РЕПУБЛИКА БЪЛГАРИЯ

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Г О Д И Ш Е Н О Т Ч Е Т

на Комисията за защита на личните данни

за дейността ѝ през 2021 г.

на основание чл. 7, ал. 6 от Закона за

защита на личните данни

СЪДЪРЖАНИЕ

I. Увод 5
II. Анализ и отчет на степента на постигане на целите и приоритетите на КЗЛД, залегнали в годишния отчет за 2020 г. 6
III. Защита на правата на субектите на данни при обработване на личните им данни 9
IV. Контролна дейност 35
V. Производства по изразяване на становища и участие в съгласувателни процедури на нормативни актове по въпросите, свързани със защита на личните данни 63
VI. Участие в механизмите за съгласуваност и сътрудничество в рамките на Европейския комитет за защита на данните 91
VII. Международна дейност 97
VIII. Подпомагане изпълнението на целите на КЗЛД чрез реализация на проекти с национално и международно финансиране 110
IX. Комисия за защита на личните данни – наблюдаващ орган относно сигурността на данните съгласно ЗЕС 115
X. Реализиране на политики за публичност и повишаване на обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработване на лични данни. Институционално взаимодействие 118
XI. Административен капацитет и финансови ресурси 159
XII. Цели и приоритети на КЗЛД за 2022 г. 168

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

АВп	Агенция по вписванията
АЛД	Администратор на лични данни
АПК	Административнопроцесуален кодекс
АСП	Агенция за социално подпомагане
АУАН	Акт за установяване на административно нарушение
ВАС	Върховен административен съд
ВИС	Визова информационна система
ВНО	Водещ надзорен орган
ГДБОП	Главна дирекция „Борба с организираната престъпност“
ГПК	Граждански процесуален кодекс
ЕГН	Единен граждански номер
ЕИК	Единен идентификационен код
ЕСГРАОН	Единна система за гражданска регистрация и административно обслужване на населението
ДВ	Държавен вестник
ЕВРОДАК	Европейска система за автоматизирана идентификация на пръстови отпечатъци
ДЛЗД	Длъжностно лице по защита на данните
ЕИП	Европейско икономическо пространство
ЕК	Европейска комисия
ЕКЗД	Европейски комитет по защита на данните
ЕНОЗД	Европейски надзорен орган по защита на данните
ЕС	Европейски съюз
ЗАНН	Закон за административните нарушения и наказания
ЗБЛД	Закон за българските лични документи
ЗГР	Закон за гражданската регистрация
ЗДОИ	Закон за достъп до обществена информация
ЗЗдр	Закон за здравето
ЗЗЛД	Закон за защита на личните данни
ЗМИП	Закон за мерките срещу изпирането на пари
ЗНО	Засегнат надзорен орган
ЗПУ	Закон за пощенските услуги
ЗЕС	Закон за електронните съобщения

ЗЕУ	Закон за електронното управление
ИВСС	Инспекторат към Висшия съдебен съвет
ИИ, AI	Изкуствен интелект
ИСВП, IMI	Информационна система на вътрешния пазар
КЗЛД, Комисията	Комисия за защита на личните данни
ККН	Комитет за координиран надзор към ЕКЗД
КРС	Комисия за регулиране на съобщенията
ЛНЧ	Личен номер на чужденец
МВР	Министерство на вътрешните работи
МИС	Митническа информационна система
МОН	Министерство на образованието и науката
МПС	Моторно превозно средство
МРРБ	Министерство на регионалното развитие и благоустройството
МСП	Малки и средни предприятия
НАП	Национална агенция за приходите
НЗИС	Националната здравноинформационна система
НП	Наказателно постановление
НСИ	Национален статистически институт
ОВЗД	Оценка на въздействието върху защитата на данните
ОИСР	Организация за икономическо сътрудничество и развитие
ОЛД	Обработващ лични данни
ПДКЗЛДНА	Правилник за дейността на Комисията за защита на личните данни и на нейната администрация.
ПОДНС	Правилник за организацията и дейността на Народното събрание
Регламент (ЕС) 2016/679, Регламент 2016/679, Регламента, ОРЗД	Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)
СЕВ	Съвет по европейските въпроси към Министерския съвет
ШИС II	Шенгенска информационна система от второ поколение
ЮЛ	Юридическо лице
IoT	Интернет на свързаните устройства

I. УВОД

Настоящият отчет за дейността на Комисията за защита на личните данни (КЗЛД/Комисията) е изготвен на основание чл. 7, ал. 6 от Закона за защита на личните данни (ЗЗЛД) и обхваща периода от 01.01.2021 г. до 31.12.2021 г.

В отчета е представена информация за основните направления на дейност на КЗЛД през посочения период. Направен е анализ на степента на постигане на поставените цели и приоритети. Включена е обобщена тематична информация по въпроси, свързани с разглеждането на жалби и сигнали, запитвания на граждани и проведените консултации по тях. Отчетена е постоянната тенденция на повишаване обема и сложността на постъпващите жалби и сигнали, и извършените проверки на администратори на лични данни на фона на намалената през 2019 и 2020 г. численост на администрацията на КЗЛД. Поставен е акцент върху изразените през отчетния период становища по въпроси от сериозен обществен интерес, както и отговорите на запитвания на администратори и обработващи лични данни по теми с принципен характер. Отчетени са административният капацитет и финансовото състояние на КЗЛД.

II. АНАЛИЗ И ОТЧЕТ НА СТЕПЕНТА НА ПОСТИГАНЕ НА ЦЕЛИТЕ И ПРИОРИТЕТИТЕ НА КЗЛД, ЗАЛЕГНАЛИ В ГОДИШНИЯ ОТЧЕТ ЗА 2020 г.

Важен елемент от ефективната надзорна дейност на Комисията за защита на личните данни през 2021 г. е анализът на съвременните тенденции и предизвикателства пред защитата на данните като изкуствения интелект, лицевото разпознаване, защитата на личните данни на деца в интернет, големите бази данни и свързаната с тях възможност за профилиране. За реализацията на тази цел е извършена много сериозна аналитична дейност, подробно представена в раздел X на годишния отчет. Фокусът на извършената дейност е не само аналитично-теоретично изясняване на съдържанието на посочените предизвикателства, но и набелязване на практическите направления за бъдещо развитие от гледна точка на защитата на правата и свободите на физическите лица и свързаната с тях надзорна дейност на КЗЛД. Формулирани са съвети и са кодифицирани добри европейски и международни практики. В допълнение към анализите на посочените теми е изготвен и информационно-разяснителен материал „Съвети към администраторите и обработващите лични данни за защита на данните в киберпространството“, който насочва вниманието на администраторите и обработващите лични данни към множеството предизвикателства пред сигурността за обработване и съхраняване на личните данни в дигиталната среда.

По линия на постоянния приоритет на КЗЛД за продължаване на усилията на надзорния орган за пълноправно членство в Шенген през 2021 г. са извършени проверки на националните системи/звена на Шенгенската информационна система от второ поколение (ШИС II), Визовата информационна система (ВИС) и националната консулска служба. Поради продължаването на ограничителните мерки с оглед пандемичната обстановка КЗЛД не е имала възможност въпреки получените покани да изпрати представители в мисии за оценки на шенгенското законодателство в областта на защитата на личните данни. Отделено е обаче специално внимание на актуализирането на раздела „Шенгенско пространство“ на институционалния сайт. Акцентът в предоставената информация е върху упражняването на правата на физическите лица и защитата на личните данни в Шенгенската информационна система.

По линия на амбицията на КЗЛД да се подготви за осъществяване на проверки относно обработването на лични данни в националните звена по Регламент (ЕС) 2019/816 на Европейския парламент и на Съвета от 17 април 2019 г. за създаване на 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 и за изменение на Регламент (ЕС)

2018/1726 и Регламенти 2019/817 (Оперативна съвместимост) следва да се отбележи, че работата по системата *ECRIS-TCN* за създаване на централизирана система за установяване на държавите членки, разполагащи с информация за присъди срещу граждани на трети държави и лица без гражданство, не е напълно финализирана. Поради тази причина през отчетния период въпросната система не е била обект на проверка от страна на КЗЛД.

Въпреки амбициите на Европейската комисия (ЕК) за бързо придвижване на пакет от документи, надграждащи правилата на Общия регламент относно защитата на данните (ОРЗД), в рамките на 2021 г. не са приети регламентите относно Електронна неприкосновеност, Актът за управление на данните, Актът за дигиталните услуги и Актът за дигиталните пазари. На етап обсъждане към края на отчетния период остава и регламентът относно Изкуствения интелект. Въпреки забавянето в графика по приемането на тези документи КЗЛД участва активно в различни формати, които подпомагат формирането на българската позиция по всеки един от посочените проекти.

При отчитане на натрупаната практика на Комисията и на приетия от Европейския комитет по защита на данните (ЕКЗД) през 2021 г. Проект на Насоки за прилагането на чл. 62 от ОРЗД (съвместни операции на надзорните органи) и Насоки 01/2021 относно уведомяването за нарушение на сигурността на личните данни през изминалата година КЗЛД е приела изменение и допълнение на Инструкцията за практическото осъществяване на надзорната дейност на КЗЛД и на Приложение №1 към нея – Методика за определяне нивото на риска при нарушения на сигурността на личните данни.

Осъществяването на надзорните функции на Комисията винаги е обвързано с наблюдение и съответен текущ анализ на добри практики или несъответствия при реализирането на защитата на личните данни в една или друга сфера на обществените отношения. В резултат на такъв текущ анализ и наблюдение Комисията констатира повишен брой нарушения на сигурността на личните данни при предоставянето на пощенски и куриерски услуги, които в цялост съставляват и нарушения на пощенската сигурност, регламентирана от Закона за пощенските услуги (ЗПУ). В тази връзка КЗЛД е сезирала Комисията за регулиране на съобщенията (КРС) с искане за институционално съдействие, изразяващо се в допълнителни проверки от страна на КРС по ЗПУ във връзка с нарушения на пощенската сигурност.

По линия на целите, свързани с информационно-разяснителната дейност на КЗЛД, през 2021 г. е разработен цялостен обучителен материал „Действия на администраторите на лични данни при настъпване на нарушение на сигурността на личните данни – чл. 33 и чл. 34 от Регламент (ЕС) 2016/679“. Същият е публикуван на интернет страницата на КЗЛД в рубриката „Полезна информация“. В този разяснителен материал са описани подробно

последователността на действия, които следва да се предприемат от администраторите на лични данни (АЛД)/обработващите лични данни (ОЛД): случаите, в които се изисква уведомяване на надзорния орган, респ. – и на засегнатите субекти на данни; минималното съдържание на уведомлението до надзорния орган; водене на отчетност в случаите на нарушения на сигурността, и по-специално, документиране на настъпили нарушения на сигурността на данните. В допълнение чрез дистанционна платформа с предварително регистрирани участници Комисията е провела онлайн обучение на тема „Какво да правим при изтичане на информация?“. Разгледани са действията на всички участници в системата за защита на личните данни при настъпване на нарушение на сигурността на данните – администратори, обработващи, КЗЛД, физически лица.

В продължение на дългогодишното успешно сътрудничество между КЗЛД и Министерството на образованието и науката (МОН) по инициатива на Комисията е поставен нов фокус върху информационно-разяснителната дейност към децата в училищна възраст. В резултат на обменена официална кореспонденция и проведени срещи между ръководствата на двете институции от КЗЛД е поет ангажимент за разработване на подходящо информационно-обучително съдържание по ключови въпроси в областта на защитата на личните данни, специално насочено към ученици в гимназиален етап. МОН е изразило готовност за разпространение на изготвените от Комисията информационни материали до училищата в цялата страна, като е обсъдена възможността темите да бъдат представени на вниманието на учениците в рамките на провеждания „час на класа“ и да бъдат публикувани в е-библиотеката на учителите. Към края на отчетния период в КЗЛД е извършен подбор на видеоклипове, подходящи за ученици в посочената възрастова категория, вкл. на англ. език, които могат да бъдат ползвани както в часа на класа, така и като елемент от чуждоезиковата подготовка на децата при проявен интерес от учителите по английски език. Същинското изпълнение на информационно-разяснителната дейност, насочена към деца, остава за 2022 г. като част от инициативите, които КЗЛД планира по повод 20-ата годишнина от създаването си.

Заложеният за 2021 г. приоритет за осигуряване на електронни административни услуги, както и осъвременяване на визията на интернет страницата на КЗЛД остава актуален и за следващия отчетен период.

III. ЗАЩИТА НА ПРАВАТА НА СУБЕКТИТЕ НА ДАННИ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ИМ ДАННИ

1. Производства по разглеждане на жалби и искания.

В изпълнение на правомощията си по Регламент (ЕС) 2016/679 и Закона за защита на личните данни Комисията за защита на личните данни разглежда жалби, подадени от физически лица. Производството е административно по своя характер, като освен специалните норми на ОРЗД и ЗЗЛД, касателно компетентността на КЗЛД и сроковете за сезиране, приложение намират и общите норми на Административнопроцесуалния кодекс, същите прилагани субсидиарно, в това число принципите на законност, безпристрастност, служебно начало, равенство на страните, истинност, достъпност, публичност и прозрачност, като гаранция за справедлив административен процес. Процесът на събиране на доказателствата и анализ на изразените от страните в производството становища често пъти не е кратък, но е задължителен и предхожда разкриването на обективната истина, на която се основават актовете, издавани от Комисията за защита на личните данни.

Производството започва по инициатива на субекта на данни или упълномощено от него лице и приключва с решение на КЗЛД, което има характер на индивидуален административен акт, подлежащ на двуинстанционен съдебен контрол. В производството по разглеждане на жалби от КЗЛД не се дължат такси и в тази връзка възможността за защита е достъпна за всяко физическо лице.

За да упражни правомощията си, Комисията следва да бъде валидно сезирана от физическото лице, чиито права са нарушени. Когато КЗЛД не се сезира лично от физическото лице, то подателят на жалбата следва да е надлежно упълномощен. В противен случай искането ще бъде разгледано като сигнал. Във всеки етап на административното производство лицето може да оттегли искането си и да десезира КЗЛД.

Субектите на данни разполагат с няколко алтернативни възможности за сезиране на КЗЛД: писмените искания се подават в деловодството на Комисията, с писмо, по факс, по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги или чрез системата за сигурно електронно връчване.

Искането следва да съдържа: данни за жалбоподателя – имена, адрес за кореспонденция и постоянен адрес (за определяне на местната подсъдност по чл. 133 от АПК), телефон за връзка, електронен адрес (при наличие), естеството на искането, дата на узнаване на нарушението, пасивно легитимирана страна, дата и подпис. При сезиране по електронен път жалбата трябва да бъде подписана с квалифициран електронен подпис, респективно подадена чрез системата за сигурно електронно връчване.

Анализ на постъпилите през 2021 г. жалби сочи, че предпочитан начин за сезиране на КЗЛД остава използването на пощенски и куриерски услуги. Единици са жалбите, депозирани лично в деловодството на КЗЛД или подадени по факс. Увеличават се жалбите, постъпили чрез системата за сигурно електронно връчване, и тези, подадени по електронен път на имейла на КЗЛД. Прави впечатление обаче големият брой жалби, подадени на имейла на КЗЛД без квалифициран електронен подпис, което е предпоставка за тяхната нередовност и забавяне на развитието на производството, респективно неговото прекратяване, в хипотезата на неизпълнени указания по потвърждаване на жалбата в законоустановените срокове.

Комисията не разглежда анонимни искания. Не се разглеждат и жалби, при съставянето на които е използвана латиница или друга графична система, различна от кирилицата (освен ако не са написани на език, различен от българския). Извън компетентността на КЗЛД са жалби, касаещи обработване на лични данни от съда, прокуратурата и следствието при изпълнение на функциите им на органи на съдебната власт, като извън правната регулация на ОРЗД и ЗЗЛД, респективно извън правомощията на КЗЛД, е и обработването на лични данни от физическо лице в хода на чисто лични или домашни занимания, както и обработването на данни за починали лица освен в случаите по чл. 25е от ЗЗЛД. Претенциите за присъждане на обезщетение също са извън компетентността на Комисията, като съгласно нормата на чл. 39, ал. 2 от Закона за защита на личните данни субектът на данни може да претендира обезщетение за претърпени от него вреди вследствие неправомерно обработване на лични данни само по съдебен ред.

Предпоставка за допустимост на искането и упражняване на правомощията на КЗЛД е сезирането ѝ в рамките на разписаните в закона преклузивни срокове – 6 месеца от узнаване на нарушението, но не по-късно от две години от извършването му – за нарушения, извършени след 02.03.2019 г. За нарушения, извършени преди 02.03.2019 г., срокът за сезиране на КЗЛД е съответно една година от узнаване на нарушението, но не по-късно от 5 години от извършването му. Предпоставки за допустимост на искането са и наличието на правен интерес на искателя, липсата на влязъл в сила административен акт със същия предмет и страни, липсата на висящо административно производство със същия предмет пред същия орган и с участието на същата страна, независимо дали е във фазата на издаване или оспорване, наличието на въпрос от компетентност на друг орган, когато актът не може да бъде издаден без предварителното решаване на този въпрос и дееспособност на субекта на данни.

Жалбите, удовлетворяващи изискванията за редовност и допустимост, се разглеждат по същество в открито заседание на КЗЛД с възможност за участие на страните и техните

процесуални представители. Във всеки етап на производството страните могат да сключат споразумение.

С решението си по същество на жалба КЗЛД може да остави жалбата без уважение като неоснователна – когато не се установи нарушение на правата на жалбоподателя, а при основателна жалба следва да упражни някое от предвидените в чл. 58, §2 от Регламент (ЕС) 2016/679 корективни правомощия:

а) да отправя предупреждения до АЛД или ОЛД, когато има вероятност операции по обработване на данни, които те възнамеряват да извършат, да нарушат разпоредбите на настоящия регламент;

б) да отправя официално предупреждение до АЛД или ОЛД, когато операции по обработване на данни са нарушили разпоредбите на настоящия регламент;

в) да разпорежда на АЛД или ОЛД да изпълни исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;

г) да разпорежда на АЛД или ОЛД да съобрази операциите по обработване на данни с разпоредбите на настоящия регламент и ако е целесъобразно, това да стане по указан начин и в определен срок;

д) да разпорежда на АЛД да съобщава на субекта на данните за нарушение на сигурността на личните данни;

е) да налага временно или окончателно ограничаване, в т.ч. забрана, на обработването на данни;

ж) да разпорежда коригирането или изтриването на лични данни, или ограничаването на обработването им съгласно чл. 16, 17 и 18, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно чл. 17, §2 и чл. 19;

и) да налага административно наказание „глоба“ или „имуществена санкция“ съгласно чл. 83 в допълнение към мерките, посочени в настоящия параграф, или вместо тях в зависимост от особеностите на всеки отделен случай;

й) да разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация.

Нормативно установена е възможността за кумулативното налагане на административно наказание „глоба“ и/или „имуществена санкция“ в допълнение към наложена принудителна административна мярка, каквито по същество са тези по буква „а“, „б“, „в“, „г“, „д“, „е“, „ж“ и „й“ от Регламента.

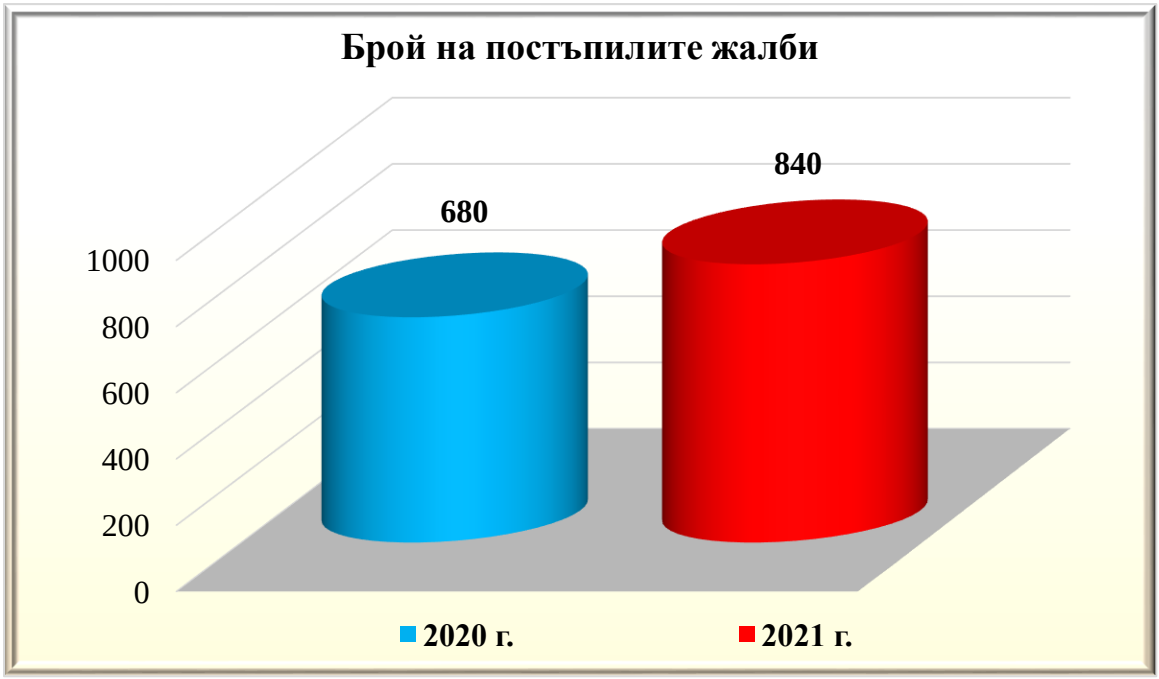
Законодателят допуска отклонение от производството. Съгласно чл. 57, §1, буква „е“ от Регламент 2016/679 всеки надзорен орган, в случая КЗЛД, следва да разглежда жалби,

подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждането на жалбите и развитието на производството е процесуално доразвита и във вътрешното законодателство – в чл. 38, ал. 4 от ЗЗЛД, – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията да бъде оставена без разглеждане. В практиката си досега Комисията не е прилагала хипотезата на прекомерност, но броят на жалбите, оставени без разглеждане като очевидно неоснователни, расте. Приложението на института на очевидната неоснователност е в рамките на оперативната самостоятелност на КЗЛД и е израз на принципа на бързина и процесуална икономия в административното производство в хипотези, в които фактическата обстановка е безспорно установена и не е спорна между страните.

