.09.2021 г. КЗЛД е възложила проверка относно изпълнението на разпорежданията, резултатите от която са обективирани в констативен акт ППН-02-610/30.11.2021 г.

Проверката на място е открита на 19.11.2021 г. на адрес: ****, в присъствието на П.Д. и нейната дъщеря М.Д. По време на проверката присъства и К.Т. - служител на КЗЛД. П.Д. и М.Д. са информирани за задължението им да окажат съдействие на проверяващия екип при упражняване на контролните правомощия на КЗЛД и да осигурят възможност за достъп до изградената система за видеонаблюдение - предмет на жалбата с оглед събиране на доказателства във връзка с изпълнението на задачата на проверката, възложена със заповедта на Председателя на КЗЛД.

П.Д. и М.Д. отказват да получат заповедта за проверка и заявяват, че няма да осигурят достъп до системата за видеонаблюдение и съдействие на проверяващия екип, както и че няма промяна в констатираните факти и обстоятелства при извършената проверка от КЗЛД на 27.08.2020 г., обективирана в Констативен акт рег. № ППН-02-428/16.10.2020 г., приет с Решение на КЗЛД от Протокол № 45/21.10.2020 г. и приобщен към преписката. П.Д. и М.Д. заявяват също, че няма да преустановят видеонаблюдението и да демонтират камерите, респ. няма да изпълнят издаденото им Разпореждане на КЗЛД, обективирано в Решение № ППН-01-1011#36/2019 г. от 01.03.2021 г., не желаят повече да бъдат притеснявани от КЗЛД във връзка с жалбата, като в противен случай ще заведат дело за тормоз.

В хода на проверката е извършен външен оглед на обекта и камерите за видеонаблюдение. От извършения външен оглед се констатира, че на обекта са налични 4 (четири) броя куполни камери за видеонаблюдение, които са със същото пространствено разположение, както при извършената проверка на 27.08.2020 г., обективирана в Констативен акт рег. № ППН-02-428/16.10.2020 г., а именно:

Камера 1 е монтирана на метална врата към имота на П.Д., насочена е към пътека в общото дворно пространство между имота на Д. и сграда в УПИ-то, собственост на Сдружение „Обе Шалом”, входа към поземления имот, прилежащата част от улица „Видин” и тротоара.

Камери 2 и 3 са монтирани на фасадата на къщата на Д., насочени са към част от дворното място в нейния имот и част от общата пътека, описана по-горе.

Камера 4 е монтирана на фасадата на къщата, насочена е към част от дворното място на Д., част от пътеката в общото дворно място, както и част от къщата, обитавана от жалбоподателя Р.Б.

На видно място на металната врата и прозорец на къщата на Д. откъм пътеката в общото дворно място, има поставени информационни табели, предупреждаващи за извършвано видеонаблюдение на обекта.

Събраните в хода на производството доказателства свидетелствата за неизпълнение на издаденото от комисията разпореждане и продължавано видеонаблюдение в нарушение на ОРЗД, въпреки влязъл в сила индивидуален административен акт и дадени с него изрични и конкретни указания относно приложното поле на ОРЗД и произтичащите от него задължения за администраторите на лични данни. Целта на упражненото корективно правомощие е преустановяване на нарушението и възстановяване на установения правово ред при обработване на лични данни, като именно във връзка с постигане на последните неизпълнението на издадени от надзорните органи разпореждания са скрепени със санкция, обстоятелство за което лицата са изрично и превантивно уведомени, като е посочено, че съгласно чл. 83, § 6 от ОРЗД неспазването на разпореждане на надзорния орган подлежи на административно наказание „глоба” или „имуществена санкция” в размер до 20 000 000 EUR.

Въпреки горното, събраните по преписката доказателства свидетелстват, че изпълнение липсва, поради което комисията счита, че са налице предпоставките на чл. 83, § 6 от ОРЗД за ангажиране на административно-наказателната отговорност на П.Д. и М.Д. за неизпълнение на издадени от КЗЛД разпореждания до всяка една от тях обективирани съответно в т. 2 и т. 3 Решение № ППН-01-1011#36/2018 г. от 01.03.2021 г. на КЗЛД.