2. Статистика и анализ на постъпилите в КЗЛД жалби.

През 2021 г. КЗЛД е сезирана с над 840 жалби, подадени от физически лица, с твърдения за нарушения при обработване на лични данни и упражняване на права. Забелязва се чувствително увеличаване на броя жалби в сравнение с предходната, 2020 г., когато броят на жалбите е 680.

Съотношението между подадените през 2020 и 2021 г. жалби е дадено в следната графика (фиг. 1):



Фиг. 1

На този фон се запазва тенденцията подадените през 2021 г. жалби да 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, а също и неиндивидуализирани от жалбоподателите ответни страни, най-често администратори на електронни сайтове – обстоятелство, което изисква и сътрудничество с органите на МВР за установяване на последните. Фактическата и правна сложност на казусите налага провеждането на повече от едно открито заседание, допускане на експертизи, събиране на гласни доказателства, служебно събиране на писмени доказателства, извършване на проверки за установяване на относимите факти и обстоятелства, служебно конституиране на страни и сътрудничество с други надзорни органи, както и междуинституционално взаимодействие. В тази връзка и в съответствие със служебното начало за поредна година може да се отчете успешно междуинституционално взаимодействие/сътрудничество между Комисията, от една страна, и Националната агенция за приходите (НАП), Централната избирателна комисия (ЦИК), Националния институт по криминалистика, Изпълнителна агенция „Главна инспекция по труда“, органите на МВР и Прокуратурата, от друга.

Като отрицателна тенденция в производствата, влияеща върху изхода им, все по-често се забелязва, че въпреки дадени от КЗЛД изрични указания за разпределяне на доказателствената тежест в процеса жалбоподателите не представят доказателства за твърдяното от тях нарушение. Липсата на процесуална активност от тяхна страна невинаги може да бъде компенсирано от служебното начало, доколкото страните следва да окажат 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 (чл. 36, ал. 2 от АПК).

Секторите на дейност на АЛД, срещу които най-често са постъпвали през 2021 г. жалби от физически лица, са следните:

Видеонаблюдение	196	жалби
Банки и кредитни институции	64	жалби
Държавни органи	57	жалби
Телекомуникации	51	жалби
Физически лица	51	жалби
Политически субекти	46	жалби
Здравеопазване	29	жалби
Медии	22	жалби
Трудови и осигурителни услуги	12	жалби
Застраховане	9	жалби
Образование	4	жалби

Наблюдава се тенденция към драстично увеличаване на жалбите срещу осъществявано видеонаблюдение – през 2021 г. техният брой расте до 196. Този сектор запазва тенденцията си от няколко години за увеличаване на броя на жалбите. За 2017 г. жалбите, подадени в КЗЛД с твърдение за неправомерно обработване на лични данни чрез системи за видеонаблюдение, са били 32 броя, за 2018 г. броят им се доближава до 84 жалби, през 2019 г. е 102, а за 2020 г. секторът се превръща във водещ по брой жалби – общо 159, тенденция, която продължава и през 2021 г., когато броят на жалбите се увеличава и достига до 196.

Както и досега, видеонаблюдението може условно да се раздели на следните категории:

• Видеонаблюдение, осъществявано в жилищни сгради в режим на етажна собственост (ЕС): в тези случаи администраторът следва да получи съгласието на останалите живущи в етажната собственост, като за целта трябва да бъде взето Решение на проведено общо събрание на ЕС с 51 на сто от присъстващите. Дори да има такова решение, обхватът на видеонаблюдението трябва да бъде ограничен в рамките на общите части на жилищната сграда, като не трябва да се заснемат публични места – улици, тротоари, затревени площи, както и други сгради.

• Видеонаблюдение на имоти в режим на съсобственост: администраторът трябва да ограничи обхвата на видеозаснемане само до частта от имота, която е определена за ползване от него, а ако имотът не е поделен условно, се взема под внимание дали легитимният интерес на охраняващия има превес над интереса на субекта на данни.

• Видеонаблюдение между съседи, обитаващи съседни имоти: администраторът трябва да ограничи обхвата на видеозаснемане само до рамките собствения си имот, като не трябва да заснема публични места – улици, тротоари, затревени площи, както и чужди имоти.

• Видеонаблюдение на работното място: в случаите, в които администраторът, в качеството си на работодател, е инсталирал системи за видеонаблюдение с цел контрол на работния процес, следва да уведоми служителите за извършване на такова видеонаблюдение. От съществено значение в такива случаи е да се извърши преценка и да се балансират легитимните интереси на администраторите и правата и свободите на субектите на данни. В обхвата на видеонаблюдение не трябва да попадат стаи за почивка, санитарни помещение, помещения за преобличане.

Голяма част от жалбите касаят видеонаблюдение на обществени места – улици, тротоари, зелени площи. Практиката на КЗЛД и резултатите от контролната дейност

констатират все по-често използването на „бутафорни“ камери, имитиращи осъществяване на видеонаблюдение, поставени с цел превенция срещу противоправни действия и евентуални криминални прояви.

Разглеждането на казуси, свързани с обработване на лични данни чрез изградени системи за видеонаблюдение, отнема сериозен финансов и експертен ресурс на КЗЛД. Отчита се липсата на уреждане на обществените отношения извън тези по Закона за частната охранителна дейност, свързани с изграждане и поддържане на системи за видеонаблюдение от физически и юридически лица с цел защита на имоти. Тежест представлява и липсата на териториални административни звена на КЗЛД, което налага разходване на средства и командироване на експерти за извършване на проверки на място. Впечатление прави обстоятелството, че в голяма част казусите са свързани с обострени междуличностни конфликти.

Ръст бележат жалбите, подадени срещу банки и дружества, предлагащи кредитни услуги. През 2020 г. техният брой е 49, а през 2021 г. достига 64. В тази категория жалби попадат освен твърдения за неправомерно предоставяне на лични данни за събиране на задължения от физическите лица, така и твърдения, свързани с употребата на лични данни за отпускане на кредити, без същите да са поискани и/или усвоени, особено такива, сключени в електронна среда посредством кандидатстване и отпускане на кредити по електронен път, като прави впечатление високият размер на отпуснатите средства. Нужно е да се посочи, че само по три от жалбите средствата, които са отпуснати, са в размер общо на 360 000 лв. В тази връзка се налага да бъде извършен анализ на необходимостта от законодателни промени с цел минимизиране на рисковете при индивидуализацията на физическите лица при отпускане на кредити.

Незначителен ръст се забелязва по отношение на жалбите, подадени срещу администратори в телекомуникационни сектор. През 2020 г. подадените жалби са 49, а за 2021 г. броят им е 51. Секторът остава сред водещите, срещу които най-често постъпват оплаквания, като предметът на жалбите, с които е сезирана КЗЛД, остава идентичен с жалбите, подавани в предходните години – предоставяне на лични данни за събиране на задължения, произтекли от сключени договори и електронни съобщения, сключване на договор за услуги без знание и съгласие на лицето и без реално същото да е ползвател на предоставената услуга.

Констатирана е тенденция на увеличаване на броя на жалбите, подадени срещу физически лица, като броят им през 2021 г. достига до 51 и се изравнява с броя на жалбите, подадени в сектор „Телекомуникация“. Жалбите са насочени предимно срещу разпространение на лични данни в социални мрежи. Предмет на тази категория жалби е и

ползването на лични данни за реализиране на конституционно гарантирани права като правото на съдебен процес и подаването на искови молби и жалби пред съдебните органи, в които се съдържат данни, безспорно индивидуализиращи физическите лица, срещу които са подадени, в това число и единни граждански номера.

Драстично е увеличението на жалбите срещу политически субекти. Докато през 2020 г. подадените жалби в този сектор са 2, то през 2021 г. броят им е 46. Причина за последното може да се търси в динамичната изборна година и проведените на 04.04.2021 г., 11.07.2021 г. и на 14.11.2021 г. избори, разпознаваемостта на КЗЛД като надзорен орган в сферата на защита на личните данни и гласуваното доверие за провеждане на справедлив и прозрачен административен процес. Забелязва се промяна в политическите субекти, както политически партии, така и коалиции от партии, срещу които са подадени жалбите, като освен субектите, срещу които са подавани жалби и в предходни години, през 2021 г. в КЗЛД постъпват и жалби срещу политически субекти, срещу които до момента не е имало оплаквания по отношение на обработване на лични данни в изборния процес. Както и досега, по-големият брой жалби касаят предимно злоупотреба с лични данни на жалбоподателите чрез включването им в списък на лицата, подкрепящи регистрацията на политически субект за участие в изборния процес. Макар и единични, налице са и жалби, съдържащи твърдения за злоупотреба с лични данни за регистриране на лица като членове на секционни избирателни комисии.

Отчита се и увеличение на жалбите, подадени в сектор „Здравеопазване“. През 2021 г. броят им е 29, като основен предмет на жалбите са твърдения за предоставяне на трети лица на чувствителна информация, касаеща здравния статус на субекта на лични данни, както и непроизнасяне по заявления за достъп до лични данни.

На този фон през 2021 г. се наблюдава намаляване на жалбите, подадени в сектор „Трудови и осигурителни услуги“, като през 2021 г. техният брой е 12, два пъти по-малко от подадените през 2020 г. 25 жалби. По-малък е и броят на жалбите в сектор „Образование“ – от 6 жалби, подадени през 2020 г., до 4 през 2021 г.

През 2021 г. Комисията е сезирана и с по-малко жалби, подадени срещу държавни органи, от 62 през 2020 г. през 2021 г. депозираните в този сектор жалби са 57, като следва да се отбележи, че по-голяма част от подадените през 2021 г. жалби са депозирани от едно и също физическо лице. Въпреки това обаче секторът остава сред водещите по отношение на твърдения за нарушение в сферата на личните данни.

Спад бележат и жалбите, подадени срещу медии, като през 2021 г. подадените жалби са 22 на фона на 26 жалби за 2020 г., като впечатление прави относително големият процент на жалби, подадени срещу администратори на електронни медии. Основно твърденията в

този сектор са за непропорционално обработване на лични данни, разкриване на чувствителна информация, обработване на специална категория лични данни, най-вече такава, свързана със здравословното състояние, респективно здравния статус на субекта на данни, както и непроизнасяне по подадени от субекти на данни заявления за упражняване на „правото да бъдеш забравен“ или изричен отказ на администратора да удовлетвори исканията за заличаване на лични данни и преустановяване на тяхното разпространение.

От разгледаните през 2021 г. жалби преобладаващ е броят на констатираните нарушения на чл. 6, §1 от ОРЗД – обработване на лични данни без правно основание, както и обработване на личните данни в нарушение на принципите по чл. 5, §1 от ОРЗД – „законосъобразност и добросъвестност“, „свеждане на данните до минимум“, „цялостност и поверителност“ и „точност“. Констатирани са и нарушения, свързани със сигурността на данните и предприетите от администраторите технически и организационни мерки за защита на личните данни, както и такива, свързани с непроизнасяне по подадени от субекти на данни заявления за упражняване на права или произнасяне извън нормативно определените срокове. В тази връзка и най-често налаганите корективни мерки са именно за тези нарушения, като тази тенденция се запазва от 2020 г.

През 2021 г. по повод постъпили жалби са приложени следните корективни правомощия по чл. 58, §2 от Регламент (ЕС) 2016/679:

- предупреждение по буква „а“ – 2 бр.;
- официално предупреждение по буква „б“ – 14 бр.;
- разпореждане по буква „в“ – 6 бр.;
- разпореждане по буква „г“ – 83 бр.;
- забрана на обработването на данни по буква „е“ – 1 бр.;
- разпореждане по буква „ж“ – 1 бр.;
- имуществени санкции/глоби по буква „и“ – 38 бр.

Предвид спецификата на някои от нарушенията в допълнение към корективните мерки, най-често по тези по буква „г“, Комисията е наложила на администраторите и/или обработващите лични данни и административни наказания „имуществена санкция“.

Размерът на наложените през 2021 г. глоби и имуществени санкции в производството по чл. 38 от ЗЗЛД е в общ размер на 112 150 лв. Санкциите варират от 100 лв. (за нарушение на чл. 12, §3 от ОРЗД) до 30 000 лв. (за нарушение на чл. 5, §1, буква „а“ и „е“ и §2 от ОРЗД). В процес на принудително събиране от НАП към 31.12.2021 г. са санкции, наложени с Решения на КЗЛД, в размер на 568 209 лв., като през 2021 г. е събрана сума в размер на 89 048,30 лв. През 2021 г. доброволно са платени глоби и имуществени санкции в размер на 458 695 лева.

Водещи за определяне на размера на наложените имуществени санкции/глоби са естеството, тежестта и продължителността на нарушението, целта на съответното обработване, броят на засегнатите субекти на данни и степента на причинената им вреда, категориите лични данни, засегнати от нарушението, действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни, предишни нарушения на санкционираното лице, както и дали нарушителят е физическо или юридическо лице, респективно микро-, малко или средно предприятие. Определящ за размера на санкциите е и приложимият материален закон.

Съотношението между упражнените корективни правомощия по чл. 58, §2 от ОРЗД е дадено в следната графика (фиг. 2):

Фиг. 2

С оглед крайното решение на КЗЛД произнасянията по жалби са, както следва:

– по основателност на жалби – 257 решения. От тях за основателни са приети 142 жалби, а за неоснователни – 115;

– за спиране на административно производство поради наличие на друго, образувано пред органите на МВР или прокуратурата – 7 решения;

– 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;

– очевидна неоснователност – 54 решения.

Оттеглените жалби са 4, с което КЗЛД на практика е била десезирана.

По 2 жалби, подадени от български граждани срещу администратори с основно място на установяване извън пределите на Република България, са стартирани процедури по международно сътрудничество с водещи надзорни органи съответно надзорните орган във Федерална република Германия и Нидерландия и засегнат надзорен орган КЗЛД.

3. Специфични казуси и практика на КЗЛД.

Що се касае за специфични казуси по жалби, постъпили или разгледани през отчетния период, могат да се посочат следните случаи:

3.1. През 2021 г. КЗЛД е постановила решение, с което е наложила имуществена санкция на териториален орган на изпълнителната власт – кмет на кметство, за това, че е осъществил неправомерен достъп до лични данни, съдържащи се в НБДН, за свои лични интереси/цели.

Решението е постановено по повод постъпила жалба от засегнатото лице с твърдения за осъществен неправомерен достъп до негови лични данни, съдържащи се в НБДН, и за тяхното разпространение.

Въпросният достъп до базата данни е предоставен на кмета на кметството от ГД ГРАО към МРРБ по силата на закона с оглед изпълняваната от него длъжност, и по-конкретно, съобразно чл. 46, ал. 1, т. 6 от Закона за местното самоуправление и местната администрация, чл. 4, чл. 35, чл. 106, ал. 1, т. 2 от Закона за гражданското състояние, глава VI, раздел III – чл. 158 и сл. от Наредба №РД-02-20-9 от 21 май 2012 г. за функциониране на единната система за гражданска регистрация, чл. 2 от Наредба №РД-02-20-6 от 24 април 2012 г. за издаване на удостоверения въз основа на регистъра на населението въз основа на подадено заявление.

Във връзка с разследването на предмета на жалбата е изискано съдействието от трети, неучастващи в производството лица – мобилни оператори, Софийската районна прокуратура и ГД ГРАО.

В хода на производството е установено, че кметът на кметството е осъществил достъп до НБДН (предоставена информация от ГД ГРАО), възползвайки се от служебното си положение и дадените права за достъп до НБДН, като единствено длъжностно лице по

гражданското състояние в населеното място, в нарушението на принципа на законосъобразността съгласно чл. 5, §1, буква „а“ от Регламент (ЕС) 2016/679

Причината за извършените действия е междуличностен конфликт между жалбоподателя и кмета на кметството, касаещ неучастващо в производството лице от женски пол.

Решението не е обжалвано и е влязло в законна сила.

3.2. През отчетния период КЗЛД постановява решение, с което отхвърля жалбата на адвокат срещу две електронни медии по повод публикувани материали на собствените на дружествата онлайн платформи във връзка с отнет талон за безплатно паркиране на лицето, сезирало КЗЛД.

Въпросните материали предоставят информация за това, че лице, което има качеството на адвокат и което през 2019 г. е регистрирано и като кандидат за кмет, е декларирало в общината като свой настоящ адрес такъв, в който се помещава адвокатска кантора. Тези обстоятелства са установени от общината и са предприети мерки по заличаване на този адрес и за отнемане на талона за безплатно паркиране издаден въз основа на адресната регистрация на лицето.

В хода на проверката е изискано съдействието на трети, неучастващи в производството лица (съответната адвокатска колегия и община).

В резултат на проведеното разследване е установено, че процесната обработка на личните данни на жалбоподателя е извършена за журналистически цели и при спазване на принципа на законосъобразността.

До този извод Комисията стига след извършена преценка относно законосъобразността на обработката въз основа на формулираните от Европейския съд по правата на човека и Съда на ЕС критерии с отчитане на обстоятелствата по конкретния случай.

С решението КЗЛД отчита важната роля, която медиите играят в демократичното общество, и по-специално, че същите имат задачата да разпространяват информация и идеи от обществен интерес, но и че самата аудитория има право да ги получава, и в разглежданият случай превес следва да се даде в полза на тези права, като приема, че свободата да се разпространява информация е оправдана, за да се гарантират демократичността на обществените процеси и възможността на гражданите за изграждане на мнение и позиция относно проблеми, касаещи обществен интерес.

Решението не е обжалвано, същото е влязло в законна сила.

Следва да се отбележи, че през 2021 г. са влезли в сила две решения, постановени от КЗЛД по жалби, подадени от същия жалбоподател срещу електронни медии. Предмет на жалбите са твърдения за незаконосъобразно обработване на личните данни посредством публикуване на снимки с видим регистрационен номер на автомобил към журналистическа статия.

В хода на административните производства и след анализ на доказателствата по преписките Комисията е приела, че обработването на лични данни на жалбоподателя, съдържащи се в публично представените фотографски изображения, носещи лични данни, име на лицето, професия, собственик на определено МПС с посочена марка, модел и регистрационен номер, е в унисон със съдържанието на отправена до неограничен кръг потребители информация за събития от обществен интерес и само по себе си не съставлява нарушение на правото на личен живот. Комисията е приела, че посочените категории лични данни са обработени от администратори на лични данни с цел информиране на обществото за дадено поведение на субекта на данни в качеството му на публична личност – кандидат за кмет. В тази връзка и доколкото обработването е единствено за журналистически цели и, публикувайки статията в електронни медии администраторите, са упражнили правото на свобода на словото в съответствие с правото да се търси и получава свободно информация за събития от обществен интерес, поради което обработването не е прекомерно и е съобразено с принципа по чл. 5 от ОРЗД личните данни да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“). По изложените съображения Комисията е оставила жалбите без уважение като неоснователни.

Постановените от Комисията две решение са обжалвани от субекта на данни и са потвърдени като правилни и законосъобразни от съда, като аргументите на КЗЛД за неоснователност на жалбите са изцяло споделени както от първа инстанция, така и от Върховния административен съд.

3.3. Друг интересен казус, по който КЗЛД е сезирана, касае жалба, подадена срещу териториален орган на изпълнителната власт – кмет на кметство, в качеството му на работодател на жалбоподателя, и лечебно заведение с твърдения за неправомерно обработване на чувствителни лични данни, касаещи здравословното състояние на лицето.

Твърди се, че кметът на кметството е разпространил получена от лечебното заведение информация, касаеща пребиваване на жалбоподателя в лечебното заведение, поставена диагноза, свързана с психичното му здраве, и периоди на лечение.

Установено е, че кметът на кметството е изискал по официален ред от лечебното заведение лекарска експертиза, касаеща жалбоподателя, негов служител, в отговор на което копие на изискания документ е предоставен.

Установено е, че са постъпили оплаквания от жители на селото, адресирани до кмета, относно агресивно поведение и отсъствие от работа на жалбоподателя. Кметът на кметството по закон съгласно разпоредбата на чл. 46, ал. 1, т. 6 от ЗМСМА води регистрите на населението и за гражданското състояние и изпраща актуализационни съобщения до ЕСГРАОН, има и задължения по опазване на обществения ред. За кмета е налице правомощие за подаване на искане (молба) до прокуратурата за започване на производство по задължително настаняване и лечение, която от своя страна има правомощие по чл. 157 от Закона за здравето (ЗЗдр). Изисканата от кмета и съответно получена информация касателно здравословното състояние на жалбоподателя се явява обработване на лични данни в нарушение на принципа на чл. 5, §1, б. „а“ от Регламента.

Доколкото жалбоподателят е посещавал лечебното заведение като пациент на болницата, е налице правно основание за обработване на личните му данни, включително и специални такива. По отношение на предоставянето на специални категории лични данни от лечебното заведение на работодателя на лицето обаче се констатира, че се касае за допълнително обработване на лични данни, касаещи здравословното състояние на лицето, за цели, различни и несъвместими с първоначалните конкретни, изрично указани и легитимни цели, за които са събрани, при което е нарушен принципът за ограничаване на целите на обработването чл. 5, §1, б. „б“ във вр. с чл. 9, §1 от Регламент 2016/679.

Жалбата е обявена за основателна както по отношение на лечебното заведение, така и по отношение на кмета на кметството, като и на двамата администратори са наложени имуществени санкции в размер от 500 лв., които са платени.

Решението не е обжалвано и е влязло в законна сила.

3.4. През 2021 г. КЗЛД е сезирана и с жалба, подадена срещу топлофикационно дружество и частен съдебен изпълнител, с твърдения за обработване на лични данни без основание, доколкото жалбоподателката не е абонат на дружеството и не притежава собственост по отношение на предоставена на конкретен адрес услуга от дружеството, за която се претендират заплащане на задължения.

В производството не е спорно, че жалбоподателката не е абонат на дружеството, не е имала и няма облигационни отношения с него, доколкото не притежава вещно право на собственост върху топлоснабден имот, за който се претендират парични задължения.

Установено е, че на жалбоподателката е наложен запор в хода на изпълнително дело, образувано пред частен съдебен изпълнител по молба на дружеството въз основа на изпълнителен лист, издаден от Софийския районен съд. В изпълнителния лист са посочени три имена и ЕГН на двамата длъжници, съпрузи. В хода на производството и след проверка от страна на дружеството е констатирано, че дружеството погрешно е посочило ЕГН на жалбоподателката в подадена до СРС молба по чл. 410 от ГПК, въз основа на която е изпълнителният лист срещу лицето. След сезиране на КЗЛД от дружеството констатират допусната грешка при обработване на лични данни на жалбоподателката поради съвпадение на имената на жалбоподателката с тези на лице, имащо задължение за топлинна енергия. Предприети са действия за вдигане на запора.

Предвид събраните по преписката доказателства Комисията приема, че личните данни на жалбоподателката са обработени от ЧСИ законосъобразно и добросъвестно в изпълнение на правомощията му по Закона за частните съдебни изпълнители, но незаконосъобразно от топлоснабдителното дружество.

Жалбата е оставена без уважение като неоснователна по отношение на ЧСИ. По отношение на дружеството е обявена за основателна за нарушение на чл. 6, §1 от Регламент (ЕС) 679/2016. Наложена е имуществена санкция в размер на 2000 лв., както и принудителна административна мярка в съответствие с разпоредбата на чл. 58, §2, б. „г“ от ОРЗД, доколкото нарушението е поредно за дружеството – издадено е разпореждане на администратора на лични данни да въведе допълнителни правила за идентификация на физическите лица преди образуване на изпълнителни производства.

Решението не е обжалвано и е влязло в законна сила.

3.5. През отчетния период КЗЛД се произнася по жалба с изложени твърдения за неправомерно обработване на личните данни на жалбоподателя, свързани със здравословното му състояние, а именно изнесена в две електронни медии информация, че е болен от КОВИД-19. Жалбоподателят твърди, че информация за заболяването му ведно с негово изображение и имена е публикувана в две статии със сензационни заглавия.

В хода на производството твърдяната от жалбоподателя фактическа обстановка е безспорно установена. Констатирано е, че в процесните статии се съдържат данни на жалбоподателя в обем от изображение, две имена (собствено и фамилия), информация за неговата длъжност – общински съветник, и заболяване от КОВИД-19, обстоятелства, които са верни и отговарят на обективната истина. Констатирано е, че статиите са публикувани в поддържани от ответниците в административното производство две електронни медии – новинарски уебсайтове, като данните безспорно са обработени за журналистически цели.

Безспорно е обаче, че личните данни за здравословното състояние на жалбоподателя и заболяването от КОВИД-19 са публикувани от електронните медии без знанието и съгласието на лицето. Липсват доказателства същите да са публично оповестени от жалбоподателя или здравните органи.

При тази фактическа обстановка и при преценка на баланса между двете конкуриращи се права Комисията е достигнала до извод за допуснато от администраторите нарушение на чл. 25з от ЗЗЛД.

В конкретния случай е безспорно, че субектът на данни е публична личност и като такава се ползва с по-ниска степен на защита на личните му данни, но само и доколкото същите са относими и свързани с упражняваните от него функции на общински съветник, но не и на такива, свързани с конкретното заболяване от КОВИД-19, което не е свързано с тях. Публичните личности имат по-нисък праг на защита на личния им живот, но намесата в него е допустима само при баланс между правото на защита на неприкосновеността на личния живот и правото на свободата на изразяване и правото на информация. В конкретния случай баланс не е постигнат. Липсва преимуществен обществен интерес, какъвто твърдят медиите, от оповестяване на информацията, доколкото се касае за данни за здравословното състояние на лицето, които не са свързани с упражняваните от него функции на общински съветник. Разкрита е чувствителна здравна информация по смисъла на ЗЗдр.

От съдържанието на процесните статии е видно, а и от депозираните становища в производството пред КЗЛД е ясно, че акцентът на статиите е представяне на информация, че на национално съвещание на политическа партия ще присъства представител, който е бил контактен с лице, заразено с КОВИД-19. В тази връзка за здравия обществен интерес и правото на информация е ирелевантно кое е конкретното лице, констатирано с инфекция за КОВИД-19, доколкото не неговата самоличност, а фактът, че е носител на вируса, е релевантен за статията и свободата на изразяване. Информация, макар касаеща обществена фигура, не е необходима за изпълнение на задача в обществен интерес, доколкото същият би бил задоволен и без публикуване на тези данни. Доколкото обаче в статиите са публикувани лични данни за конкретното лице, се налага изводът за допуснато от администраторите нарушение на личната му неприкосновеност, доколкото тази информация в цялост и конкретика, отнесена към целта на публикацията, е несъотносима и по същество прекомерна.

Предвид събраните по преписката доказателства Комисията е приела, че и двата администратора на лични данни са допуснали нарушение на чл. 25з, ал. 1 от ЗЗЛД. Предвид констатираното нарушение и обстоятелството, че и към датата на произнасяне на КЗЛД данните за жалбоподателя са достъпни в процесните публикации, Комисията по

целесъобразност с оглед прекратяване на нарушението е издала разпореждане на администраторите по чл. 58, §2, буква „г“ от ОРЗД да съобразят операциите по обработване на личните данни с разпоредбите на ЗЗЛД и Регламента, като заличат личните данни на жалбоподателя – имена и изображение, от процесните статии.

Решението е обжалвано от един от администраторите, потвърдено е от съда и е влязло в законна сила, като са представени доказателства за изпълнението му.

4. Съдебна практика по оспорвани решения на КЗЛД.

Постановените в хода на производството по чл. 38 от ЗЗЛД решения на КЗЛД подлежат на двуинстанционен съдебен контрол по реда на АПК.

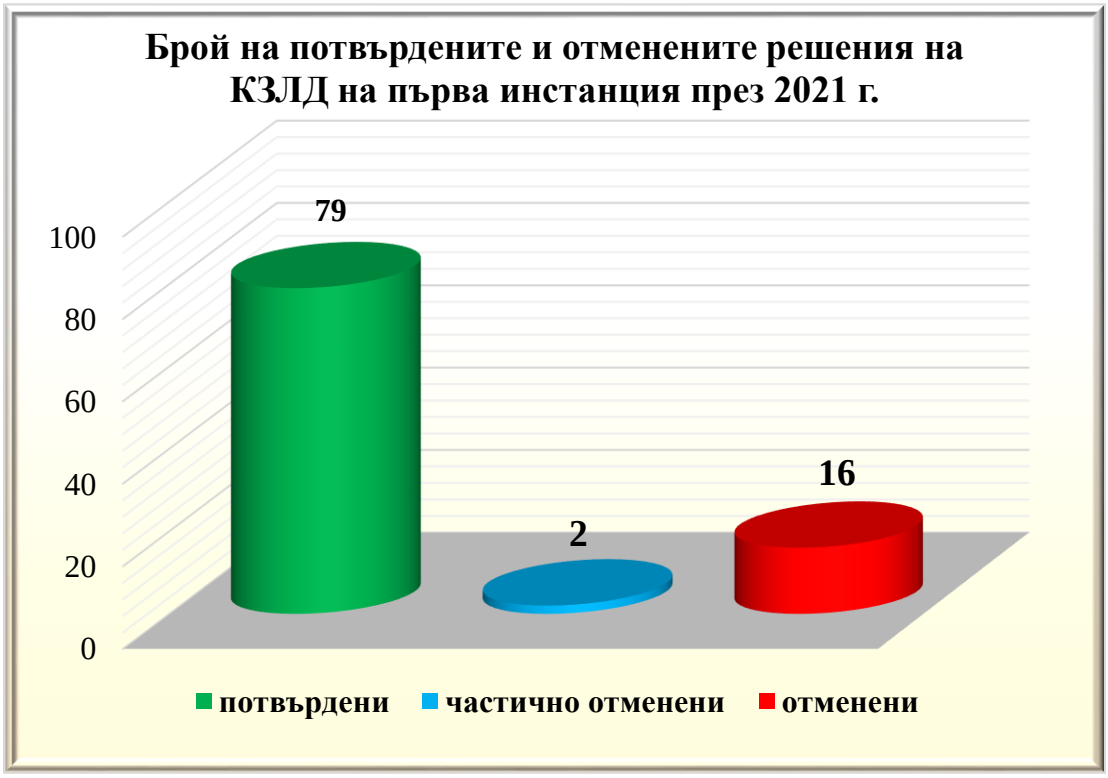
Съобразно местната подсъдност по чл. 133, ал. 1 и 2 от АПК делата се разглеждат от административния съд по постоянен адрес или седалище на посочения в акта адресат, съответно адресати. Когато посоченият в акта адресат има постоянен адрес или седалище в чужбина, споровете се разглеждат от Административен съд София-град. Когато посочените в акта адресати са повече от един и са с различен постоянен адрес или седалище, но в рамките на един съдебен район, делата се разглеждат от административния съд в района на териториалната структура на органа, издал акта. Във всички останали случаи делата се разглеждат от административния съд, в района на който е седалището на органа, в случая Административен съд София-град. Втора касационна инстанция по законосъобразност на актовете, издадени от КЗЛД в производството по чл. 38, ал. 1 от ЗЗЛД, е Върховен административен съд.

През 2021 г. са проведени над 170 съдебни заседания по дела, образувани през 2020 и 2021 г., с участие на процесуален представител на КЗЛД по оспорени на първа и втора инстанция актове на КЗЛД, постановени по реда на чл. 38 от ЗЗЛД.

През 2021 г. по жалби, подадени срещу постановени по този ред решения на КЗЛД, са образувани общо 76 първоинстанционни съдебни дела, от тях: в Административен съд София-град – 52, в Административен съд Варна – 12, Административен съд Пловдив – 3; Административен съд София (област) – 2; Административен съд Враца – 2; Административен съд Стара Загора – 2; Административен съд Смолян – 1; Административен съд Пазарджик – 1, и Административен съд Велико Търново – 1.

През 2021 г. първоинстанционният съд се е произнесъл с решения по 97 дела, включително по такива, образувани и преди 2021 г. Със 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.

На графиката е изобразен броят на потвърдените и отменените решения на КЗЛД на първа инстанция (фиг. 3):

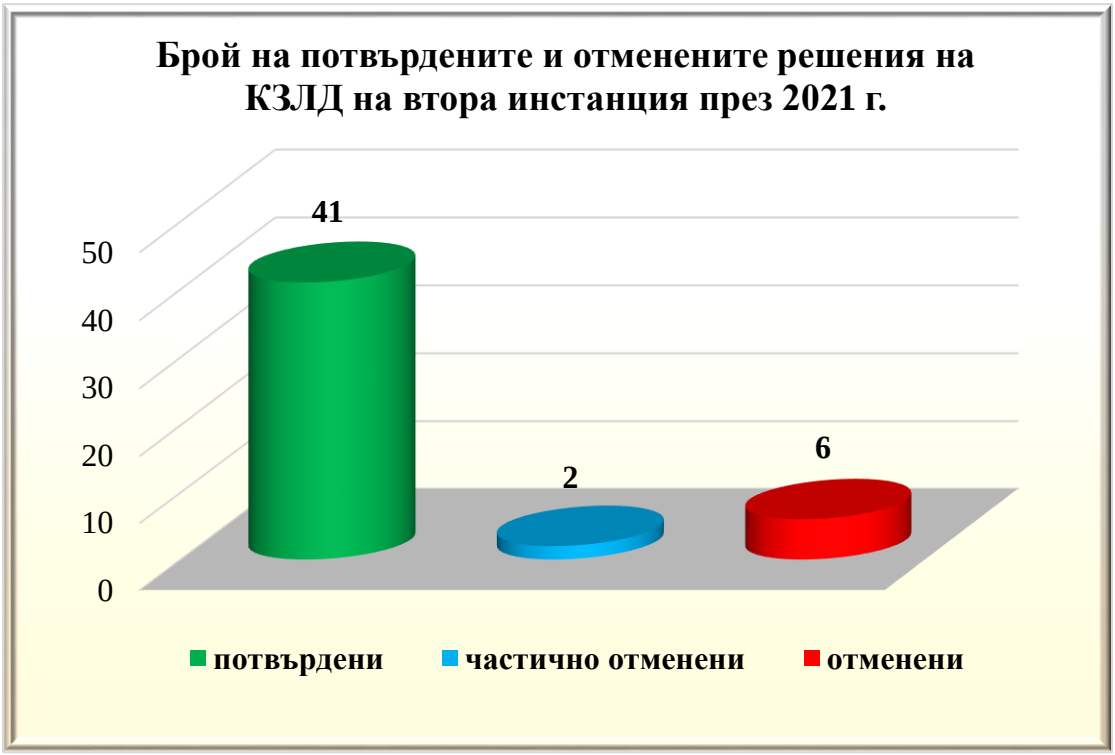


Фиг. 3

През 2021 г. пред Върховния административен съд (ВАС), като касационна инстанция, са образувани 62 дела.

През 2021 г. ВАС се е произнесъл с решения по 59 дела, в това число такива, образувани преди 2021 г., като е потвърдил 41 издадени от КЗЛД индивидуални административни акта, 2 индивидуални административни акта на КЗЛД са частично отменени или изменени в санкционната част, 6 решения на КЗЛД са отменени изцяло.

На графиката са изобразени броят на потвърдените и отменените от решения на КЗЛД на втора инстанция (фиг. 4):



Фиг. 4

5. Консултации на субекти на лични данни.

Изпълнените през отчетния период дейности по линия на консултациите на субекти на данни са под формата на писмени отговори на поставени въпроси в областта на защитата на личните данни. Неформални консултации се предоставят по линия на обслужването на институционалния телефон за устни консултации по законодателството за защита на личните данни.

През изтеклата година продължава тенденция за сезиране на КЗЛД с искания по различни теми от обществения живот както от отделни граждани, така и от широк кръг администратори. Анализът, който може да се направи по отношение на предмета на запитванията на субектите на данни, е, че темата за защита на личните данни става все по-актуална във всички сфери на съвременното общество, а проблемите, свързани със защитата на правата в тази област – все по-разпознаваеми.

Видеонаблюдението в етажната собственост е най-често обсъжданата тема и през 2021. Запитванията в тази област се фокусират върху законосъобразността на видеонаблюдението в тези случаи, като по-конкретно въпросите са свързани с процедурата по вземане на решение от общото събрание на собствениците във вход на жилищната сграда за инсталиране на система за видеонаблюдение.

Друга част от повдигнатите през 2021 г. въпроси касаят случаи, при които системите за видеонаблюдение са инсталирани в сгради, които са частна собственост, но в обхвата на камерите попадат други, съседни сгради или обществени места като тротоари, паркинги и улици. По този въпрос КЗЛД има утвърдена и трайна практика, напълно в духа на решенията на Съда на ЕС, съгласно която заснемането на публични площи надхвърля целите за охраната на собствен обект, за които обикновено се твърди, че е монтирана система за видеонаблюдение.

Друга група запитвания, касаещи видеонаблюдението, се отнасят за случаите, когато тази дейност се извършва в обществени сгради, болници, детски градини и училища. Тук фокусът на отговорите е върху необходимостта да се разграничат случаите, когато видеонаблюдението се извършва от търговец, лицензиран да извършва частна охранителна дейност, с цел осигуряване на пропускателен режим в охраняваните обекти и охрана в самия обект. Дейностите по видеонаблюдение в тези случаи се извършват в съответствие със специалните изисквания на Закона за частната охранителна дейност наред с общите изисквания на Регламент (ЕС) 2016/679. Във всеки конкретен случай КЗЛД препоръчва да се следи за наличието на условие (основание) за законосъобразно обработване на личните данни.

По традиция продължават и запитванията във връзка с извършване на видеонаблюдение на работното място от страна на работодателите, които чрез монтираните видеокамери извършват наблюдение както на своите служители, така и на клиентите си. Много често извършването на видеозапис е придружено с аудиозапис. От запитванията става ясно, че в много от случаите работниците и служителите дори не са уведомявани за извършване на такъв вид обработване на лични данни. По тази тема Комисията за защита на личните данни неведнъж е изразявала становища и е отговаряла на конкретни запитвания по тези въпроси, като основната линия, към която се придържа, е, че физическите лица, обект на видеонаблюдение, следва да бъдат уведомявани предварително за целите на извършваното по този начин обработване на лични данни, включително чрез информационни табла, поставени на видно място, за използването на технически средства за наблюдение и контрол на обекта, без да е необходимо да се уточнява тяхното местоположение. От гледна точка защитата на личните данни и доколкото по принцип видеонаблюдение и звукозапис се извършват на основание на легитимните интереси на администратора, се изисква да бъде направена преценка във всеки конкретен случай чий интерес има превес – този на работодателя (администратор на лични данни) или на физическото лице (субект на данни). В отговорите на КЗЛД се подчертава задължението на работодателя (администратор) да предоставя предварително необходимата информация,

както същата е определена в чл. 13 от ОРЗД. Съществен елемент от тази информация е тя да съдържа указание към субекта на данни относно неговите права и съответно тяхното упражняване пред надзорния орган или по съдебен ред, както и възможностите в конкретния случай. Общо правило е, че информираността включва конкретното физическо лице да знае кой и с какви цели обработва данните му, какви са конкретно обработваните данни и на какво основание се извършва обработването, на кого се предоставят данните или кои лица имат достъп до тях.

Продължават да са многобройни въпросите, които се получават в КЗЛД относно регистрацията на администраторите на лични данни – задължение, отпаднало от 25 май 2018 г., когато започва да се прилага ОРЗД. Като цяло отговорите препращат към редица разяснителни материали на официалната страница на институцията, които подробно обясняват правното положение и изискванията към администраторите на лични данни, считано от започване на прилагането на ОРЗД.

Анализът на характера на запитванията сочи, че остават все още неизяснени въпроси относно изпращането и получаването на непоискани търговски съобщения, а именно извършването на директен маркетинг, например по електронна поща. Практиката на КЗЛД в тази посока е, че осъществяването на директен маркетинг в националното ни законодателство се регламентира от Закона за електронната търговия и Закона за електронните съобщения (ЗЕС), чрез които са транспонирани разпоредбите на Директива 2002/58/ЕС. С разпоредбата на чл. 6, ал. 4 от ЗЕТ се забранява изпращането на непоискани търговски съобщения на потребители без предварителното им съгласие. В същото време съгласно чл. 261, ал. 1 от ЗЕС осъществяването на повиквания, съобщения или електронна поща със или без човешка намеса за целите на директния маркетинг и реклама се позволява само при предварително получено съгласие на потребителя. Съгласието може да бъде оттеглено по всяко време. Съгласно ал. 2 на същата разпоредба се позволява на търговеца, който е получил при търговска сделка за предоставяне на продукти или услуги данни от физически лица, които в резултат на сделката са вече клиенти, да използва тези данни за изпращане на съобщение за маркетинг и реклама на негови собствени сходни продукти или услуги, като дава възможност на всеки потребител безвъзмездно и по лесен начин:

1. да изразява несъгласие в момента на сключване на сделката;

2. да изрази несъгласие с бъдещо получаване на подобни съобщения, когато това не е направено в момента на сключване на сделката.

В първия случай, по ал. 1, основанието за обработването на лични данни е съгласието на лицето, а във втория случай, по ал. 2, директният маркетинг се осъществява на основание легитимните интереси на търговеца. И двете хипотези не противоречат на разпоредбите на

Общия регламент относно защита на данните (Регламент (ЕС) 2016/679), стига да са съобразени конкретно приложимите му изисквания. По чл. 261, ал. 1 от ЗЕС субектът на данни има възможност да оттегли съгласието си и като резултат не трябва повече да получава маркетингови съобщения.

Не са редки и запитванията във връзка със заснемане на рекламни видеоклипове от администраторите на лични данни, в които участват техни служители. Повдигат се въпроси, свързани с това как да бъдат защитени правните интереси на администратора, от една страна, и съответно как да бъдат гарантирани правата на служителите/участници във видеоклиповете в качеството им на субекти на данни, като се вземат предвид всички аспекти, включително и на трудовоправните взаимоотношения между тях. По тези казуси следва да се съобразят различни обстоятелства, но основанията за обработването на лични данни, които могат да се приложат, са или съгласието на субекта на данни, или сключено между работодателя (администратор) и служителя (субект на данни) споразумение с тази цел, което създава по-голяма правна сигурност и за двете страни. Между страните трябва да са изяснени всички параметри във връзка с публикуването и ползването на снимките и видеоклиповете, както и при какви условия и в какъв срок биха могли да се обработват, в каква зависимост са по отношение на вече съществуващите трудови отношения между тях и т.н. Двете възможности предоставят известна гъвкавост и избор на администраторите, които предприемат действия по създаването на рекламни клипове с участието на свои служители. Освен съгласието на субектите КЗЛД препоръчва за по-голяма правна сигурност във връзка с публикуването и използването на заснетия видеоклип, свързани с дейността на работодателя, между работодател и служител да бъде сключено споразумение. Това споразумение може да обхваща параметрите във връзка с публикуването и ползването на снимките и видеоклиповете, както и при какви условия и в какъв срок биха могли да се обработват. Както при обработването на основание съгласие, така и при сключването на споразумение служителите следва да получат предварително цялата необходима информация във връзка с целите, условията, срока за обработване на личните им данни и възможностите за упражняване на правата по смисъла на чл. 15 – 22 от ОРЗД.

Въпреки многократно публикуване на сайта на КЗЛД на информация относно задължението на определени категории администратори да копират/сканират документ за самоличност (лична карта) на физическите лица запитванията по този въпрос не намаляват. Широкият кръг от задължени лица по смисъла на Закона за мерките срещу изпирането на пари (ЗМИП) и Закона за мерките срещу финансирането на тероризма налагат все повече субекти на данни да попадат под действието на предприетите в тази област мерки и съответно възникващите съмнения за незаконосъобразно обработване на лични данни

нарастват. Една от основните мерки по ЗМИП включва идентификация на клиентите физически лица в хода на комплексната проверка, която съгласно чл. 53, ал. 1 от ЗМИП се извършва чрез представяне на официален документ за самоличност и снемане на копие от него. Това законово задължение спрямо администратора представлява условие за обработване на лични данни съгласно чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 и следва да се извършва в съответствие с въведените от него политики и процедури.

По друг начин стои въпросът относно копиране и сканиране на лична карта от страна на работодател, каквито случаи също са предмет на запитвания от субекти на данни. Практиката на надзорния орган в това отношение е постоянна и се изразява в това, че работодателят няма право да копира личната карта на работника/служителя, а само да запише данните от нея при необходимост (например при сключване на трудов договор), след което трябва да я върне на притежателя ѝ. Право да копират лична карта имат ограничен кръг от администратори, само тези администратори, които имат такова задължение, регламентирано в нормативен акт.