В конкретния случай при определяне на размера на глобата, общо за двете лица, като смекчаващи следва да се отчетат обстоятелствата, че задължените са физически лица и се касае за обработване на лични данни чрез видеонаблюдение – изображение, евентуални контакти и навици на наблюдаваните лица и няма данни от обработването да са настъпили вредни последици за жалбоподателите. Като отегчаващи следва да се квалифицират обстоятелствата, че се касае за умишъл при неизпълнение на разпорежданията, както и продължителността на деянието – осъществявано неправомерно видеонаблюдение в продължение на две години, в частност неизпълнение на разпореждане повече от три месеца от влизане в сила на решението на КЗЛД.

Като утежняващи обстоятелства при определяне не на по-висок размер на глобата наложена на М.Д. комисията приема, че нарушението е поредно за санкционираното лице. С Решение ППН-01-1011/18.07.2019 г. на КЗЛД с идентичен предмета, видеонаблюдение осъществявано на адрес *****, на М.Д. е издадено разпореждане по чл. 58, § 2, буква „г” от ОРЗД „да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като в 14-дневен срок от влизане в сила на решението преустанови видеонаблюдението на обществени места, имотите на жалбоподателите и прилежащото към тях съсобствено дворно място, като демонтира камерите”. Решението е съобщено на г-жа Д., не е обжалвано и е влязло в сила, а на КЗЛД са представени доказателства за демонтиране на камерите по твърдение извършено на 22.07.2019 г. Видно обаче по събраните по настоящата преписка доказателства, „в края на месец юли 2019 г.”, т.е. седмица след това, е изградена нова система за видеонаблюдение, при която макар камерите да са позиционирани на други места, са с идентичен обхват, като този констатиран с решението на КЗЛД. С последващо Решение ППН-01-1011#36/2019 г. от 01.03.2021 г. е ангажирана административно-наказателната отговорност на М.Д. за извършвано видеонаблюдение на адреса с налагане на глоба в размер на 1 000 лв., в допълнение с дадено разпореждане за преустановяване на същото. Хронологията свидетелства за умишъл в действията на М.Д. и явно незачитане правилата в сферата на личните данни, доколкото същата е наясно с последиците от видеонаблюдението, а именно извършването му в нарушение на ОРЗД.

По изложените съображения комисията счита, че с оглед принципа на пропорционалност между тежестта на нарушението и размера на наказанието, наложената на П.Д. глоба следва да е в размер на 1 000 лв. (хиляда лева), а глобата наложена на М.Д. в завишен размер - 2 000 лв. (две хиляда лева).

Съобразявайки целта на наказанието, което следва да има възпираща и предупредителна функция, естеството и тежестта на нарушението, обществените отношения които засяга, категориите засегнати лични данни, комисията счита, че упражнените правомощия по вид и размер безспорно отговарят на търсените от ЗЗЛД и Регламент 2016/679 ефективност и възпиращ ефект, като в същото време не нарушава принципа на пропорционалност и изискването за съразмерност.

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

РЕШИ:

1. На основание чл. 83, § 6 от ОРЗД да налага на П.Д. глоба в размер на 1 000 лв. (хиляда лева) за неизпълнение на влязло в сила разпореждане на КЗЛД, обективирано в т. 2 от Решение № ППН-01-1011#36/01.03.2021 г.

2. На основание чл. 83, § 6 от ОРЗД налага на М.Д., глоба в размер на 2 000 лв. (две хиляди лева) за неизпълнение на влязло в сила разпореждане на КЗЛД обективирано в т. 3 от Решение № ППН-01-1011#36/01.03.2021 г.

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

След влизане в сила на решението, сумата по наложеното наказание следва да бъде преведена по банков път:

Банка БНБ – ЦУ, IBAN: BG18BNBG96613000158601

BIC BNBGBGSD

Комисия за защита на личните данни, БУЛСТАТ 130961721.