По повод копирането на документ за самоличност се затвърждава тенденцията за многобройни въпроси дали куриерските фирми имат право да изискват предоставяне на лична карта, за да бъдат сравнени данните на получателя. Позицията на КЗЛД е константна и е в унисон с разпоредбата на чл. 20, ал. 1, т. 11 от ЗПУ, съгласно която пощенските оператори (каквито са и доставчиците на куриерски услуги) са длъжни да събират идентификационни данни за физически и юридически лица, както и на упълномощени от тях лица, което по своята правна същност е основание за законосъобразното им обработване по смисъла на чл. 6, §1, б. „в“ от Регламент (ЕС) 2016/679 („обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора“). Надзорният орган използва възможността и да разяснява и други задължения на пощенските оператори, свързани с обработването на лични данни и изрично разписани в чл. 20, ал. 1, т. 1 и т. 2 от ЗПУ, според които пощенските оператори са длъжни да: 1) осигуряват неприкосновеност на пощенските пратки; и 2) опазват тайната на кореспонденцията. Тези задължения не могат да бъдат спазени без идентифициране на физическото лице, получател на пратката.

Въпреки трансформациите на пазара на хазартни игри не намалява броят на запитванията на субектите на данни, изразяващи притеснение при обработване на техните лични данни при участия в такива онлайн игри. Тук също съществува постоянна практика на надзорния орган, основана на задълбочен анализ на приложимото законодателство. Съгласно разпоредбите на чл. 47а от Закона за хазарта участниците в онлайн залагания подлежат на индивидуална регистрация по ред и начин, определени в Наредбата за

условията и реда за регистрация и идентификация на участниците, съхраняването на данни за организираните онлайн залагания на територията на Република България и за подаване на информация за хазартите игри към сървър на Националната агенция за приходите. В глава II от Наредбата изчерпателно са изброени необходимите условия и реквизити при регистрация и идентификация на участниците в онлайн залагания. Централната компютърна система (ЦКС) на организаторите на онлайн залагания трябва да има система за регистрация и идентификация на участниците в игрите. Условие за участие в онлайн залагания е участникът да е регистриран в ЦКС. За онлайн залагания чрез интернет системата следва да идентифицира и регистрира участниците от територията на Република България на база географско локализиране на *IP* адреса, от който участникът се регистрира. За онлайн залагания чрез електронни съобщителни средства системата следва да идентифицира и регистрира участниците, изпращащи кратки текстови съобщения (*SMS*) от територията на Република България. Като участници могат да се регистрират само навършили 18-годишна възраст дееспособни физически лица. В описаните случаи организатор на хазартни игри, в качеството си на администратор на лични данни, обработва такива на основание чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), когато обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора.

През 2021 г. в КЗЛД са получени и запитвания във връзка с реда и условията за издаване на препис-извлечение от акт за смърт на трети лица, както и други удостоверения за гражданското състояние на лицата. Позицията на КЗЛД е, че предоставянето на данни от ЕСГРАОН и издаването въз основа на актовете за гражданско състояние на официални документи (каквото е препис-извлечението от акт за смърт и др.) са две самостоятелни юридически действия, които са предмет на регулация от различни правни режими по смисъла на Закона за гражданската регистрация (ЗГР).

От една страна, разпоредбата на чл. 106 от ЗГР регламентира реда и условията за предоставяне на данни от ЕСГРАОН, докато, от друга, въз основа на актовете за гражданско състояние длъжностните лица по гражданското състояние в общинските администрации по местосъхранението им издават документи по утвърден образец (чл. 88 от ЗГР). В практиката си КЗЛД отбелязва, че издаването на документите, посочени в чл. 88 от ЗГР, респ. предоставянето им на съответните правоимащи лица, не попада в обхвата на чл. 106, ал. 1, т. 3, пр. 3 от ЗГР, по който КЗЛД е компетентна да се произнесе с разрешение по отношение на искания на български и чуждестранни юридически лица за предоставяне на данни от ЕСГРАОН.

Усложнената епидемиологична обстановка в страната както през 2020-а, така и през 2021 г. води до възникване на проблеми, с които обществото не се е сблъсквало преди, в т.ч. преминаването на обучението на ученици и студенти в онлайн среда и свързаното с това засягане на правата на субектите на данни. Комисията продължава да насърчава популяризирането на мерки за защита правата на субектите на данни в контекста на дистанционното обучение, чието въвеждане крие редица предизвикателства за учителите, родителите и учениците. Затова през отчетния период КЗЛД дава насоки по отделни запитвания във връзка с обезпечаването на сигурността на обработването на лични данни, задължения, произтичащи за администраторите на лични данни от разпоредбата на чл. 32 от ОРЗД.

Традиционно задавани въпроси от граждани и организации са свързани с правилно прилагане на критериите за определяне на длъжностно лице по защита на данните и предотвратяване на рисковете от възникване на конфликт на интереси по повод изпълнението на неговите функции и задачи, като през отчетния период тенденцията се запазва.

Все по-често се проявява интерес към обработване на лични данни за целите на изследвания, свързани с историята на родовете и родовата памет на населението и историческия очерк. Основавайки се на натрупан опит по темата, КЗЛД подкрепя извършването и анализа на научноизследователската дейност. Постоянната практика при консултиране на гражданите по подобни казуси включва и насоки за предприемането на подходящи технически и организационни мерки за защита правата и свободите на засегнатите субекти на данни, спазване стриктно на основните принципи за обработването на лични данни, прогласени в чл. 5 от Регламент (ЕС) 2016/679. В този смисъл КЗЛД традиционно препоръчва мерките да включват псевдонимизация, при условие че посочените цели могат да бъдат постигнати по този начин. Когато посочените цели могат да бъдат постигнати чрез по-нататъшно обработване, което не позволява идентифицирането на субектите на данни, целите могат да бъдат постигнати и чрез анонимизация. Когато едно такова проучване с научноизследователска или историческа насоченост засяга лични данни и на публични личности, се вземат предвид и някои принципни положения, закрепени в редица конституционни решения, че данните на лица, заемащи висши публични длъжности и данни на публичните фигури, са с „по-занижена защита“ в сравнение с данните на останалите лица.

Прави впечатление, че през отчетния период зачестяват казусите, свързани с искания за предоставяне на документи, съдържащи лични данни. В отговорите по такива въпроси се

подчертава съществената разлика между двата режима – от една страна, правото на достъп до лични данни, което трябва да се различава от правото на достъп до официални документи. Пример за сложността в разграничението между двата правни режима е различният смисъл, който се влага в понятието „съгласие за обработване на лични данни“ и съответно „съгласие за извършването на определени медицински дейности по смисъла на чл. 87, ал. 7 от Закона за здравето“ в контекста на лица с психични разстройства и установена неспособност за изразяване на информирано съгласие. Такова съгласие се изразява от лицата, определени по реда на чл. 162, ал. 3 от ЗЗдр – с решение от компетентния съд. Информираното съгласие съгласно ЗЗдр не съвпада по своята същност и съдържание със съгласието като основание за обработване на лични данни – чл. 6, пар. 1, б. „а“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, а именно, когато субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели. Комисията изразява позицията, че по отношение на изискваната от лечебното заведение етапна експертиза за психичноболно лице от страна на лице, определено по реда на чл. 162, ал. 3 от ЗЗдр, следва да се прилагат специалният ред и определените условия за предоставяне на здравна информация на трети лица, разписани в разпоредбите на чл. 28 от ЗЗдр, а не общият ред за достъп до лични данни по смисъла на чл. 15 от ОРЗД.

Съществена част от дейността на експертите е даването на консултации по телефона. Това е друг канал, чрез който КЗЛД насърчава обществената информираност и спомага за разбиране и ограничаване на рисковете при обработване на лични данни. Телефонът за експертни консултации по прилагането на Регламент (ЕС) 2016/679 и на националното законодателство за защита на личните данни има предимството за получаването на бърз отговор по нетолкова сложни казуси. Запитванията, получени по телефона за консултации, понякога могат да са индикатор за наличието на обществено значими проблеми, свързани със защитата на личните данни. Наред с това по телефона често се задават въпроси от клиенти на банки или на доставчици на платежни услуги, които се интересуват дали съответният администратор има правно основание да изисква копие от документ за самоличност. Поставят се въпроси относно правото да се проверява цифровият *COVID* сертификат, необходимостта от регистрация на администратор на лични данни, копиране на лични карти и т.н. Практиката е в случаите, когато поставеният въпрос изисква по-задълбочено проучване на правната материя, запитващият да се пренасочва да зададе своя въпрос писмено. През отчетния период са предоставени 1693 експертни консултации по телефон.

IV. КОНТРОЛНА ДЕЙНОСТ

1. Сигнали и искания

През отчетната 2021 г. в КЗЛД са постъпили **487** бр. сигнали, искания и запитвания по актуални въпроси във връзка с обработването на лични данни и изложени твърдения за нарушения на Регламент 2016/679 и ЗЗЛД, без да са регистрирани значителни пробиви в базите данни при големи администратори като НАП през 2019 г. От тях са отработени **468** бр., като на всички податели са изпратени съответни отговори, а при необходимост получените сигнали са изпращани и на съответните органи или институции за произнасяне по компетентност. За сравнение през 2018 г., първата от прилагането на Регламент 2016/679, са постъпили 290 бр. сигнали и запитвания.

Най-много запитвания и сигнали са получени срещу администратори на лични данни, предоставящи интернет услуги – 120 бр. На следващо място са сигнали за евентуално незаконосъобразно обработване на лични данни от администратори на лични данни органи на държавната администрация – 42 бр., администратори, обработващи лични данни чрез изградени системи за видеонаблюдение – 28 бр. Сигнали са получени 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 броя, 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.

На графиката е изобразен сравнителен анализ на назначените за периода 2017 – 2021 г. сигнали (фиг. 5)

Фиг. 5

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. В контекста на пандемичната обстановка се забелязва склонност към увеличаване на запитванията (по брой и съдържание) по теми, свързани със социалните мрежи, провеждане на онлайн събития, видеонаблюдение и видеозаснемане, обработване на лични данни от куриерски дружества и онлайн платформи за хазартни залагания.

Традиционно постъпват и множество запитвания, свързани с използване на лични данни от страна на мобилни оператори, пощенски оператори, фирми за бързо кредитиране и предоставяне на лични данни на т.нар. колекторски фирми и директния маркетинг. Очертават се и нови проблемни сфери като онлайн платформите за търсене и предлагане на работа и онлайн залагания. Основно запитванията са относно количеството и видовете лични данни, обработвани от сайтове, предлагащи хазартни залагания.

През 2021 г. са обработени и множество сигнали и запитвания, свързани с провеждането на три последователни парламентарни избори и избор за президент на страната, както и проведеното Преброяване на населението и жилищния фонд в Република България, регламентирано в Закона за преброяване на населението и жилищния фонд в Република България през 2021 г.

Прави впечатление, че субектите на данни са добре запознати с правата си по Регламент (ЕС) 2016/679 и ЗЗЛД. Значително са намалели сигналите и запитванията, касаещи съгласието като основание за обработване на лични данни, което вече се разбира от физическите лица и не се разглежда като „най-значимо“ правно основание за обработване на лични данни. Хипотезите за законосъобразно обработване на лични данни, изчерпателно изброени в разпоредбите на чл. 6, пар. 1 и чл. 9, пар. 2 и пар. 4 от Регламент (ЕС) 2016/679, вече са познати на значителен брой субекти на лични данни относно хипотезите и тяхната самостоятелност и равнопоставеност, като същите не са изброени в йерархически ред по важност.

Все още отказът на администратори на лични данни (институции или правнозадължени администратори) да изтрият данни на физически лица – субекти на данни, продължава да се възприема като злоупотреба с данни. Продължава тенденцията, в която субектите се опитват да избегнат или заобиколят свои финансови или други задължения чрез упражняване на „правото да бъдеш забравен“ или посредством оттегляне на съгласие за обработване на данните им.

Комисията за защита на личните данни системно и методично разработва както отговори, така и информационни материали през годините, които разясняват правата на лицата и задълженията на администраторите при защитата на личните данни. Константна практика е да се обръща внимание, че институции и дружества, които осъществяват своята дейност в условията на строга регламентация, не обработват лични данни на основание съгласието на субектите на данни. Системно се разяснява също, че правото на изтриване („да бъдеш забравен“) не е абсолютно право и то е подложено на редица ограничения, сред които попадат законовите задължения, обвързващи администраторите на лични данни със задължението да съхраняват данни за определен период от време (например публични органи, кредитни и финансови институции, мобилни оператори и т.н.), но и често пъти е с преобладаващ обществен интерес (например при средствата за масово осведомяване).

Новост през отчетния период са значителният брой запитвания на субектите на данни относно основанията за обработване на данни в кампания на Министерството на здравеопазването за приканване на гражданите за ваксиниране чрез партньори – мобилните оператори. Основното притеснение на гражданите е споделена ли е или не с партньорите мобилни оператори информация, съдържаща медицински чувствителни данни. От направеното проучване не е установено незаконосъобразно обработване на чувствителни лични данни.

Тези въпроси разбираемо са свързани с развитието на пандемията в световен мащаб и често се комбинират с искания за информация по отношение правата на лицата в онлайн

среда. Следва да се отчита, че голяма част от чисто организационните мерки по преодоляване на последиците и за борба с коронавируса са свързани директно със защитата на неприкосновеността на личния живот и защитата на личните данни както на национално, така и на международно ниво.

В тази връзка са изготвяни отговори на запитванията на физическите лица в съответствие с прието Становище на КЗЛД относно обработване на данни за ваксинационния статус с рег. №ПНМД-01-93/2021 г., публикувано на официалната ѝ интернет страница. В него е посочено, че съгласно чл. 10, параграф 2 от Регламент (ЕС) 2021/953 (който е *lex specialis* по отношение на Регламент (ЕС) 2016/679) личните данни, съдържащи се в сертификатите, се обработват единствено с цел достъп до и проверка на информацията, съдържаща се в тях, за да се улесни упражняването на правото на свободно движение в Съюза по време на пандемията от *КОВИД-19* и само в рамките на определения от регламента срок, като след това не следва да се извършва по-нататъшно обработване.

Към настоящия момент националното ни законодателство не регламентира разширеното използване на лични данни от Цифровия *COVID* сертификат на ЕС за цели, различни от улесняването на правото на свободно движение в Съюза по време на пандемията от *КОВИД-19* и само в рамките на определения от Регламент (ЕС) 2021/953 срок.

Въпреки това и с оглед необходимостта от спазване на заповедите на министъра на здравеопазването, с които се въвеждат противоепидемични мерки, администраторите на лични данни могат да обработват агрегирани (обобщени) данни за ваксинационния статус на лицата, които да ги подпомогнат при извършване на оценката на риска при осигуряването на здравословни и безопасни условия на труд.

Единствената правна възможност за администраторите извън посочената в чл. 10, параграф 2 от Регламент (ЕС) 2021/953 да осигурят баланс при изпълнението както на заповедите на министъра на здравеопазването, така и на законодателството за защита на личните данни е да извършват проверка на Цифровия *COVID* сертификат на ЕС, без да съхраняват резултатите от нея. Тези действия могат да се извършат само при доброволно представяне на сертификата, а липсата на такова представяне не може да се използва за ограничаване на правата и свободите на физическите лица.

За пълнота на информацията следва да се има предвид, че Министерството на здравеопазването е разработило и пуснало за употреба приложение за проверка на Цифровия *COVID* сертификат на ЕС – т.нар. *Covid Check BG*. Функцията на приложението позволява единствено моментна проверка валидността на представения сертификат, като информация не може да бъде съхранена на устройството, на което с инсталирано

приложението. Съгласно чл. 2, ал. 1 от Закона за частната охранителна дейност: „Частната охранителна дейност е търговска дейност, насочена към опазване на живота и здравето на физическите лица, охраняване на имуществото на физическите и юридическите лица, гарантиране на максимално ниво на сигурност при транспортиране на ценни пратки и товари, осигуряване на безпрепятствено провеждане на различни по характер и вид мероприятия“.

Чл. 56, ал. 1, буква „а“ от същия закон посочва: „При извършване на дейност по чл. 5, ал. 1 изпълнителите на частна охранителна дейност:

осигуряват спазването на установения пропускателен режим за влизане и излизане от охранявания обект и вътрешния ред в него чрез:

а) проверка на документите за самоличност на външни лица и служебните пропуски на работещите“.

В тази връзка за КЗЛД няма причина да предприеме последващи действия и да упражни контролните си правомощията, тъй като е налице законово основание за идентификация на приносител на зелен сертификат чрез представяне на документ за самоличност.

През целия отчетен период се запазва и тенденцията за запитвания по отношение на процедурите, които се прилагат при подаването на жалби и сигнали. Гражданите се интересуват от действията, които трябва да предприемат в качеството си на жалбоподател, срокове за разглеждане на техния казус и начините за получаване на обратна връзка, въпреки че тази информация е налична на институционалната страница на КЗЛД.

През 2021 г. се забелязва значително нарастване на препратените по компетентност преписки от прокуратурата, органите на МВР, когато е отказано образуване на наказателно производство поради липсата на достатъчно събрани доказателства за престъпление, но има събрани факти и твърдения за евентуално извършени нарушения в областта на защитата на личните данни. Следва да се отбележи, че Комисията е получила препратени по компетентност сигнали в кръга на правомощията си, както следва: от органи и структури на МВР (ДАНС, ГДБОП, РПУ) – **30** бр., от Прокуратурата – **27** бр., от КЗП – **28** бр., КРС – **3** бр., омбудсман на Република България – **1** бр., и др.

Относително голям е броят на постъпилите сигнали и запитвания относно работата на телекомуникационните компании, куриерските дружества, дружествата за събиране на вземания, интернет сайтове и платформи и банкови институции, застрахователни дружества, сайтове за търсене и предлагане на работа и сайтове за хазартни игри. Голям брой сигнали и запитвания касаят публично оповестени/публикувани документи с лични данни.

Значителен е броят на постъпилите преписки, касаещи обработване на лични данни на физически лица от различни интернет сайтове и платформи по отношение неспазване на изискванията на Регламент 2016/679 и ЗЗЛД, и по-точно, на задълженията на администраторите на интернет платформите да публикуват своите правила или политики за обработване на личните данни на потребителите, политики за поверителност при използването на т.нар. „бисквитки“. Посочва се, че липсват данни за контакт с администратора на сайта и/или с лицето по защита на данните с оглед упражняване на правата на потребителите по Регламент 2016/679.

Много от сигналоподателите искат съдействие от КЗЛД за упражняване на правото на регистрираните потребители да бъдат деактивирани техните акаунти и/или изтрита публикувана от/за тях информация, съдържаща лични данни.

За отбелязване е и нарасналият брой сигнали за неправомерен достъп до потребителски профили във Фейсбук, *Google* и други електронни платформи. Сигналите са за създаване на фалшиви (неистински) профили, злоупотреба с публикувана в мрежата информация (вкл. видео и снимков материал) и др. На подателите на този род сигнали и запитвания се разяснява, че относно установяване на авторите на такива деяния, когато извършителят е неизвестен, е необходим достъп до „трафични данни“, който обаче се осъществява на основание и по реда на Закона за електронните съобщения, по който КЗЛД няма правомощия. За съжаление, практиката на компетентните да извършват справки по Закона за електронните съобщения органи показва, че често пъти домейните са хоствани и регистрирани извън територията на страната от чужди граждани с непълен адрес, поради което КЗЛД не е в състояние да упражни своите корективни правомощия. В тази връзка дейността на КЗЛД е насочена към повишаване на правната култура за защита на личните данни на субектите чрез публикации и интервюта в средствата за масово осведомяване и публикуване на интернет страницата си на становища, решения по казуси, брошури с цел информиране на гражданите за техните права и начини за защита на личните им данни.

2. Назначени и извършени проверки през 2021 г.

Постоянна цел на КЗЛД, в качеството ѝ на национален надзорен орган, е прилагането на ефективен механизъм за надзор в областта на защитата на личните данни. В изпълнение на този приоритет през 2021 г. КЗЛД ефективно използва и прилага разработени и утвърдени ключови документи, достъпни на официалната ѝ интернет страница, както следва:

• Инструкция за практическото осъществяване на надзорната дейност на КЗЛД (инструкцията е изцяло в синхрон с приетите от ЕКЗД през януари 2021 г. Насоки за

прилагането на чл. 62 от Регламент 2016/679 (вътрешен документ, предназначен само за надзорните органи по защита на данните, който урежда осъществяването на съвместни операции между тях);

- Методика за определяне нивото на риска при нарушения на сигурността на личните данни (методиката е приложение към Инструкцията за практическото осъществяване на надзорната дейност на КЗЛД и представлява инструментариумът, с помощта на който КЗЛД оценява рисковете за правата и свободите на физическите лица, чиито лични данни са с нарушена сигурност);
- Въпросник за извършване на проверки при осъществяване на надзорната дейност на КЗЛД (въпросникът е приложим към всички видове проверки, осъществявани от КЗЛД и нейната администрация).

През 2021 г. са назначени **227** бр. проверки на място по повод постъпили в КЗЛД жалби, искания и сигнали, от които са извършени **206** бр., като 13 бр. са по уведомления за нарушаване на сигурността на личните данни с висок риск съгласно чл. 33 от Регламент 2016/679. Забелязва се трайна тенденция за увеличаване на казусите, при които следва да се съберат правнорелевантни факти и доказателства за преценка дали има или не незаконосъобразно обработване на лични данни, което съответно да бъде санкционирано по реда на Закона за административните нарушения и наказания (ЗАНН) или да бъдат наложени корективни мерки по реда на Регламент 2016/679, което на фона на двойно увеличената бройка на преписките води до изключително натоварване.

На графиката е изобразена сравнителна статистика на назначените в периода 2017 – 2021 г. проверки (фиг. 6).

Фиг. 6

Най-много проверки са извършени в областите: София – 95 бр., Варна – 15 бр., Пловдив – 11 бр., Благоевград – 8 бр.; Бургас – 8 бр.; Велико Търново – 8 бр.; Пазарджик – 6 бр.; Русе – 6 бр.; Стара Загора – 5 бр.; Плевен – 4 бр.; Хасково и Ямбол – 3 бр., и в по-малка степен в други области на страната.

Трайно увеличеният ръст на жалбите и сигналите с предмет видеонаблюдение има за последица засилена и натоварена контролна дейност върху обработването на лични данни на физически лица посредством изградени системи за видеонаблюдение. Анализът показва, че предметът на сигналите е идентичен с този при жалбите, а именно видеонаблюдение на обществени места (улици, тротоари, зелени площи), както и общи части в етажна собственост. КЗЛД констатира все по-често използването на модерни в техническо отношение камери, голяма част от тях с широк ъгъл на видеонаблюдение и запис на звук, както и поставени „бутафорни“ камери, имитиращи осъществяване на видеонаблюдение. Тенденцията за множество оплаквания с посочения предмет води до това, че през 2021 г. най-голям брой проверки са извършени след подадени жалби и сигнали за обработване на лични данни посредством изградени системи за видеонаблюдение. Липсата на нормативна регламентация на осъществяваното в страната видеонаблюдение от различни администратори и субекти води до множество сигнали и жалби, както и до конфликтни ситуации между администраторите и субектите, чиито данни се обработват.

Изразходват се изключително много човешки ресурси и средства за осъществяване именно на този вид контрол на нарушения.

3. Значими проверки и казуси през 2021 г.

Извършени са проверки на администратори по ШИС – Национален институт по криминалистика, МВнР – Национален визов център, МВР – дирекция „Международно оперативно сътрудничество“ – Бюро СИРЕНЕ, МВР – дирекция „Международно оперативно сътрудничество“ – Национално звено „Европол“, МВР – дирекция „Комуникационни и информационни системи“, като са наложени корективни мерки с цел повишаване на сигурността на обработваните бази данни.

През отчетния период във връзка с постъпил в КЗЛД Одитен доклад на Сметната палата „Ефективност на организацията и контрола на дейностите на водене и съхраняване на поддържаните от Агенция по вписванията регистри“, обхващащ периода 01.01.2017 – 30.12.2019 г., в изпълнение на Решение на Комисията за защита на личните данни е извършена проверка на Агенция по вписванията. В резултат от проверката е наложена 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 лв. Наказателното постановление е обжалвано и в края на отчетния период се намира в съдебна фаза.

Друга значима проверка през 20021 г. е на банкова институция след получено уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679 относно получено електронно съобщение с твърдения за нарушаване на сигурността. Изпратилият съобщението заявява, че разполага с кредитното портфолио на банката, данни за банкови карти и списък с лични данни на клиенти на банката. Като доказателство е предоставен линк към файлов сървър, съдържащ три файла, за които е установено, че са истински данни от банковите системи. Лицето, изпратило имейла, дава срок от 72 часа банката да преведе парични средства, в противен случай ще предостави кредитното портфолио на други банки в България и ще го сподели в интернет пространството, а номерата на банковите карти ще предостави на нелегални организации в т.нар. *dark web,* като уведоми КЗЛД, медиите и социални мрежи.

В хода на извършената проверка е установено, че служител на банката съзнателно е нарушил и/или избегнал част от мерките за сигурност и съответствие, което е довело до нарушаване на сигурността на личните данни. Заеманата от него длъжност е свързана с достъп до голям обем данни при изпълнение на служебните задължения. В резултат на извършените проверки и анализи на информационните системи, цифровите устройства и

регистрационните файлове е установено, че чрез своите идентификационни данни (потребителско име и парола) служителят е създал справка с обем и съдържание, идентични с тези, получени в банката като доказателство за предполагаемата успешна кибератака.

Извършени са проверки след подадени от застрахователно дружество уведомления по чл. 33 от Регламент (ЕС) 2016/679 относно откраднати от куриерска компания, с която има сключен договор, пратки, съдържащи лични данни. При първото уведомление кражбата на пратка е осъществена от служител на дружеството, а при второто – от неизвестно лице. По време на проверките са обсъдени данните и обстоятелствата относно получените уведомления. Обсъдени са процедурата за доставка на куриерските пратки, проследимостта на пратките посредством използвания софтуерен продукт за администриране и управление на процеса по осъществяване на куриерските услуги, както и предприетите от двете дружествата действия във връзка с възникналите инциденти.

През 2021 г. е извършена и втора проверка на същото застрахователно дружество във връзка с получено уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679 относно установен неоторизиран достъп (кибератака) до клиентските му портали в периода 02.10.2020 г. – 26.10.2020 г., през който е източена информация от двата портала. По време на проверката са изяснени задачите на проверката и са обсъдени данните и обстоятелствата относно полученото уведомление. Демонстрирана е функционалността на клиентските портали. Като основна причина за инцидента всички страни, участващи в разследването и неговото противодействие, посочват силно остарелите операционни системи и софтуерния стек. Обсъдени са предприетите от дружеството действия във връзка с възникналия инцидент и предотвратяване на такива в бъдеще.

Получено е уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679 относно осъществена хакерска атака на уеббазирана информационна система на дружество, която подпомага дейността и бизнес процесите на застрахователните брокери, с искане за изплащане на откуп. За случая е уведомена незабавно ГДБОП. Констатирано е, че нарушението на сигурността се изразява в целенасочена атака, осъществена чрез едновременно инициирани от чуждестранни *IP* адреси (*Internet Protocol*) голям брой справки от страна на потребители (потребителски акаунти) в множество различни инсталации на информационната система. Нерегламентираният достъп е осъществен чрез т.нар. *brute force* на потребителски пароли. По време на проверката е установено, че при евентуален неоторизиран достъп до интерфейса на конкретна инсталация чрез потребителски профил се ограничава нарушаването на сигурността на лични данни само до достъпните за конкретния потребител

записи. Обсъдени са предприетите от дружеството действия във връзка с възникналия инцидент и въведените впоследствие технически и организационни мерки за защита.

На основание чл. 58, §1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. във връзка с изпълнение на Решение на Комисията за защита на личните данни (КЗЛД) от 15.09.2021 г. по повод получени сигнали и заповед на председателя на КЗЛД се извършва проверка на Националния статистически институт (НСИ) във връзка с обработването на лични данни на физически лица при осъществяване на „Електронно преброяване 2021“ и твърдения за предоставянето им на трети страни извън Европейския съюз.

В изпълнение на ангажиментите на Република България като държава – членка на ЕС, по силата на Регламент (ЕС) 2016/679 за осъществяване на „Електронно преброяване 2021“ НСИ обработва лични данни в изпълнение на нормативно установено задължение, а именно провеждане на преброяване на населението и жилищния фонд в Република България, регламентирано в Закона за преброяване на населението и жилищния фонд в Република България през 2021 г.

НСИ провежда електронно преброяване на населението и жилищния фонд в Република България в периода от 00:00 часа на 7 септември до 24:00 часа на 30.09.2021 г. чрез попълване на електронна преброителна карта. Приложението за въвеждане на електронната преброителна карта е достъпно единствено за населението на територията на страната на интернет адрес *https://e-census2021.bg* 24 часа в денонощието.

Във връзка с нарасналата необходимост от гарантирано изпращане и получаване на огромни количества масови електронни писма за различните кампании по изследванията на НСИ е използвана външна услуга, предоставяна от компания, базирана в ЕС. Целта е предпазване от влизане в „черни списъци на изпращачи на имейли“, което би нарушило работата на НСИ по изследванията, както и възможност за по-добро управление и контрол на този процес. Услугите, извършвани от наетия доставчик, са изпращане на автоматично генерирани от платформата за електронно преброяване три типа имейли: активиране на акаунт, смяна на парола и получаване на преброителен код до регистрираните лица. Осигуряването и поддръжката на услугата за нуждите на НСИ са за период от 12 месеца.

Във връзка с изпълнение на указания за повишаване на нивото на мрежовата и информационната сигурност и зачестилите атаки към сайтове на държавната администрация от НСИ приемат решение за ползване на външна услуга за нуждите на *https://e-census2021.bg,* предоставяна от компания, базирана в САЩ, която предлага множество облачни услуги и поддържа представители в различни европейски страни (доставчик). Предоставяните услуги за нуждите на системата за електронно преброяване

(домейн *e-census2021.bg*) са единствено за повишаване на нивото на мрежовата и информационната сигурност за период от 5 месеца.

Взаимоотношенията между НСИ и доставчика са уредени чрез българска компания, търговски посредник. Нает е стандартен пакет от услуги, за който няма сключен нарочен договор между представителя в България и НСИ, но важат Общите условия за продажба на стоки и услуги на доставчика и неговия представител. В хода на проверката е установено, че търговският посредник не извършва операции по обработване на личните данни на преброилите се лица.

Проверката установява, че услугите, предоставени на НСИ, касаят обработката на лични данни дотолкова, доколкото пакетите с информация, обменяна между потребителите и системата, се инспектират за *Cross-Site Request Forgery* (*CSRF*), *Cross-site Scripting* (*XSS*), *file inclusion, SQL injection* и др. съгласно изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС) към Закона за киберсигурност (ЗКС) и е възможно тя да бъде инспектирана за наличието на подобен зловреден код. Интерфейсът, използван между НСИ и доставчика, е стандартен *HTTPS* протокол. Пренасяне на лични данни в САЩ не се извършва. Данните се обработват на сървъри в ЕС и не се трансферират извън ЕС.

Доставчикът предоставя агрегирани (анонимизирани) данни на НСИ по отношение на обема трафика, сигурност, производителност и *DNS* заявки относно *https://e-census2021.bg*. Ключът за криптиране и декриптиране на информацията е собственост на НСИ.

Констатирано е, че информацията от преброяването се обработва на сървъри на доставчика на територията на Европейския съюз. Видно от събраната в хода на проверката документация и Общите условия на доставчика (*Cloudflare Privacy Policy*), към сървърите на САЩ се подават единствено анонимизираните *IP* адреси и метаданните на потребителите на информационната система, като информацията се съхранява 25 часа.

При обработване на данните от страна на НСИ приложимото законодателство е законодателството на Република България и на ЕС. Приложимото законодателство в съответствие с приетите от доставчика договорни условия и в частност приетите стандартни договорни клаузи (въз основа на одобрените с Решение на Европейската комисия от 04.06.2021 г., касаещи защитата на личните данни) е приложимото право на Европейския съюз и е в юрисдикцията на Съда на ЕС (*Data Processing Addendum: Standard Contractual Clauses for Customers* – клаузи 17 и 18). Стандартните договорни клаузи, подписани от доставчика, са актуализирани и са в съответствие с последните приети от Европейската комисия, които отразяват решението на Съда на ЕС по делото „Шремс II“.

По съображения от засилен обществен интерес Комисията е уведомила чрез прессъобщение обществеността и гражданите, подали сигнали със съмнения относно обработването на техните лични данни, че в хода на извършената проверка не са установени незаконосъобразни действия по обработването на данни на граждани на Република България, участващи в провежданото от НСИ „Електронно преброяване 2021“.

След получен в КЗЛД сигнал, на основание чл. 58, §2, буква „и“ и чл. 83, §2, букви „а“, „в“, „г“, „е“ и „ж“ от Регламент (ЕС) 2016/679 и чл. 87, ал. 2 от ЗЗЛД във връзка с чл. 36 от ЗАНН през отчетния период е съставен и връчен акт за установяване на административно нарушение (АУАН) на управителя на куриерско дружество. При осъществяване на дейността си дружеството не е отчело естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, като не е приложило подходящи технически и организационни мерки, гарантиращи постоянна поверителност, цялостност и устойчивост на системите и услугите за обработване, в резултат на което са осъществени неоторизиран достъп, неразрешено разкриване и разпространение на лични данни (имена, адрес) в различен обем на общо 2004 (две хиляди и четири) физически лица, видими през прозрачния отвор на пощенските пликове, които са изхвърлени на публично място, с което е нарушен чл. 32, §1, буква „б“ във връзка с чл. 5, §1, буква „е“ от Регламент (ЕС) 2016/679 и чл. 66, ал. 1 от ЗЗЛД.

Във връзка с постъпил сигнал в КЗЛД относно оставени без надзор документи, съдържащи лични данни, и непредприети мерки за защита е извършена проверка в „Специализирана болница за долекуване и продължително лечение на пневмо-фтизиатрични заболявания и рехабилитация – Радунци“ ЕООД (СБДПЛПФЗР – Радунци), която е в процес на ликвидация. При извършената проверка е установено огромно количество от документи – болнична документация (трудови досиета, ведомости за заплати, картони на персонала, медицински картони на пациенти, цялостна архивна документация, свързана с болничното заведение, история на заболяването и др.), разпръсната в разрушаващите се сгради на болницата. Документите са за периода от основаване на болницата през 1955 г. до преустановяване на дейността ѝ през 2015 г.

В помещение, където са съхранявани медицински досиета на последните пациенти на СБДПЛПФЗР – Радунци, е констатирано наличието на: над 567 броя медицински досиета на физически лица – пациенти, постъпили за лечение през 2014 г.; над 958 броя медицински досиета на физически лица – пациенти, постъпили за лечение през 2013 г.; над 1202 броя медицински досиета на физически лица – пациенти, постъпили за лечение през 2012 г. В друго помещение са установени над 20 895 броя медицински досиета на физически лица – пациенти, постъпили за лечение преди 2012 г. В друго архивно помещение са установени

още над 16 310 броя медицински досиета на физически лица – пациенти, постъпили за лечение преди 2012 г. В следващо помещение са констатирани още над 12 880 броя медицински досиета на физически лица – пациенти, постъпили за лечение преди 2012 г. В последното архивно помещение са установени още над 9520 броя медицински досиета на физически лица – пациенти, постъпили за лечение преди 2012 г. Констатираният общ брой на медицински досиета на физически лица – пациенти, постъпили на лечение в СБДПЛПФЗР – Радунци до 2014 г. е над 65 000 броя. Медицинските документи съдържат всички лични данни на пациента (три имена, ЕГН, паспортни данни, телефон, адрес, лица за контакт и др.), както и чувствителни данни относно заболяването на пациентите, проведеното лечение, направени изследвания и ТЕЛК. Счетоводните документи съдържат всички лични данни на служителите (три имена, ЕГН, паспортни данни и др.), както и данни за получаваното заплащане, изплащането на допълнителни възнаграждения и др.

В резултат на извършената проверка са съставени два броя актове за установяване на административно нарушение на Министерството на здравеопазването и на назначения ликвидатор на дружеството за неспазване на разпоредбите на чл. 32, §2 и §3 от Регламент (ЕС) 2016/679., като на Министерството на здравеопазването е издадено и Разпореждане на основание чл. 58, §2, б. „г“ във връзка с чл. 32, §1, б. „б“ от Регламент (ЕС) 2016/679, в качеството му на администратор на лични данни, да съобрази операциите по обработване на данни, като приложи подходящи технически и организационни мерки за осигуряване на съобразено с риска ниво на сигурност на обработване чрез съхранение на лични данни на физически лица – персонал и пациенти на „Специализирана болница за долекуване и продължително лечение на пневмо-фтизиатрични заболявания и рехабилитация – Радунци“ ЕООД, до тяхното предаване на Държавен архив – Стара Загора, или до унищожаване на тези, които са с изтекъл срок на съхранение. Решението, с което е разпоредено на МЗ да предприеме действия, изискуеми съгласно българското законодателство по съхраняване и опазване на документите, съдържащи лични данни, е изпълнено. Наказателното постановление, с което е наложена имуществена санкция в размер на 60 000 лева, е обжалвано и се намира в съдебна фаза.

През 2021 г. е извършена проверка в медицински център във връзка със сигнал с изложени твърдения, че в едно от помещенията на центъра, представляващо чакалня, има свободен достъп до документи (здравни картони), съдържащи лични данни на физически лица – пациенти на починал общопрактикуващ личен лекар. Съгласно разпоредбата на чл. 140 от Националния рамков договор за медицински дейности 2020 – 2022 г. всеки общопрактикуващ лекар посочва в договора си с НЗОК, респективно със СЗОК, свой заместник, когато не може да изпълнява лично задълженията си. При обективна

невъзможност от страна на официалните заместници да поемат задълженията на отсъстващия общопрактикуващ лекар е предвидено те да бъдат поети от друг правоспособен лекар посредством подаване на уведомително писмо и писмена декларация за съгласие за заместване във връзка с промяна на обстоятелствата по чл. 122 от Националния рамков договор за медицински дейности 2020 – 2022 г. За срока на заместването заместващият общопрактикуващ лекар има всички права и поема всички задължения на титуляря.

При извършената проверка на място е констатирано, че в кабинета на заместващия лекар идват голям брой пациенти на замествания лекар, които желаят да получат медицинските си картони. Те нахлуват и изнасят всички медицински документи, като ги захвърлят в чакалнята пред кабинета. Заместващият лекар не е бил в състояние да събере и прибере всички останали документи, поради което те са оставени в чакалнята, достъп до която имат единствено той и хигиенистката. Изложени са твърдения, че още на следващия ден документите са прибрани в изолирано помещение (манипулационна) с ограничен достъп единствено на заместващия лекар.

На основание констатациите от извършената проверка, на основание чл. 58, §2, б. „б“ във връзка с чл. 32, §1 от Регламент (ЕС) 2016/679 КЛЗД отправя към определеното за заместване лице официално предупреждение за това, че в качеството на обработващ лични данни не е приложило подходящи технически и организационни мерки за съобразяване с риска ниво на сигурност на обработването, в резултат на което е допуснало лични данни на физически лица – пациенти на замествания лекар, съдържащи се в техните здравни картони, да бъдат общодостъпни за неограничен кръг външни лица.

От извършените през отчетния период проверки може да се направи обоснован извод, че голяма част от администраторите на лични данни са добре запознати с нормативната база за защита на личните данни, прилагат в голяма степен необходимите технически и организационни мерки за защита на данните, уведомяват физическите лица за техните права, изпълняват задълженията си при упражняване на правата на физическите лица, както и съдействат на КЗЛД при упражняване на нейните правомощия.

През 2021 г. е направено проучване на топлинните счетоводители в страната във връзка с постъпили сигнали за предоставяне на изравнителните сметки на абонатите, съдържащи лични данни на неоправомощени лица. В тази връзка са изпратени 22 писма до визираните администратори, като са изискани: 1. Правила и процедури, удостоверяващи качеството им на субект в процеса на обработване на личните данни на физическите лица; 2. Правила и процедури за връчване на изравнителните сметки; 3. Попълнен въпросник съгласно Инструкцията за практическо осъществяване на надзорната дейност на КЗЛД. В

тази връзка 18 дружества предоставят отговор, при 4 писмата са непотърсени, 10 администратора са предоставили изисканите документи. Установено е, че 6 от дружествата предоставят изравнителните сметки на топлофикационните дружества, която ги връчва чрез куриерски дружества, с които има договори. Прави впечатление, че секторът не е достатъчно добре запознат с изискванията на Регламент 2016/679 и ЗЗЛД, няма изградени бази данни с оторизираните да получават изравнителни сметки на съответната етажна съсобственост и с договорите с куриерски дружества се прехвърля отговорността.

4. Наложени корективни мерки и сравнителен анализ.

Констатираните през 2021 г. нарушения по постъпили сигнали, за които КЗЛД е наложила корективни мерки след извършени проверки от отдел „Контрол и административнонаказателни производства“ в дирекция „Правни производства и надзор“, **са 64 бр**.: **38** разпореждания, **7** официални предупреждения и **19** предупреждения основно за нарушение на чл. 32, §1, букви „б“ и „г“ от Регламент (ЕС) 2016/679, чл. 6, §1, букви „а – е“ от Регламент (ЕС) 2016/679, чл. 25г от ЗЗЛД, чл. 6, §1 от Регламент (ЕС) 2016/679 и чл. 38, §6 от Регламент (ЕС) 2016/679. Прави впечатление, че броят им е завишен двойно – през **2020 г. те са общо 36 бр**. (32 разпореждания, 3 официални предупреждения и 1 предупреждение).

Издадени са разпореждания проверените администратори да преустановят заснемането на публични площи (улици и тротоари) посредством изградени системи за видеонаблюдение; да изработят конкретни правила и механизми за контрол за спазване на издадените заповеди и да предприемат технически и организационни мерки, които ефективно да гарантират защитата на физическите лица.

В резултат на наложени корективни мерки КЗЛД е съдействала за спасяване и съхраняване на повече от **65 000** бр. медицински досиета и над **3300** бр. трудови досиета, съдържащи пълен набор от лични данни, включително и чувствителни такива.

При формулиране на предложенията до надзорния орган за налагане на санкции по постъпили сигнали и проверки, при които са констатирани нарушения, е спазван принципът, че нарушението на Регламент (ЕС) 2016/679 и ЗЗЛД следва да води до налагане на „еквивалентни санкции“. Наложените от КЗЛД административните наказания „глоба“ или „имуществена санкция“ са определени така, че да осъществят в пълен обем правоохранителната и превантивна роля, тоест да бъдат „ефективни, пропорционални и възпиращи“. Същите отразяват адекватно естеството, тежестта и последиците от нарушението, като всички факти по случая се оценяват по начин, който е последователен и обективно обоснован.

Оценката за това какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай отразява целта, преследвана с избраната корективна мярка, т.е. възстановяване на спазването на правилата или санкциониране на неправомерно поведение (или и двете).

Във всеки конкретен казус са взети предвид критериите за оценка в чл. 83, §2, засягащи естеството на нарушението: дали се касае за непредприети достатъчни мерки за предотвратяване на незаконосъобразно обработване на лични данни; дали се отнася до фишинг атака или друг умишлен противозаконен подход с цел незаконосъобразно обработване на лични данни; човешка грешка; тежестта на нарушението: дали е извършено умишлено или по небрежност; продължителността на нарушението (продължителността на нарушението може да е индикация например за умишлено поведение от страна на администратора или непредприемане на подходящи превантивни мерки, или неспособност да се въведат изискваните технически и организационни мерки).

На задължителна преценка подлежи и фактът относно броя на засегнатите субекти на данни, за да се определи дали това е изолиран случай, или показва системно нарушение или липса на подходящи практики. Това означава, че и изолираните случаи подлежат на действия по правоприлагане, тъй като дори един изолиран случай може да засегне множество субекти на данни. При всеки конкретен казус по сигнал или проверка, при който са констатирани нарушения на сигурността на личните данни, се вземат предвид и размерът и относителната тежест на настъпилите и/или възможни вреди за субектите на данни, както и степента на причинените им вреди предвид факта, че обработването на лични данни може да породи рискове за правата и свободите на лицата.