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-01-25/2022 г. гр. София, 17.03.2022 г.

ОТНОСНО: *Снемане на данни от документ за самоличност съгласно чл. 2, ал. 3 от Наредба за документите за заемане на държавна служба*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов и Мария Матева, на свое редовно заседание, проведено на 02.03.2022 г., разглежда искане за становище с вх. № ПНМД-01-25/17.02.2022 г. от представляващ сдружение с нестопанска цел „Асоциация на длъжностните лица по защита на данните”.

В искането се отправя въпрос дали снемането на данни от документ за самоличност съгласно чл. 2, ал. 3 от Наредба за документите за заемане на държавна служба (наричана по-нататък „Наредбата”) включва действие по копирането на документа за самоличност. Наред с това, от сдружението питат, ако под „снемане” не се разбира копиране, как ще бъде изпълнено изискването за представяне на документ за самоличност (лична карта/паспорт) към заявлението по чл. 2, ал. 1 (Приложение № 1 от Наредбата).

Правен анализ:

Съгласно чл. 8 от Закона за държавния служител (ЗДСл) за заемане на държавна служба се подава писмено заявление за назначаване, към което се прилагат необходимите документи за заемането на съответната длъжност, определени в наредба на Министерския съвет.

Наредба за документите за заемане на държавна служба (приета с ПМС № 314 от 23.11.2011 г.) е приета на основание чл. 8, ал. 2 от ЗДСл. С нея се определят необходимите документи за назначаване на длъжност, определена за заемане от държавен служител (държавна служба). В чл. 2, ал. 1 от Наредбата се сочи, че за заемане на държавна служба се подава писмено заявление за назначаване по образец съгласно приложение № 1 от същата. Съгласно ал. 2 на същия член към заявлението се представят:

- 1. документ за самоличност;**
- 2. документ за образователно-квалификационна степен, специалност, квалификация, правоспособност, които се изискват за длъжността;**
- 3. документ, удостоверяващ професионалния опит;**
4. документ за медицински преглед при първоначално постъпване на работа, както и когато трудовата дейност е прекратявана за повече от 3 календарни месеца;
5. (отм. - ДВ, бр. 48 от 2018 г.)
- 6. други документи, които удостоверяват изпълнението на специфичните изисквания за заемането на длъжността;**
7. (отм. - ДВ, бр. 48 от 2018 г.)
8. документ за ползван платен годишен отпуск, ако през същата година лицето е работило по друго правоотношение. Документът не се представя, в случай че лицето е работило в същата или друга администрация и той може да бъде получен по служебен път.

Според ал. 3 данните от документите по ал. 2, т. 1, 2, 3 и 6, посочени по-горе, се снемат и те се връщат на притежателите им.

Правилата на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) се прилагат за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Съгласно легалната дефиниция, посочена в чл. 4, т. 2 от ОРЗД „обработване” на лични данни означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване. Видно от дефиницията, същата не изрежда изчерпателно операциите, които могат да бъдат извършени при обработването на лични данни.

С изменението и допълнението на Закона за защита на личните данни (ЗЗЛД) (ДВ, бр. 17 от 2019 г.) законодателят предвиди, че администратор или обработващ лични данни може да копира документ за самоличност, свидетелство за управление на моторно превозно средство или документ за пребиваване само ако това е предвидено със закон (чл. 25г от ЗЗЛД).

Систематичното тълкуване на понятието „снемане”, като операция по обработване на лични данни, следва да се разглежда с оглед естеството, обхвата, контекста и целите на конкретното обработване. Традиционно българското законодателство конкретизира действията и операциите, които могат да се извършват за осъществяване на т.нар. „снемане”, като например:

- снемане на самоличност по чл. 170 от Гражданския процесуален кодекс (ГПК);
- снемане на копие от официален документ за самоличност по чл. 53 от Закона за мерките срещу изпиране на пари (ЗМИП);
- снемане на пръстови отпечатъци по чл. 71 от Закона за МВР (ЗМВР) и т.н.

В конкретния случай Наредбата изрично посочва в чл. 2, ал. 3, че от съответните документи се „снемат данни” и същите се връщат на притежателите им, като в разпоредбата няма никакви индикации за снемане на копия или такива да се задържат/съхраняват от органа по назначаването. Това налага извода, че при подаването на заявление за назначаване, лицето представя¹ документа си за самоличност за целите на сверяване на идентификационните му данни, попълнени от него в заявлението, респ. отразяването им в документацията за назначаването, без обаче същият да се копира и съхранява от органа по назначаването. Този извод е застъпен и в трайната практика² на КЗЛД, според която, обработването на лични данни, чрез събиране и съхранение на копие на документ за самоличност за целите на възникване на трудовото или служебно правоотношение, е недопустимо. Това е така, тъй като чрез тези операции администраторът (работодател/орган по назначаването) обработва лични данни, които не му се следват (напр. снимката и данните за ръст и цвят на очите), което от своя страна представлява нарушение на принципите за обработване на лични данни, прогласени в Регламент (ЕС) 2016/679, а преди това и в отменената от него Директива 95/46/ЕО.

Отчитайки гореизложеното, може да се направи обосновано заключение, че копирането или възпроизвеждането по какъвто и да е друг начин на образа на документите по чл. 2, ал. 2, т. 1, 2, 3 и 6 от Наредбата, е недопустимо.

¹ Неслучайно в чл. 2, ал. 2 от Наредбата е използван глаголът „представя“, а не „прилага“.

² Решения, задължителни предписания и други актове на КЗЛД в този смисъл могат да бъдат открити в секция „Практика“ на официалния ѝ сайт: <https://cpdp.bg>

В контекста на настоящия казус е от значение да се спомене и разпоредбата на чл. 25к, ал. 2 от ЗЗЛД, съгласно която, когато в процедурата по набиране и подбор на персонал, работодателят или органът по назначаването е изискал да се представят оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, той е длъжен да върне тези документи на кандидата (субекта на данни), който не е одобрен за назначаване, в 6-месечен срок от окончателното приключване на процедурата, доколкото специален закон не предвижда друго. Тук следва да се отчита и обстоятелството, че държавният служител се назначава по специалните правила и процедури, регламентирани в ЗДСл и Наредбата за провеждане на конкурсите и подбора при мобилност на държавни служители (НПКПМДС), която предвижда, че органът по назначаването трябва да съхранява в архива на администрацията всички документи, които са свързани с провеждането на конкурса, в сроковете, определени по реда на чл. 43 от Закона за Националния архивен фонд (чл. 5, ал. 2 от НПКПМДС).

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:

Копирането или възпроизвеждането по какъвто и да е друг начин на образа на документите по чл. 2, ал. 2, т. 1, 2, 3 и 6 от Наредбата за документите за заемане на държавна служба, както и съхранението на техни копия, е недопустимо, доколкото в чл. 2, ал. 3 от същата се посочва ясно, че се снемат данни от тях, а не копия, като след това документите се връщат на притежателите им.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

СТАНОВИЩЕ НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № ПНМД-01-27/2022 г. гр. София, 06.04.2022 г.

ОТНОСНО: *Законосъобразност на обработването на лични данни чрез видеозапис при провеждането на устните изпити по конкурсите за първоначално назначаване в органите на съдебната власт*

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 30.03.2022 г., разгледа писмо с вх. № ПНМД-01-27/08.03.2022 г. от заместник-председателя на Комисията по атестирането и конкурсите към Съдийската колегия на Висшия съдебен съвет (ВСС). С него се иска становище по отношение на законосъобразността на обработването на лични данни чрез видеозапис при провеждането на устните изпити по конкурсите за първоначално назначаване в органите на съдебната власт. Искането

е продиктувано от обсъждане за изработване на проект за изменение и допълнение на *Наредба № 1 от 9 февруари 2017 г. за конкурсите за магистрати и за избор на административни ръководители в органите на съдебната власт*, която се издава от ВСС на основание чл. 194г от Закона за съдебната власт (ЗСВ). В тази връзка, на КЗЛД е изпратено извлечение от Протокол № 9 от заседание на Комисията по атестирането и конкурсите към Съдийската колегия на ВСС, проведено на 28.02.2022 г., от което е видно, че е взето решение да се изпрати запитване до надзорния орган по този въпрос.