Рискът за правата и свободите на физическите лица с различна вероятност и тежест може да произтича от обработване на лични данни, което би могло да доведе до физически, материални или нематериални вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдоанонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за нарушени свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално,

анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално, на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни. Важен аспект от извършваните проверки е и констатирането дали има търговия с лични данни за маркетингови цели, т.е. продажбата на данните като данни, за които е дадено разрешение за обработване от субектите на данни.

Огромно значение за налаганите санкции и/или корективни мерки има и оценката на проверяващите за действията, предприети от администратора или обработващия лични данни, за смекчаване на последиците от вредите, претърпени от субектите на данни. Това е основата за преценка за наличието на утежняващи или смекчаващи обстоятелства, предвид което се налагат подходящи мерки, които наклоняват везните към мерките, които са по-ефективни, пропорционални и възпиращи в дадения казус.

Важни за преценката на проверяващия екип и предложението за прилагане на определена санкция или мярка е и степента на отговорност на администратора или обработващия лични данни, като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с чл. 25 и чл. 32 от ОРЗД.

От значение е и наличието на предишни нарушения, извършени от администратора или обработващия лични данни. Степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него се взема предвид при изготвяне становището на проверяващия екип.

За размера и вида на предложената корективна мярка или санкция значение имат и категориите лични данни, засегнати от нарушението – най-вече свързано ли е нарушението с обработване на специални категории данни по чл. 9 или чл. 10 от Регламента, могат ли физическите лица да бъдат идентифицирани пряко или непряко, обработването включва ли данни, разпространението на които би довело до непосредствени вреди/затруднения за лицето и които попадат извън обхвата на категориите по чл. 9 или чл. 10, и др.

Показателен за сътрудничеството на администратора е и начинът, по който нарушението е станало известно на надзорния орган, по-специално, дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението.

На графиката е изобразена сравнителна статистика на наложените корективни мерки в периода 2017 – 2021 г. проверки (фиг. 7).

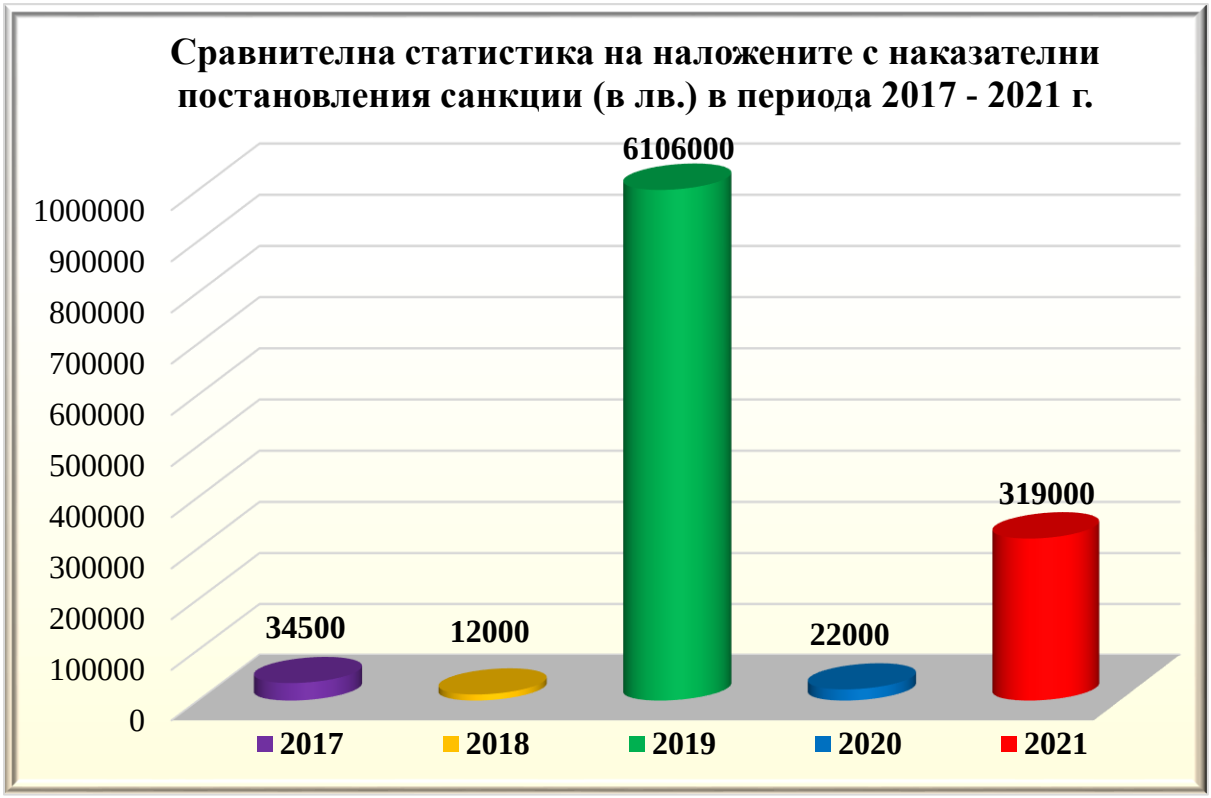
Фиг. 7

5. Административнонаказателни производства.

Въз основа на извършени проверки по искания и сигнали за 2021 г. са съставени **5** акта за установяване на административни нарушения и са издадени **4** наказателни постановления.

Наложените санкции при извършени проверки по искания и сигнали са в размер на **319 000** лв. От издадените наказателни постановления **едно е** влязло в сила и е платено, **3** бр. са обжалвани и се намират в съдебна фаза. В сравнение с 2020 г. наложените санкции като размер са с 297 000 лв. повече на фона отсъствието на големи пробиви в сигурността на администратори, обработващи големи бази данни, като НАП през 2019 г.

На графиката е изобразена сравнителна статистика на наложените санкции с наказателни постановления в периода 2017 – 2021 г. проверки (фиг. 8).



Фиг. 8

През 2021 г. с наказателни постановления (НП) на председателя на КЗЛД са наложени санкции на стойност 319 000 лв. В процес на принудително събиране от НАП към 31.12.2021 г. са санкции, наложени с НП, в размер на 81 200 лв., като през 2021 г. е събрана сума в размер на 4961,78 лв. От наложените с НП санкции през 2021 г. една е платена доброволно в размер на 3000 лв.

Видно от приложените диаграми и сравнителен анализ от въвеждането на Регламента сигналите от 290 бр. през 2018 г. са удвоили размера си, и то без наличие на големи пробиви в сигурността на личните данни през 2021 г. като този на НАП от 2019 г. През 2021 г. са постъпили 487 сигнала и запитвания. При проверките има неколкократен ръст, от 68 бр. проверки през 2018 г. и 37 бр. през 2017 г. на фона на прилагането на Регламент 2016/679 проверките за 2021 г. са 206 бр., извършени от възложени 227 бр. Проверките на територията на цялата страна се извършват от 4 екипа по двама служители съгласно изискванията на ЗАНН.

6. Уведомления за нарушения на сигурността на личните данни.

6.1. Статистика и анализ на получените уведомления.

Един от важните елементи в контролната дейност на КЗЛД е свързан с уведомленията по чл. 33 от Регламент (ЕС) 2016/679. Администраторът в случай на

нарушение на сигурността на личните данни без ненужно забавяне – но не по-късно от 72 часа след като е разбрал за него, освен ако не съществува вероятност нарушението да породи риск, е длъжен да уведоми надзорния орган, а в някои случаи и физическите лица, субекти на данни, за настъпили нарушения на сигурността на данните. Съгласно определението в Регламента – „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин“. Следва да се отбележи, че в зависимост от обстоятелствата нарушението може да засегне поверителността, цялостността и наличността на личните данни, както и каквато и да е комбинация от тях. Регламентът задължава администратора да оцени рисковете с различна вероятност и тежест и да приложи всички подходящи технически и организационни мерки за защита правата на субектите. Установяването на нарушение и своевременното информиране на надзорния орган и на субектите на данни са свързани с отчитането на естеството и тежестта на нарушението и последиците, както и с оценяването на неблагоприятното въздействие от тях върху субектите на данни.

С цел подпомагане на администраторите при уведомяване на надзорния орган за настъпило нарушение на сигурността, както и за по-добро ориентиране и улеснение при изпълнението на това тяхно задължение през 2021 г. КЗЛД одобри образец на уведомление. На институционалния сайт в рубриката „Подаване на уведомление“ може да бъде намерена информация за начините за подаване на такова, както и самият образец.

В изпълнение на чл. 15 от ЗЗЛД и чл. 62 от Правилника за дейността на Комисията и на нейната администрация КЗЛД регистрира уведомленията за нарушение на сигурността на личните данни в съответния регистър и извършва анализ за наличие на информацията по чл. 33, §3 от Регламент (ЕС) 2016/679, както и определя нивото на риска съгласно Методика за оценка на риска при нарушение на сигурността на личните данни, приета от Комисията.

За отчетния период в КЗЛД са получени общо 140 уведомления за нарушения на сигурността на данните, като 62 от тях са свързани с нарушение на сигурността на данните в информационна система, обслужваща и ползвана от множество самостоятелни администратори на лични данни, които съгласно изискванията на Регламента са длъжни да подадат към надзорния орган индивидуални уведомления.

От общо подадените уведомления с ниско ниво на риск са преценени 10 уведомления. Това са случаите, в които вероятността от нарушението на сигурността на личните данни за субекта на данни да настъпят имуществени или неимуществени вреди е

малка или незначителна. По такива случаи не се предприемат допълнителни действия от страна на надзорния орган.

Със средно ниво на риск са преценени 81 уведомления, в т.ч. 62 (посочени по-горе), касаещи едно и също нарушение. Касае се за случаи, при които вероятността за субекта на данни да настъпят имуществени или неимуществени вреди в резултат на нарушението на сигурността на личните данни е голяма или много голяма и/или тези вреди включват незначителни финансови загуби, незначителни икономически или социални неблагоприятни последствия, накърняване на репутацията, разкриване, разпространяване или осигуряване на неразрешен достъп до лични данни по чл. 9, пар. 1 или чл. 10 от Регламент (ЕС) 2016/679, автоматизирано вземане на решение, което може да породи правни последствия за отделен субект на данни или по подобен начин да го засегне в значителна степен, вкл. профилиране, лишаване на субекта на данни от контрол върху негови лични данни, незначително засягане на права или свободи на едно или повече физически лица. В тези случаи се извършва проверка по документи, като се изисква от администратора представяне на допълнителна информация. След получаване на информацията случаите отново се разглеждат и преценяват. Осъществени са 81 такива проверки, в т.ч. по посочените 62 уведомления за нарушения на сигурността на личните данни, свързани с едно и също нарушение, засягащо множество администратори.

С високо ниво на риск са оценени 6 уведомления, т.е. вероятността за субекта на данни да настъпят имуществени или неимуществени вреди в резултат на нарушението на сигурността на личните данни е сигурна или значителна и/или тези вреди включват кражба на самоличност, измама с фалшива самоличност, финансови загуби, значителни икономически или социални неблагоприятни последствия на едно или повече физически лица, лишаване от права или свободи на едно или повече физически лица, автоматизирано вземане на решение, което може да породи правни последствия за множество субекти на данни или по подобен начин да ги засегне в значителна степен, вкл. профилиране, или когато вредите засягат голям брой субекти на данни или уязвими лица или се засяга голям обем лични данни. В тези случаи Комисията извършва проверка на място при администратора.

При 14 от случаите, свързани с нарушения на сигурността на личните данни, има трансгранично обработване, което налага на основание чл. 56 от Регламента КЗЛД да се конституира като засегнат надзорен орган (ЗНО) и да се регистрира като такъв в Информационната система на вътрешния пазар (ИСВП).

На фиг. 9 е представено процентното съотношение на постъпилите уведомления за нарушение на сигурността на данните и съответното решение на КЗЛД. Най-висок е

процентът на случаите, за които при анализа е установено средно ниво на риск – 58%. Случаите на инциденти с ниско ниво на риск са 7%, а с високо ниво на риск са 4%. КЗЛД е ЗНО в 10% от случаите, като 21% са „други“ случаи.

Фиг. 9

В частта „други“ са 29 от уведомленията, които са преценени, както следва: 7 на застрахователни дружества, които препредават информация без засягане на данни, 5 на основание чл. 261в от ЗЕС, по които Комисията не е компетентна да се произнесе и ги приема за сведение, и 9, по които е установено, че няма реален пробив в сигурността на данните. Тук са включени и 3 случая на уведомления, които са приобщени към преписки по сигнали, касаещи същото нарушение. Една преписка е изпратена по компетентност и за съдействие до отдел „Киберпрестъпност“ на ГДБОП към МВР. Висящи са 4 преписки, които също влизат в това число.

Натрупаните данни по отношение на преценения риск за правата и свободите на засегнатите от нарушенията субекти на данни през годините (фиг. 10) показват тенденция за намаляване на „високия“ риск. За периода от началото на прилагане на ОРЗД броят на регистрираните в КЗЛД уведомления за нарушение на сигурността на данните е сравнително еднакъв. Намаляването на „високите“ рискове сред уведомленията за

нарушение говори за повишено разбиране от страна на администраторите за задълженията им, произтичащи от приложимото законодателство в областта на защитата на личните данни, и особено за предприемането на подходящи технически и организационни мерки за осигуряване на сигурност на обработването.

Фиг. 10

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. Броят на дигиталните пробиви е 86, докато физическите са 38. В 16 от уведомленията няма установено нарушение в сигурността на данните.

А видно от разреза според причините/причинителите на нарушения в сигурността на данните (фиг. 11), най-голям процент са случаите на инциденти, свързани с външни злонамерени атаки към системите на администраторите, представляващи различни по вид киберпрестъпления, включително кражби или криптиране на бази данни, съдържащи лични данни, за което са уведомени и съответните правоохранителни органи – 69%. На следващо място с 15% са инцидентите, свързани с разкриването на данни пред трети лица вследствие на неволни технически грешки или загуба на документи, които са дигитален носител, предизвикани от човешки фактор. В 6% от случаите нарушенията са причинени от злоупотреба със служебно положение. Загубени/откраднати куриерски пратки има в 10% от случаите. В сравнение с 2020 г. прави впечатление тенденцията на нарастване на

относителния дял на нарушения, свързани с предоставянето на куриерски услуги, което предизвика отнасянето на тези случаи до знанието и на Комисията за регулиране на съобщенията като орган, контролиращ сигурността на пощенските услуги, за предприемане на действия по компетентност.

Фиг. 11

Прави впечатление и голямото разнообразие на засегнатите сектори, в които оперират подалите уведомления администратори. Сред тях от застрахователния сектор – 69 бр., като всички те са свързани с едно и също нарушение, от банки – 9 бр., софтуерни компании – 9 бр., куриерски фирми – 2 бр., интернет магазини – 3, държавни институции – 5, и др.

От регистрираните пробиви на сигурността на данните 6% засягат публични институции (държавни и образователни структури), а останалите са от частния сектор.

6.2. Извършени проверки/одити по получените уведомления.

По получените уведомления за нарушения на сигурността на личните данни компетентната дирекция от специализираната администрация е изготвила съответни

доклади за определяне нивото на риск и за засегнат надзорен орган. Изготвените констативни актове за отчетния период са 19, становищата – 13. Изготвени са и 20 решения на основание чл. 58, §2 от Регламента за налагане на корективни мерки.

6.3. Наложени мерки по чл. 58, §2 от Регламент (ЕС) 2016/679.

Във връзка с постъпили уведомления за нарушения на сигурността на личните данни по чл. 33 с решения на КЗЛД са приложени следните корективни правомощия по чл. 58, §2 от Регламент (ЕС) 2016/679:

– официално предупреждение по буква „б“ – 6 бр.;

– разпореждане по буква „г“ – 14 бр.;

– разпореждане по буква „д“ – 3 бр.;

– имуществена санкция по буква „и“ в размер на 5000 лв. – 1 бр.

Съставен е един АУАН при условията на чл. 40, ал. 4 от ЗАНН и е връчено наказателно постановление, с което е наложена имуществена санкция в размер на 8000 лв.

И двете наложени имуществени санкции са изплатени.

Издадените разпореждания са за прилагане на подходящи технически и организационни мерки за осигуряване ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване, срещу случайна загуба и неоторизиран достъп до личните данни на физически лица; обучение на служителите по отношение на работата с лични данни; спазване на разпоредбите на чл. 34 от Регламента за уведомяване на субектите на данни в случаи на нарушение на сигурността на личните данни и др.

Обжалвано е едно решение на Комисията във връзка с нарушение на сигурността на данните, по което предстои произнасяне от ВАС.

7. Предварителна консултация с КЗЛД по чл. 36, пар. 1 – 3 от Регламент (ЕС) 2016/679.

Предварителната консултация по чл. 36 от Регламент (ЕС) 2016/679 е част от контролните функции на КЗЛД и е в пряка връзка с извършването от АЛД/ОЛД на оценка на въздействието върху защитата на данните (ОВЗД) по чл. 35 от ОРЗД.

Самата ОВЗД е процес, чиято цел е да опише обработването на лични данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, като ги оцени и определи мерки за справяне с тези рискове. Тя представлява и важен инструмент за отчетност на АЛД, че са предприети подходящи мерки за гарантиране на спазването на Регламента.

Минималното съдържание на ОВЗД е посочено в чл. 35, параграф 7 от Регламента, а в параграф 3 на същата норма се посочва кога задължително следва такава да се извърши. На сайта на КЗЛД е публикуван и „Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните съгласно чл. 35, пар. 4 от Регламент (ЕС) 2016/679“. ОВЗД следва да се направи, преди да започне самото обработване, а задължено да извърши ОВЗД лице е администраторът на лични данни заедно с длъжностното лице по защита на данните, ако има определено такова.

Когато ОВЗД констатира, че остатъчните рискове са високи и администраторът не може да установи достатъчни мерки за намаляване на тези рискове до приемливо равнище, задължително се осъществява консултация с надзорния орган. Преди да започне консултацията, АЛД представя на надзорния орган цялата информация, посочена в чл. 36, параграф 3 от Регламента и чл. 58, ал. 2 от ПДКЗЛДНА.

Целта на предварителната консултация по чл. 36 от Регламента е да се определят подходящи технически и организационни мерки, които да понижат високото ниво на риск, показано от ОВЗД, до приемливи за целта на обработването нива. В този процес на комуникация между администратора на лични данни и надзорния орган последният може да използва всяко от правомощията си по чл. 58 от Регламента, за да ограничи или спре такова обработване, докато администраторът не набележи подходящи технически и организационни мерки за намаляване на високия риск до приемливо равнище.

През 2021 г. Комисията е била адресат на две искания за предварителна консултация по чл. 36 от ОРЗД. В първия случай АЛД иска становището на Комисията във връзка с предприети действия, касаещи комуникацията с потребителите му. Поради това, че липсват описаните по-горе предпоставки за приложимост на производството по чл. 36 от Регламента, Комисията е установила, че не става въпрос за предварителна консултация. След анализ на преписката КЗЛД е изпратила на АЛД свои коментари и предложения, които могат да бъдат взети предвид, без да представляват становище на Комисията в хода на предварителна консултация.

Вторият случай, с който КЗЛД е сезирана през 2021 г., е във връзка с предоставяне на цялата база данни с чувствителни данни, поддържана от АЛД на законово основание, на друг АЛД, който е в кръга на лицата, които по принцип имат безвъзмезден достъп до същата, с цел базата данни да се интегрира с такава поддържана от втория АЛД. Тъй като визираната миграция представлява мащабно обработване на лични данни (засяга данните на 1 400 000 лица), от първия АЛД е извършена оценка на въздействието върху защитата на личните данни, чийто резултат е показал наличие на остатъчен висок риск за правата и свободите на засегнатите физически лица.

С оглед необходимостта от пълното изясняване на фактическата и правна обстановка по случая Комисията е изискала допълнителна информация, уточняваща целта на миграцията на данните, тяхната пропорционалност по отношение на целта и във връзка с какви законови функции на втория АЛД се изисква.

Основен елемент от характеристика на качеството на един АЛД е безспорното изясняване на факта, че същият носи отговорността по чл. 24 от ОРЗД, т.е. той следва да е отговорен за въвеждането на подходящите технически и организационни мерки, чрез които да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с нормативните изисквания за защита на личните данни; той взема предвид естеството, обхвата, контекста и целите на обработването, както и той оценява рисковете с различна вероятност и тежест за правата и свободите на физическите лица.

След анализ на преписката е установено, че за втората база данни не може да се установи безспорна правна регламентация за нейното поддържане, което се явява предпоставка за възникване на спор по отношение на правомощията по обработване на личните данни на физическите лица между двамата АЛД като отделни АЛД (в случая публични органи) с определени от специалното законодателство задачи и правомощия. Наличието на такъв спор преграждa пътя за изясняване на обективната обстановка и по повод отделните задължения на двете ведомства, свързани с обработването на лични данни, и води до обективна невъзможност за иницииране на съответното производство, а разглеждането на депозираното искане за провеждане на предварителна консултация с КЗЛД по чл. 36 от Регламент (ЕС) 2016/679 се явява недопустимо.

V. ПРОИЗВОДСТВА ПО ИЗРАЗЯВАНЕ НА СТАНОВИЩА И УЧАСТИЕ В СЪГЛАСУВАТЕЛНИ ПРОЦЕДУРИ НА НОРМАТИВНИ АКТОВЕ ПО ВЪПРОСИТЕ, СВЪРЗАНИ СЪС ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1. Обща статистика и по-интересни случаи от практиката на КЗЛД.

През изтеклата година КЗЛД е изразила 55 становища по въпроси от областта на защитата на личните данни както по искания на публични органи, така и по принципни запитвания на юридически и физически лица. Съществена част от работата на Комисията е свързана с приемането на решения, с които се разрешава предоставянето на лични данни от ЕСГРАОН на основание чл. 106, ал. 1, т. 3, предл. 3 от Закона за гражданската регистрация (ЗГР). Това правомощие на КЗЛД произтича от Закона за гражданската регистрация. През отчетния период са приети 11 такива решения.

Като по-интересен случай може да се отбележи искането за становище от Агенцията по вписванията (АВп) относно правото на изтриване по чл. 17 от ОРЗД по отношение на физически лица, които имат качеството управляващи и/или представляващи, съдружници, еднолични собственици на капитала и т.н., относно техни лични данни, съдържащи се в подлежащи на обявяване актове в Търговския регистър и регистъра на юридическите лица с нестопанска цел. От направения анализ на нормативната рамка КЗЛД стига до заключението, че за търговците и юридическите лица с нестопанска цел съществува правно задължение за предприемане на правни и фактически действия по заявяване на подлежащите на вписване и обявяване обстоятелства, свързани най-общо с представляваното от тях юридическо лице/търговец. Това задължение представлява основание за законосъобразно обработване на данните на физическите лица, въвлечени в производството, по смисъла на чл. 6, §1, б. „в“ от ОРЗД. Същевременно в изпълнение на чл. 5, §1, б. „в“ от ОРЗД описаното обработване на данни следва да се реализира при стриктно спазване на принципа за обработване само на данни, които са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“). Следователно при заявяване на факти и обстоятелства по партидата на търговец/юридическо лице обработването на лични данни чрез предаване на АВп не следва да надвишава изискуемия законов максимум от лична информация.

Успоредно с това самото предоставяне на личните данни от администратора – търговец/юридическо лице с нестопанска цел, представлява операция по обработване на данни и именно в този момент администраторът следва да прецени какъв обем данни следва да бъде публично оповестен и какъв не в зависимост от желанието за прозрачност на дейността му и при спазване на изискванията на чл. 5 от ОРЗД (необходимост,

пропорционалност, свеждане на данните до минимум и т.н.). В този случай АВп се явява „получател“ на същите данни по смисъла на легалната дефиниция на чл. 4, §1, т. 9 от ОРЗД (физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна). Видно от приложимото законодателство, АВп, като получател на данните, следи единствено за подсигуряване на тяхната публичност (една от целите на водените регистри), като проверките за законосъобразност в регистърното производство напълно изключват преглед и преценка на законосъобразността, точността и обема на лични данни на физическите лица, заявени пред АВп в лично качество.

Предвид направения анализ КЗЛД изразява становище, че АВп е администратор на Търговския регистър, но по смисъла на чл. 4, т. 9 от Регламент (ЕС) 2016/679 се явява „получател“ на данните на физическите лица, които се обработват чрез обявяване в лично, а не служебно качество на представляващ/управляващ. В този смисъл АВп не разполага с правна възможност или правомощие, служебно или по искане на субект на данни, да ограничава обработването на вече оповестени данни. Така исканията на физическите лица по реда на Регламент (ЕС) 2016/679 следва да се отправят до администратора на лични данни, заявил ги за обявяване на получателя им (АВп), доколкото на администратора, а не на получателя е преценката дали и доколко данните следва да бъдат „ограничени“. Ако тези искания са отправени до АВп, а не до администратора, заявил данните, Агенцията следва служебно да препрати искането до този администратор и да уведоми за това заинтересованото физическо лице.

Друг интересен случай през отчетния период е подадено искане за становище от председателя на Комисията за противодействие на корупцията и за отнемане на незаконно придобито имущество (КПКОНПИ). Искането за становище е свързано с изискванията на Правилника за устройството и дейността на КПКОНПИ (чл. 156, ал. 4 от него), който предвижда изчерпателно съдържание на публичния регистър по чл. 169, ал. 1, т. 3 от ЗПКОНПИ, като се уточнява, че по смисъла на същия закон всяко лице има право на достъп до данните от електронния публичен регистър при спазване на Закона за защита на личните данни и че всяко лице има право да получава информация, свързана с данните от регистрите, по реда на Закона за достъп до обществена информация. Моли се, доколкото воденето на публичен регистър представлява действие по обработване на лични данни, което следва да съответства на изискванията на Регламент (ЕС) 2016/679, за становище доколко разширеното съдържание на регистъра, в това число името и длъжността на наказаното физическо лице, не би оказало негативно влияние върху неприкосновеността на личния живот на субектите на данни.

Изводите на КЗЛД по отношение на поставения за обсъждане случай са, че данните, оповестявани по реда на чл. 169, ал. 1, т. 3 от ЗПКОНПИ от КПКОНПИ, в качеството ѝ на администратор на личните данни, при стриктно спазване на принципите по чл. 5 от ОРЗД следва да бъдат обработвани по критерии, отчитащи защитата на обществения интерес и пропорционалността на намесата в личния живот на субектите на данни. Разпространяването на имена и длъжност на лица преди влизането в сила на подлежащите на вписване в регистъра актове на КПКОНПИ, както и на лица, които не попадат в обхвата на чл. 6 от ЗПКОНПИ, води до незаконосъобразно идентифициране на субектите на данни и надхвърля целите, за които личните данни се обработват. Същевременно личните данни, оповестявани в описания регистър, следва да са предмет на периодичен преглед и снемане от публичен достъп при отпадане на необходимостта от публикуването им.

Друг интересен казус, имащ отношение и към установяване на пределите на правомощията на КЗЛД и на Инспектората към Висшия съдебен съвет (ИВСС) – надзорен орган за защита на данните по чл. 17 и сл. от ЗЗЛД, е този относно условията за законосъобразно основание за издаване на електронни квалифицирани подписи от административния ръководител на съд на съдебни заседатели към него с цел подписване на съдебни актове. При разпределяне по компетентност на искането за становище е преценено, че описаната дейност попада в обхвата на „общия“ надзор на КЗЛД, доколкото не касае самата валидност или хода на постановяване на съдебни актове, а се отнася до организация на чисто административни и служебни отношения между ръководителя на съда и съдебните заседатели. В този смисъл КЗЛД е изразила позиция, че няма пречка администрацията на съответния съд да опосреди предаването на копия от документите за самоличност на съдебните заседатели на издателите на квалифицирания електронен подпис, доколкото няма да обработва данните от копията. Направено е заключение, че административното ръководство на съда следва да реализира събирането и съхраняването на копията на документите за самоличност по начин, който не позволява обработване на данните от тях. Редът и условията на събиране и съхранение трябва да включват освен подходящи технически и организационни мерки и уведомяване на физическите лица за това опосредствано предаване на данните им, както и запознаване с обстоятелството, че съдът няма да обработва данните от тях в качеството си на администратор на лични данни. Обърнато е внимание обаче, че и самите доставчици на квалифицирани електронни услуги следва да разполагат с валидно основание по чл. 25г от ЗЗЛД, за да обработят данните от копие на документ за самоличност. При липса на такова те следва само да сверят така предоставените им данни с цел еднозначното идентифициране на титуляря на подписа и да върнат копието от документа за самоличност на администрацията на съда, която от своя

страна трябва да го унищожи по надлежния ред, като документира това действие съгласно принципа за отчетност по чл. 5 от Регламент (ЕС) 2016/679.

През отчетния период 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.

Дело C-180/21, „Инспектор в Инспектората към Висшия съдебен съвет пред Съда на Европейския съюз“, образувано по преюдициално запитване на Административен съд Благоевград, България

Преюдициалното запитване се отнася до тълкуването на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни и за отмяна на Рамково решение 2008/977/ПВР на Съвета и на Регламент (ЕС) 2016/679.

Предоставената информация е за производството по дело, образувано пред Административен съд Благоевград по жалба на *VS* срещу решение на Инспектората към Висшия съдебен съвет, което се развива по реда на чл. 145 и сл. от АПК, във вр. с чл. 38в, ал. 4 от ЗЗЛД. Спорът по главното производство се отнася по същество до твърдяно неправомерно обработване на лични данни на жалбоподателя, събрани по различни прокурорски преписки. Жалбоподателят твърди, че неправомерното обработване на личните му данни се изразява, от една страна, в използването им за привличането му в качеството на обвиняем в досъдебно производство, а от друга страна, в използването на тези данни от прокуратурата в защитата ѝ пред съд в хода на гражданско производство. Тези твърдения са били обект на разглеждане от ИВСС в качеството на надзорен орган по защита на данните при обработване на данни от съда при изпълнение на функциите му на орган на съдебната власт и от прокуратурата и следствените органи при изпълнение на функциите им на органи на съдебната власт за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания.

Изводите на КЗЛД по отделните преюдициални въпроси са, че целите за обработване на лични данни по чл. 42 от ЗЗЛД (съответно чл. 1, §1 от Директива (ЕС) 2016/680), макар и различни и изброени поотделно за постигане на изчерпателност на обхвата на Директива (ЕС) 2016/680, сами по себе си са неразделни и са съвместими помежду си по смисъла на

същата директива. Целта на обработването на личните данни не се влияе от процесуалното качество на субектите на данни, а от търсения резултат на обработването – съответно предотвратяване, разследване, разкриване и наказателно преследване на престъпление. Дадена операция по обработване може да се изчерпа и преустанови само до една цел, но може да се наложи обработване последователно за всички изброени цели. КЗЛД счита, че в конкретния случай дейностите по обработване на лични данни, макар и реализирани от компетентен орган по чл. 42, ал. 4 от ЗЗЛД, са предприети извън приложното поле на Директива (ЕС) 2016/680 и следователно попадат в обхвата на Регламент (ЕС) 2016/679. В заключение е посочено, че страните в исковото производство вече са еднозначно идентифицирани на етапа на образуване и докладване на делото. Обработване на допълнителен набор от данни, в случая на данни по чл. 10 от Регламент (ЕС) 2016/679, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност въз основа на член 6, параграф 1, може да се извършва само под контрола на официален орган, каквито се явяват и гражданските съдилища. Позоваването на такива данни и официални документи обаче следва да е предмет на тест за баланс във всеки отделен случай между легитимните интереси на администратора на данни и на правата на субекта на данни.

Преюдициално дело C-205/21, „Министерство на вътрешните работи, Главна дирекция за борба с организираната престъпност“ пред Съда на Европейския съюз, образувано по преюдициално запитване на Специализирания наказателен съд

Преюдициалното запитване се отнася до тълкуването на разпоредби от Регламент (ЕС) 2016/679 и на Директива (ЕС) 2016/680, и по-конкретно, правилното транспониране на чл. 10 и чл. 6 от нея, като в преюдициалните въпроси се твърди, че същите са транспонирани в Закона за Министерството на вътрешните работи (ЗМВР). Като цяло виждането на КЗЛД е, че чл. 10 от Директива (ЕС) 2016/680 е транспониран коректно в чл. 51 от ЗЗЛД, като условията за законосъобразност на обработването са то да е абсолютно необходимо, да е предвидено в законодателството на Република България (каквито са чл. 68 от ЗМВР и чл. 2 от Наредбата за реда за извършване и снемане на полицейска регистрация) и да са налице подходящи гаранции за правата и свободите на субектите на данни. Видно от съображенията на директивата и от ЗЗЛД, правото на преценката за необходимостта на обработването е оставено на компетентните органи по смисъла на ЗЗЛД, а подходящите гаранции при неизразяване на съгласие от страна на субекта на данни са заложени чрез въведения предварителен съдебен контрол на принудителното обработване на чувствителни данни (каквато е и трайната практика на Европейския съд по правата на човека.

По отношение на чл. 4 и чл. 8 от Директива (ЕС) 2016/680 виждането на КЗЛД е, че те са транспонирани съответно в чл. 45 и чл. 49 от ЗЗЛД. Условията за законосъобразно обработване на лични данни за целите на същата директива предвиждат това обработване да е необходимо за упражняване на правомощия от компетентен орган и да е предвидено в правото на Европейския съюз или в нормативен акт, в който са определени целите на обработването и категориите лични данни, които се обработват. Видно от изложената правна рамка, обработването е необходимо за упражняване на правомощията на органите на МВР, а самото обработване е предвидено в ЗМВР и приложимата наредба, които описват подробно всички категории лични данни, които изчерпателно и лимитативно се обработват по този ред. Преценка изцяло в дискрецията на националния законодател е за кои субекти на данни подобен род обработване на данни е необходимо за реализиране на целите на упражняване на официалните правомощия на компетентните органи. Изискване както на Регламент (ЕС) 2016/679, така и на Директива (ЕС) 2016/680 е след преценка относно необходимостта на обработването то да се реализира от правоприлагащите органи по прозрачни правила, които изключват субективен и произволен подход при и след обработването на определени данни.

Преюдициално дело C-340/21, Национална агенция за приходите пред Съда на Европейския съюз, образувано по преюдициално запитване на Върховния административен съд

Главното производство по делото е във връзка с жалба против решение на Административен съд София-град. С решението е отхвърлен като неоснователен иск против НАП с цена 1000 лв. за претърпени неимуществени вреди с правно основание чл. 82 от Регламент (ЕС) 2016/679, чл. 1, ал. 1 от Закона за отговорността на държавата и общините за вреди, чл. 203 от АПК и чл. 39, ал. 2 от ЗЗЛД. В запитването е посочено, че на 15.07.2019 г. от медиите е станало известно на цялото общество, че е осъществен неразрешен достъп до информационната система на НАП и е публикувана информация, съдържаща се в информационните бази данни на Агенцията, представляваща лични данни и данъчна и осигурителна информация. Засегнати са 4 057 328 бр. активни български граждани, като в това число е и ищцата. Пред Административен съд София-град са предявени искове на 157 физически лица против НАП с искания да бъдат присъдени обезщетения за претърпени неимуществени вреди в размер за всеки от ищците по 1000 лв.

Случаят е свързан с небезизвестния инцидент с изтичане на лични данни от системите на НАП, по който казус КЗЛД вече работи към момента на преюдициалното запитване. В този смисъл отговорите на поставените въпроси изцяло отразяват трайната ѝ

практика и съответстват на последователния ѝ подход по прилагане на нормите на Регламент (ЕС) 2016/679, както следва:

„1. Принадлежността на лицето, реализирало нарушение на сигурността на данните и на тяхното обработване, към организацията на работата на администратора на лични данни не представлява елемент от фактическия състав на нарушението на сигурността на данните или съответно на принципа за отчетност при определяне на степента на ефективност на техническите или организационните мерки, които администраторът е длъжен да въведе. И при вътрешни за администратора и при външни лица, осъществили нерегламентиран достъп, нарушението на сигурността на данните навежда на недостатъчност на предприетите технически и организационни мерки.

2. Преценка за законосъобразност на обработването на лични данни се извършва след обсъждане и преценка дали и доколко техническите и организационните мерки, въведени от администратора на лични данни както по отношение защитата на самите данни, така и по отношение на сигурността на обработването им, са подходящи.

3. Принципът за отчетност, прогласен в чл. 5 от Общия регламент относно защитата на данните, вменява именно на администратора доказателствената тежест за удостоверяване на предприети формални и фактически действия и по документирането им с цел доказване спазване на изискванията на същия регламент. Доказателствените способи в хода на съдебно производство могат да включват всички позволени такива съгласно приложимия процесуален закон.

4. Доколко и дали администраторът на лични данни носи отговорност за конкретна „хакерска атака“, е елемент на доказване по отношение на техническите и организационните мерки, които са предприети, и на преценка дали същите са „подходящи“ по смисъла на Регламент (ЕС) 2016/679. Самата норма на чл. 82 §3, доколкото е аргумент за освобождаване от деликтна отговорност, предполага по-скоро наличието на форсмажорни обстоятелства, които са извън волята и властта на администратора на лични данни, а не на „хакерска атака“.

5. Съгласно съображение 85 от Регламент (ЕС) 2016/679 нарушението на сигурността на личните данни (т.е. на чл. 24 и 25 от същия) обхваща и загубата на контрол върху личните данни от страна на субекта на данни. Същевременно наличието на нарушение по чл. 32 от същия регламент, т.е. при констатирано обработване на лични данни в нарушение на Регламент (ЕС) 2016/679 съгласно негово съображение 146, предполага субектите на данни да получат пълно и действително обезщетяване на всички претърпени вреди, като изрично се посочва, че понятието „вреда“ следва да се тълкува и прилага в широк смисъл“.

2. Сравнителен анализ на исканията за становища.

През втората година на пандемията от *КОВИД-19* надзорният орган се изправя пред редица предизвикателства, намерили отражение в исканията както на администраторите на лични данни, така и на субектите на данни. Наблюденията показват, че пандемичната криза въздейства изключително сериозно върху всички сфери на обществения живот. Не прави изключение и областта, свързана със защитата на личните данни. През 2021 г. се запазва тенденцията за нарастване броя на поставените за разглеждане казуси, свързани с различни аспекти, въздействия и ограничения, произтичащи от извънредните обстоятелства, пред които сме изправени. Около една пета от становищата, изразени през отчетния период, са във връзка с теми, провокирани пряко или косвено от пандемията и нейните ефекти върху обществените отношения, включително свързани с правата на субектите на данни и спазване изискванията на правната рамка в тази област.

На първо място следва да се подчертае, че КЗЛД в контекста на пандемичната криза разглежда принципни положения, основани единствено на нейните правомощия и задачи, произтичащи от Регламент (ЕС) 2016/679 и Закона за защита на личните данни. С поредица от становища и през 2021 г. е коментирано законосъобразното обработване на лични данни при изпълнението на въведените от министъра на здравеопазването противоепидемични мерки.

Постоянната практика на КЗЛД по темите на здравеопазването се основава на изискванията на чл. 9 от ОРЗД, с който се регламентира обработването на специални категории данни, в това число данни за здравето. Принципно положение е, че за обработването на такива данни се дължи по-специална защита, поради което е въведена изрична забрана за тяхното обработване освен в изчерпателно изредените случаи, посочени в чл. 9, пар. 2 от ОРЗД. В допълнение относно данните за здравето се налага и допълнителното изискване по смисъла на чл. 9, пар. 3 от ОРЗД същите да се обработват от или под ръководството на професионален работник, обвързан от задължението за професионална тайна по силата на правото на Съюза или правото на държавата членка.

В този смисъл въведените противоепидемични мерки следва да се изпълняват при наличието на едно от тези основания и при зачитането на всички останали изисквания на ОРЗД и ЗЗЛД. Мотиви в тази посока могат да се открият в изразените становища, като по-общественозначимите от тях са публикувани в интернет сайта на Комисията. Като надзорен орган в областта на защитата на личните данни, КЗЛД има компетентност да съблюдава и контролира дали обработването на лични данни е в съответствие с ОРЗД и ЗЗЛД, като това не включва въпроси относно необходимостта и адекватността на въвежданите

противоепидемични мерки от медицинска гледна точка, а единствено тяхното законосъобразно изпълнение тогава, когато то засяга извършването на операции по обработване на лични данни. В същото време независимо от естеството на противоепидемичните мерки трябва да се има предвид, че всички ограничения по отношение правата на субектите на данни, възникнали във връзка с обработването на техни лични данни, следва да са въведени с нормативен акт в съответствие с изискванията на чл. 23 от ОРЗД във връзка с чл. 37а от ЗЗЛД. В този дух са и Насоки 10/2020 на Европейския комитет по защита на данните относно ограниченията по чл. 23 от Регламент (ЕС) 2016/679, приети след обществената консултация на 13.10.2021 г. На официалния сайт на Комисията е налично и становище, в което подробно са изложени и разяснени правилата за законосъобразното обработване на лични данни за ваксинационния статус от страна на работодателите, включително относно данните за резултатите от тестването на работниците и служителите.

Като примери за конкретни казуси, свързани пряко или косвено с проблемите на пандемията, по които се изразяват становища през отчетния период, могат да се представят различни случаи. Един от тези казуси е по искане на министъра на труда и социалната политика по повод законосъобразността на обработването на лични данни на български граждани с оглед изпълнението на предвидено в Закона за държавния бюджет на Република България за 2021 г. задължение на държавата за предоставяне на еднократна финансова подкрепа за хранителни продукти на обособена група правоимащи лица. Същата е предвидено да се изплаща от бюджета на Министерството на труда и социалната политика по предоставена от НОИ информация за правоимащите лица. С реализацията на този законоворегламентиран ангажимент е натоварена Агенцията за социално подпомагане (АСП), като посочените институции организират дейността си по предоставянето на тази помощ в пълно съответствие с Регламент (ЕС) 2016/679 и ЗЗЛД. Ключов елемент от изпълнението на дейността е предоставянето на лични данни от НОИ и ЕСГРАОН на АСП.

При изразяване на становището КЗЛД отчита, че за изпълнението на функцията по предоставянето на социални помощи дирекциите „Социално подпомагане“ и регионалните дирекции за социално подпомагане имат право на безплатен достъп до Национална база данни „Население“, който се осигурява чрез споразумение между МРРБ и АСП, и задължително изискват по служебен път необходимата им информация от автоматизираните информационни системи на ЕСГРАОН, териториалните структури на НАП, Агенцията по вписванията, Агенцията по заетостта, НОИ и от други държавни и общински органи, както и от физически и юридически лица, като те са длъжни да я предоставят безплатно в 14-дневен срок от датата на поискването ѝ (арг. чл. 6, ал. 2 от

Закона за социалното подпомагане). От друга страна, нормата на чл. 64, ал. 2 от Закона за държавния бюджет на Република България за 2021 г. (ЗДБРБ2021) предвижда ясно задължение на НОИ за предоставяне на надлежната информация (лични данни) за правоимащите лица с оглед реализиране изплащането на финансовата подкрепа. С оглед изложените съображения КЗЛД изразява становище, че НОИ е длъжен да предостави на АСП лични данни на правоимащите лица, необходими за реализиране изплащането на финансова подкрепа за хранителни продукти на основание чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 във връзка с чл. 64, ал. 2 от ЗДБРБ2021.

Честа практика е КЗЛД да разглежда преписки по повод постъпили в различни публични органи **заявления за достъп до обществена информация**. Подобни казуси възникват, доколкото същата може да съдържа и лични данни и е необходимо да се намери точният баланс при прилагането на конкуриращите се правни норми. През отчетния период такова искане постъпи от Министерството на здравеопазването. Със заявлението за достъп до обществена информация от министерството се изисква предоставянето на имената на членовете на работни групи, комисии и съвети във връзка с избора и доставките на ваксини. Съществен елемент при разглеждането на такива случаи е да се приложат правилно нормите на Закона за достъп до обществена информация (ЗДОИ), като при това се спазват изискванията на правната рамка за защита на данните. Принципно положение е, че съгласно чл. 13 от ЗДОИ достъпът до обществена информация е свободен. Той може да бъде ограничен при определени условия. В конкретно разглеждания случай КЗЛД е изразила становище, че не са налице нормативни ограничения МЗ в отговора по искането да предостави лични данни на лицата, участвали в съответните работни групи, комисии, съвети и т.н., във връзка с избора и доставката на ваксини на основание чл. 6, пар. 1, б. „д“ от Решение (ЕС) 2016/679 (обработването е необходимо за изпълнението на задача от обществен интерес) във връзка с чл. 13, ал. 4 от ЗДОИ в обем: собствено и фамилно име, длъжност и ведомство и служебен официален адрес за кореспонденция. На МЗ са дадени и допълнителни насоки с оглед законосъобразното обработване на лични данни при предоставяне на достъп до обществена информация, които могат да се считат за принципни и приложими в други подобни случаи:

- В случай че предоставяните документи съдържат и лични данни на трети лица, които не са пряко относими към искането за достъп до обществена информация, същите следва да бъдат заличени.
- При предоставянето на копия от документи съдържащите се в тях подписи трябва да бъдат заличени.