Правен анализ:

Видеонаблюдението е дейност, свързана със събиране и запазване на образни или аудиовизуални данни за лица, попадащи в наблюдавана зона, които подлежат на пряко или косвено идентифициране въз основа на техния външен вид или други специфични признаци. Съществен елемент от тази дейност е, че самоличността на лицата може да бъде установена въз основа на тези данни, а също така се създава възможност за обработване на данни относно присъствието и поведението на лицата в съответната зона.

Съгласно съображение (40) от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД), за да бъде обработването законосъобразно, личните данни следва да бъдат обработвани въз основа на някое от основанията, посочени в чл. 6, пар. 1 и/или чл. 9, пар. 2 от ОРЗД. По отношение на обработването на лични данни, необходимо за спазване на нормативно задължение, за изпълнение на задача от обществен интерес или при упражняване на официални правомощия, предоставени на администратора на лични данни, следва да са налице национални разпоредби, които да уточняват по-нататък реда за прилагане на правилата на ОРЗД.

От друга страна, всяко обработване на лични данни следва да отговаря на принципите, прогласени в чл. 5 от ОРЗД, съгласно които обработването трябва да е законосъобразно и добросъвестно (чл. 5, пар. 1, б. а) от ОРЗД). Наред с това, за физическите лица следва да е ясно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират, предоставят или обработват по друг начин, както и в какъв обхват се извършва или ще се извърши обработването на данните. Принципът за прозрачност (чл. 5, пар. 1, б. а) от ОРЗД) изисква всяка информация и комуникация във връзка с обработването на тези лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Този принцип се отнася в особена степен за информацията, която физическите лица (субекти на данни) получават за идентификация на администратора и целите на обработването, и за допълнителната информация, гарантираща добросъвестното и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват. Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на личните им данни, както и за начините, по които могат да ги упражняват. По-специално, **конкретните цели** (чл. 5, пар. 1, б. б) от ОРЗД), **за които се обработват личните данни, следва да бъдат ясни и законни и определени към момента на събирането им**. По общо правило, личните данни следва да са адекватни, относими и ограничени до необходимото за целите (чл. 5, пар. 1, б. в) от ОРЗД), за които се обработват. Това налага по-специално да се гарантира, че срокът (чл. 5, пар. 1, б. д) от ОРЗД), за който се съхраняват, е ограничен до строг минимум. Личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства. С цел да се гарантира, че срокът на съхранението им не е подълъг от необходимия за който се обработват, администраторът трябва да установи съответни срокове за тяхното изтриване, както и да извършва периодичен преглед на същите. Администраторът следва да предприеме всички разумни мерки, за да се гарантира, че неточните лични данни (чл. 5, пар. 1, б. г) от ОРЗД) се коригират или заличават. Личните данни следва да се обработват по начин, който гарантира подходяща степен на сигурност и поверителност (чл. 5, пар. 1, б. е) от ОРЗД), включително за предотвратяване на непозволен достъп до тях и до оборудване за тяхното обработване или за предотвратяване на използването им.

Кумулативното спазване на горепосочените принципи следва да се докаже от администратора (т.нар. принцип за „отчетност”, предвиден в чл. 5, пар. 2 от ОРЗД). Администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с ОРЗД, като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица (отговорност на администратора по чл. 24 от ОРЗД). За да бъдат въведените мерки адекватни и да съответстват на основните принципи, същите следва да се преразглеждат и при необходимост да се актуализират от администратора.

Принципно положение е, че целите и средствата за обработването на лични данни се определят или от администратора, или произтичат от правото на ЕС или националното законодателство (арг. чл. 4, т. 7) от ОРЗД). При създаването на нови разпоредби, въвеждащи извършването на видеозапис при провеждането на устни изпити по конкурсите за първоначално назначаване в органите на съдебната власт, ВСС следва ясно да дефинира целта/целите на въпросното обработване на лични данни. В качеството си на администратор – публичен орган, ВСС би могъл да обработва лични данни, чрез видеозапис при провеждането на устни изпити, единствено при условията на чл. 6, пар. 1, б. в) или б. д) от ОРЗД, а именно:

- обработването е необходимо за спазването на **законово задължение**, което се прилага спрямо администратора; или
- обработването е необходимо за изпълнението на задача от **обществен интерес** или при упражняването на **официални правомощия**, които са предоставени на администратора.

Съгласно чл. 6, пар. 3 от ОРЗД посочените основания следва да са установени в правото на Съюза или националното ни законодателство. В съответствие с практиката на Съда на Европейския съюз и на Европейския съд по правата на човека, тези основания трябва да бъдат ясни и точни, а прилагането им предвидимо за лицата, за които се отнасят (арг. съобр. 41 от ОРЗД). Отчитайки това принципно положение, за всяко от посочените основания се изисква да бъдат въведени конкретни разпоредби, които да адаптират прилагането на изискванията на ОРЗД по отношение на следните основни елементи, касаещи обработването на лични данни:

- общите условия, които определят законосъобразността на обработването от администратора (целите на обработването, за което личните данни са предназначени, както и правното основание за това);
- категориите данни, които подлежат на обработване;
- категориите субекти на данни, засегнати от обработването;
- операциите и процедурите за обработване и последиците от тях;
- лицата/органите, пред които могат да бъдат разкривани личните данни и целите, за които се разкриват;
- ограниченията по отношение на целите на разкриването;
- периодът на съхранение;
- информираност на субектите на данни (чл. 13 и/или чл. 14 от ОРЗД) и прозрачност на обработването (чл. 12 от ОРЗД);
- мерки за гарантиране на правата и свободите на засегнатите субекти на данни.

Следователно, въвеждането на видеозапис при провеждане на устните изпити по конкурсите за първоначално назначаване в органите на съдебната власт, налага регламентирането на посочените по-горе елементи с изменението и допълнението на *Наредба № 1 от 9 февруари 2017 г. за конкурсите за магистрати и за избор на административни ръководители в органите на съдебната власт*.

За пълнота на изложението следва да се отчита и обстоятелството, че видеозаснемане, което включва и звукозапис, засяга в по-висока степен сферата на личната неприкосновеност на субекта на данни. В този смисъл, ако се предвижда и звукозапис, това следва да е изрично посочено в разпоредбите на Наредба № 1, като се предвидят и подходящи допълнителни гаранции за защита правата на засегнатите субекти на данни.

В контекста на настоящото искане за становище е от значение да се отбележи, че КЗЛД се е произнасяла по аналогичен казус, свързан с допустимостта на въвеждането на видеозаснемане при провеждане на изпитите за националните външни оценявания, като в резултат на това министърът на образованието и науката приема конкретни норми, които са обективирани в *Наредба № 11 от 1 септември 2016 г. за оценяване на резултатите от обучението на учениците*.

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:

Висшият съдебен съвет може да въведе разпоредби в *Наредба № 1 от 9 февруари 2017 г. за конкурсите за магистрати и за избор на административни ръководители в органите на съдебната власт*, които да регламентират извършването на видеозапис при провеждането на устните изпити по конкурсите за първоначално назначаване в органите на съдебната власт, като се отчитат изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/



Комисия за защита на личните данни

Председател: Венцислав Караджов

Членове: Цанко Цолов
Мария Матева
Веселин Целков

Информационен бюлетин № 3 (96) 2022 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