• Предоставящият достъп до обществена информация е длъжен да предостави на засегнатите субекти на данни информация по смисъла на чл. 13 от Регламент (ЕС) 2016/679 относно извършваното обработване на лични данни, а именно – предоставянето на информация и документи при осъществяването на достъп до обществена информация.

Отново в контекста на епидемичната обстановка праз отчетния период пред КЗЛД е поставен за разглеждане **казус относно предоставянето на информация за мястото на хоспитализация** от Центъра за спешна медицинска помощ (ЦСПМ). Увеличеният обем на работа на спешните медици по време на т.нар. вълни на заразата поставя на изпитание екипите, които не могат да предоставят предварително информация на близките на пациента за мястото на хоспитализация. Като част от медицинската документация мястото на хоспитализация попада в обхвата на понятието „здравна информация“, въведено с чл. 27, ал. 1 от ЗЗдр. Анализът показва, че нито една от хипотезите на специалното национално законодателство (ЗЗдр) не е приложима в конкретния случай, следователно приложение трябва да намерят пряко правилата на общото законодателство, а именно Регламент (ЕС) 2016/679. Приложението на законодателството в областта на защитата на личните данни, доколкото с него не се въвеждат абсолютни права, налага да се отчетат всички специфични обстоятелства на конкретното обработване на лични данни. Извънредната обстановка и вълнообразният характер, свързани с натовареността на болниците в продължаващата епидемия, както и отказите на хоспитализация и спешният характер на действията на медицинските екипи на ЦСМП показват, че не съществува друг начин за близките на пациента да се информират за мястото на хоспитализация, освен да потърсят информация по телефона. Хуманното отношение както към пациента, така и към неговите близки изисква балансирано прилагане на правата по отношение на защитата на личните данни (които не са абсолютни), тъй като в тези случаи надделява защитата на по-висш интерес – живота и здравето. Следователно предоставянето на информация по телефона на близки на пациента, дори извън семейния кръг, е обработване на лични данни за здравословното състояние, необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данни е физически или юридически неспособен да даде своето съгласие по смисъла на чл. 9, пар. 2, т. в) от Регламент (ЕС) 2016/679.

Ситуацията на извънредно положение и последвалата извънредна епидемична обстановка във връзка с възникналата пандемия от *КОВИД-19* насочва през отчетния период вниманието на КЗЛД към **процесите по обработване на лични данни в сферата на здравеопазването**, включително развитието на електронното здравеопазване като приоритетна област на развитие. Вследствие от разглеждането на конкретни случаи в тази

област и изразените по тях становища се налагат и някои изводи, с които периодично се запознават компетентните публични органи. Обработването на специални категории данни в сферата на здравеопазването, които се отличават със своята чувствителност и завишен риск по отношение правата и свободите на субектите на данни, предполага задълбочен анализ и въвеждане на подходяща правна регламентация, осигуряваща съответствие с изискванията на Регламент (ЕС) 2016/679 и ЗЗЛД. Дигиталната трансформация в областта на здравеопазването като приоритетна област за развитие следва да се осъществи при наличието на стабилна правна регламентация, осигуряваща защитата наред с другите пациентски права и на правата в областта на личните данни. Особеностите на обработването на лични данни в дигитална среда следва да отчитат допълнителните предимства, но и предизвикателствата, произтичащи от използването на съвременните технологии в здравеопазването, и по-специално, вземането на автоматизирани решения, включително основани на профилиране, използването на изкуствен интелект, облачни технологии и мащабно обработване на големи обеми от данни и осигуряването на високи нива на киберзащита.

Наблюдението показва, че с оглед динамичния характер на развиващите се в здравеопазването процеси, както и поради различни обективни причини, по различни въпроси все още липсва специална уредба за вече съществуващи и функциониращи системи, което в повечето случаи пряко въздейства върху правата и свободите на субектите на данни.

На настоящия етап въз основа на практиката на КЗЛД констатациите могат да се обобщят, както следва:

- НЗИС (Националната здравноинформационна система)

– Недовършена правна рамка (липса на наредбата, предвидена в чл. 28г, ал. 6 вр. с ал. 7 от ЗЗдр), която следва да регламентира реда и условията за обработване на личните данни, в т.ч. всички параметри, свързани с това, като напр. участниците, техните роли и връзки помежду им, нива на достъп, основания, срокове, технически и организационни мерки, прозрачност и информираност, упражняване на права и т.н.

– Несъответствие между използваната терминология в ЗЗдр и понятията в НЗИС. Не е ясно какви данни се включват в понятията „електронно медицинско досие“ и „електронен здравен запис“.

– Липса на прозрачност на обработването на лични данни в НЗИС спрямо субектите на данни с оглед мащабите на обработваните данни, наличието на множество участници в системата със специфични роли и отговорности, както и произтичащите от това задължения за администраторите на лични данни с достъп до НЗИС.

– Неизяснени правила за достъп до НЗИС за различните участници в системата.

– Не са изяснени ролите и връзките на НЗИС със системите на НЗОК и НАП, както и дали има връзка с други регистри и информационни системи.

• Регистри и информационни системи в сферата на здравеопазването и тяхната взаимна свързаност

Все още не са изчерпателно дефинирани и правно регламентирани всички регистри в системата на здравеопазването, както и някои функциониращи или в процес на разработване информационни системи. Пример за това са системи, свързани с дейността на НЕЛК, ТЕЛК и НЗОК, чието управление предизвиква спорове между отделните ведомства в системата на здравеопазването, дублиране на базите данни, а оттам и повишаване на риска за правата и свободите на субектите на данни.

• Специални правила за обработването и съхранението на медицинската документация

Констатира се, че липсва специална правна уредба за обработването и съхранението на лични данни във връзка с поддържаната медицинска документация от общопрактикуващите лекари. Съществен проблем остава неяснотата за правата и свободите на субектите на данни при прекратяването на практиката на отделен личен лекар, особено при липсата на правоприемство. Доколкото досиетата, водени от общопрактикуващите лекари за отделните пациенти, формират и захранват на базово ниво информационните системи на здравеопазването, е необходимо за тях да съществуват единни правила, уредени с нормативен акт, като се отчитат изискванията на законодателството в областта на защитата на данните.

В контекста на **най-често обсъжданата тема – видеонаблюдението**, КЗЛД е сезирана с искане за изразяване на становище по въпроса налице ли е правно основание за съхранение на видеозаписи от администратор – частен охранител, за срок, по-дълъг от двумесечния, предвиден в чл. 56, ал. 4 от Закона за частната охранителна дейност (ЗЧОД). Анализът на специалната правна уредба показва, че търговците, лицензирани да извършват частна охранителна дейност, имат законово задължение да съхраняват записите от техническите средства за видеонаблюдение единствено в рамките на посочения в чл. 56, ал. 4 от ЗЧОД двумесечен срок, считано от изготвянето им. Цитираната правна норма е императивна и в съответствие с принципа „ограничение на съхранението“, формулиран в чл. 5, пар. 1, б. „д“ от Регламент (ЕС) 2016/679. С оглед правната уредба на видеонаблюдението с охранителна цел съхранението на записите за по-дълъг период от предвидения в ЗЧОД е допустимо само при наличието на изрично самостоятелно основание за законосъобразно обработване на лични данни.

В началото на 2021 г. Комисията за защита на личните данни е **сезирана с искане за становище от МОН,** с което се поставя въпрос за подписване на документи от служители в администрацията с квалифициран електронен подпис и предоставянето им в електронна среда за целите на документооборота. В контекста на изискванията на законодателството и предприемането на стъпки за дигитализация на предоставяните административни услуги въпросите за електронната идентификация са от решаващо значение. След задълбочен анализ на материята и анализ на приложимото законодателство – Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, КЗЛД стига до извода, че липсва нормативно изискване и съответното правно основание ЕГН на титуляря на КЕП да е видим при подписване на електронни документи. Нещо повече, в такива случаи следва да се обръща внимание на доставчика, предоставил съответните електронни удостоверителни услуги, с цел предприемането на действия по преустановяване на визуализацията на ЕГН на титуляря на КЕП при подписване на електронни документи.

През 2021 г. КЗЛД разглежда и **искане от Държавната агенция за закрила на детето** по въпроси относно защитата на личните данни, свързани с изпълнението на проекта „Координиран отговор към насилието и пренебрегването на деца чрез минимална база от данни – от планирането към практиката“ – *CAN-MDS II*, финансиран по програма „Права, равенство и гражданство“ на ЕС. Освен насоките, дадени във връзка със законосъобразното обработване на лични данни при изпълнение на проекта, КЗЛД изразява становище по конкретно поставените въпроси относно съгласието като основание за обработването на данни, обмена на данни между страните по проекта, както и изясняване ролите на Държавната агенция за закрила на детето и Агенцията за социално подпомагане като съвместни администратори на лични данни за целите на изпълнението на проекта.

През отчетния период КЗЛД има възможност да разгледа казус за **постоянното съхранение в държавните архиви** (чрез Държавна агенция „Архиви“) на писмата от конкурса „Най-красивото писмо до Дядо Коледа“, организиран от „Български пощи“ ЕАД. При анализа на правната рамка, относима към случая, се взети предвид разпоредбите на чл. 89 във връзка със съображение (156) от преамбюла на Регламент (ЕС) 2016/679, чл. 25н от Закона за защита на личните данни, както и специалните изисквания на Закона за националния архивен фонд. Съществен елемент от законосъобразното обработване на данните е статутът на администратора на данните „Български пощи“ ЕАД – публична институция с действителен собственик Министерството на транспорта, информационните технологии и съобщенията, провеждала конкурса в продължение на 26 години и

съхранявала писмата под формата на архивна сбирка (арг. чл. 33, ал. 2 от Закона за националния архивен фонд). КЗЛД изразява становище, че „Български пощи“ ЕАД може да предостави получените писма от конкурса „Най-красиво писмо до Дядо Коледа“ на Държавна агенция „Архиви“, като дава насоки и за предприемането на конкретни технически и организационни мерки за защита правата на субектите на данни, които в случая са деца. Материалите от конкурса се предоставят на ДА „Архиви“, без да съдържат данни за адресите на децата участници. Допустимо е да се съдържат имената на авторите на съответните писма. Пликовете за писма, които съдържат личните данни на подателите (деца, родители и др.), не следва да бъдат предавани за архивиране ведно със съдържанието. Съществен елемент при обработването на лични данни за целите на архивирането в обществен интерес е то да се осъществява в съответствие с принципите на Общия регламент относно защитата на данните.

През отчетната 2021 г. КЗЛД е сезирана с **искане за становище от главния секретар на Народното събрание на Република България** със следния въпрос: „Следва ли в рамките на осъществяване на парламентарната дейност да бъдат определени експлицитно (на базата на възложените им с нормативен акт задачи и дадени правомощия) или на базата на оценка на „фактическото влияние“ при определяне на целта и средствата за конкретна операция по обработка на лични данни ролите и отговорностите на парламентарните групи, парламентарните комисии и народните представители в качеството на администратори на лични данни по смисъла на чл. 4, т. 7) от ОРЗД?“. Разглежданият казус е от съществено значение за задълбочения анализ и изясняване на понятието администратор на лични данни, което има своите специфични особености.

Комисията има принципното разбиране, че правната фигура на администратора на лични данни е ключова за определяне и точното прилагане на законодателството за защита на личните данни. В случая НС е конституционно установен върховен представителен орган на държавната власт, който изразява волята на народа и неговия суверенитет. Народното събрание организира и осъществява дейността си въз основа на Конституцията и разпоредбите на Правилника за организацията и дейността на Народното събрание (ПОДНС). От своя страна, ПОДНС, приет на основание чл. 73 от Конституцията, макар и да не е озаглавен като „Закон“, е нормативен акт, който има задължителна сила за държавните органи, организациите и гражданите, и същият стои паралелно със закона в йерархията на нормативните актове (Решение №7/2010 на КС). В тази връзка както Конституцията на Република България, така и ПОДНС конституират НС и регламентират неговата дейност като единен орган на държавна власт, в чиято структура попадат

парламентарната дейност от парламентарните групи, постоянните и временните комисии и народните представители.

Определянето на администратора не е самоцелно, а в конкретния случай произтича от възложените му от КРБ и ПОДНС функции и правомощия, които биха могли да обуславят дейности по обработване на лични данни. От своя страна, организационни единици на НС – парламентарните групи, постоянните и временните комисии и народните представители, нямат самостоятелна правосубектност извън неговата организация. Този съществен белег обуславя способността да се носи юридическа отговорност, която е присъща характеристика на всеки администратор на лични данни (арг. чл. 24 от Регламент (ЕС) 2016/679). Подобен структурнодиференциран подход би довел до налагането на различни режими за обработване на лични данни и защита правата на субектите на данни в рамките на НС, което би било несъвместимо с действащото законодателство в тази област. Евентуалното определяне на парламентарните групи, постоянните и временните комисии и народните представители като самостоятелни администратори би довело до невъзможност за реализиране на административнонаказателна отговорност (глоба или имуществена санкция) по смисъла на чл. 83 от Регламент (ЕС) 2016/679, включително и поради липсата на самостоятелен бюджет на същите. По тези съображения КЗЛД е изразила становище, че парламентарните групи, постоянните и временните комисии и народните представители, като организационни единици на Народното събрание, не могат да бъдат самостоятелни администратори на лични данни.

Чрез Министерството на икономиката в КЗЛД е постъпило искане за **изразяване на становище относно допустимостта на продажбата на алкохол и цигари чрез автомати**, оборудвани с видеоконтрол и дистанционен достъп от оператор съгласно българското законодателство. С оглед комплексния характер на искането, за да се произнесе по него, КЗЛД е разгледала приложимото законодателство (Закона за тютюна, тютюневите и свързаните с тях изделия (ЗТТСТИ), Закона за виното и спиртните напитки, Закона за храните, Закона за здравето) в тази област и е изложила мотиви по отношението на обработването на лични данни. Комисията изразява становище, че обработването на лични данни, което би могло да произтече от дейностите, забранени с чл. 30, ал. 2, т. 10 от ЗТТСТИ, е незаконосъобразно поради липса на правно основание, респективно противоречие с принципа, посочен в чл. 5, пар. 1, б. „а“ от Регламент (ЕС) 2016/679. По отношение продажбата на алкохол, в случай че законодателството допуска продажбата му да се извършва чрез вендинг машини или автомати, проверката на данни от документа за самоличност, извършвана чрез отдалечен достъп посредством видеоконтрол, следва да се счита за обработване на лични данни по смисъла на чл. 4, т. 2) от Регламент (ЕС) 2016/679,

респективно да отговаря на всички негови изисквания за законосъобразност. В този случай администраторът не трябва да извършва действия по копиране, сканиране или съхранение на изображение на документа за самоличност и/или личните данни, съдържащи се в него, тъй като това би представлявало нарушение на законодателството за защита на личните данни. Становището на КЗЛД затвърждава принципни положения, от една страна, че защитата на правата на субектите на данни зависи пряко от законосъобразния характер на целите на конкретното обработване на лични данни, и от друга – да се отчита разпоредбата на чл. 25г от ЗЗЛД, според която администратор или обработващ лични данни може да копира документ за самоличност само ако това е предвидено със закон.

Разпоредбата на чл. 25г от ЗЗЛД намира съответното приложение и при **разрешаването на казуса, поставен от Патентното ведомство**, относно изискването Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означения за посочване на ЕГН при подаването на заявка за регистрация на марка или на географско означение, когато заявителят е физическо лице. Това изискване произтича от дефинирането на марка, регламентирано с чл. 9, ал. 1 от Закона за марките и географските означения. Видно от законовите разпоредби, важен елемент от придобиването на права по Закона за марките и географските означения, както и за тяхната защита, е еднозначното идентифициране на заявителя на тези права. Такава функция има ЕГН, който е административен идентификатор, служещ за еднозначна идентификация на физическо лице. В заключение КЗЛД посочва, че изискването на Наредбата за оформяне, подаване и експертиза на заявки за регистрация на марки и географски означения да се предоставя ЕГН при регистрация на марка или географско означение представлява законосъобразно условие за обработването му според хипотезата на чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679, а именно – обработването е необходимо за спазване на законово задължение, което се прилага от администратора въз основа на Закона за мерките и географските означения.

През отчетния период КЗЛД е имала възможност да направи анализ и на въпроса **дали и в каква степен Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация противоречи на императивните правила и законни цели, установени с ОРЗД,** и дали пряко нарушава законоустановената независимост на длъжностното лице по защита на данните при изпълнение на неговите задачи. Въпросът е насочен към изследването на паралелното действие на два режима, привидно в колизия, от една страна, оценяване работата на длъжностното лице по защита на данните, от друга – гаранциите същото да не получава никакви указания, да не бъде освобождавано или санкционирано при изпълнение на възложените му от ОРЗД задачи. Съществен елемент от независимостта на длъжностното лице по защита на данните е, че

същото „се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни“ (чл. 38, пар. 3 от ОРЗД). Дори когато длъжностното лице по защита на данните съвместява и друга заемана длъжност, същото подлежи на оценка, извършена от съответния пряк ръководител, който в случая, за да бъде изпълнено условието на ОРЗД, е ръководителят на организацията. Това разбиране напълно съответства на изискванията на чл. 4, ал. 1 от Наредбата за условията и реда за оценяване изпълнението на слу жителите в държавната администрация, в който се посочва, че оценяващ е ръководителят, на когото съответният служител е непосредствено подчинен – в случая длъжностното лице по защита на данните трябва да бъде оценявано като държавен служител, заемащ длъжността длъжностно лице по защита на данните, съгласно Класификатора на длъжностите в администрацията пряко от органа по назначаването. В този смисъл предвиденият механизъм за оценка на държавен служител, заемащ длъжността длъжностно лице по защита на данните, не противоречи на изискването за неговата независимост по чл. 38, пар. 3 от Регламент (ЕС) 2016/679.

В рамките на 2021 г. КЗЛД е разгледала **искане на министъра на финансите от първото служебно правителство** за годината. Искането е свързано с постъпили в Министерството на финансите предложения за промени в Наредбата за определяне на реда, начина, сроковете и обхвата на подлежащата на публикуване информация от Системата за електронни бюджетни разплащания (СЕБРА), приета с постановление на Министерския съвет през 2016 г. КЗЛД е обърнала внимание, че Регламент (ЕС) 2016/679 не обхваща обработването на данни, които засягат юридически лица, и по-специално, предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка с юридическото лице. Становището на КЗЛД се базира на принципните положения, че правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа за пропорционалност. При изразяване на становището е взето предвид, че доколкото с предложенията се засягат пряко правата и свободите на лицата във връзка с обработването на техни лични данни, тези правила трябва да са предмет на закон, тъй като чрез него се уреждат първично или въз основа на Конституцията на Република България обществени отношения, които се поддават на трайна уредба (арг. чл. 3, ал. 1 от Закона за нормативните актове). В мотивите към становището се посочва и че предвидената информация попада в обхвата на чл. 62, ал. 2 от Закона за кредитните институции, според който фактите и обстоятелствата, засягащи наличностите и операциите по сметките и влоговете на клиентите на банките са банкова тайна, като се предвижда обща забрана за разгласяването ѝ освен по предвидения специален

ред за изключения от тази забрана, както и на чл. 72 от Данъчно-осигурителния процесуален кодекс, които определят тази информация като „данъчна и осигурителна информация“ и тя се предоставя по реда на ДОПК. Така КЗЛД стига до извод, че предложението е в противоречие с редица правни норми, регламентиращи обработването на лични данни и специалния ред за обработването на данъчна и осигурителна информация и опазването на банкова тайна, доколкото същите съдържат и лични данни.

3. Становища по законодателни инициативи. Участие в процедури по съгласуване на проекти на нормативни актове.

В рамките на процедурата по външноведомствено съгласуване на проекти на нормативни актове през 2021 г. КЗЛД изразява становище по проект на Закон за допълнение на Закона за митниците. Проектът предвижда в случаите на представителство на физическите лица – български граждани, и на юридическите лица, вписани в Търговския регистър и регистъра на юридическите лица с нестопанска цел, както и в регистъра БУЛСТАТ, Агенция „Митници“ да издава автоматично *EORI* номер, като използва ЕГН, съответно ЕИК или код по БУЛСТАТ, след идентификатора на държавата. След направен анализ на предходната законодателна рамка и на действащата такава към момента на подаване на искането за изразяване на становище, и по-конкретно, Наредба №Н-9 от 7 ноември 2018 г. за регистрите, водени от Агенция „Митници“, КЗЛД е установила, че няма предвиден конкретен формат на съдържание освен този по чл. 23, ал. 2, а именно: *EORI* номерът, издаден в Република България, е с формат: *BG* (идентификатор на държавата) и уникален идентификатор в Република България. Следователно се налага изводът, че уникалният идентификатор не е пряко и нормативно свързан с единния граждански номер на физическото лице. Като отчита набора от информация, която ЕГН разкрива, както и нормата на чл. 25ж от Закона за защита на личите данни, КЗЛД изразява виждане, че следва да се предвиди ред за генериране на *EORI* номер за физически лица, като се избегне той да възпроизвежда в цялост ЕГН на тези лица. Заключението на надзорния орган е и че предвид възможното публично оповестяване и евентуални трансфери в трети държави на информацията от *EORI* номера няма пречка ЕГН на лицето да се използва за автоматизирано генериране на номер, като част от цифрите се заменят с други контролни знаци и/или символи.

На основание чл. 34 във вр. с чл. 32 от Устройствения правилник на Министерския съвет и на неговата администрация през 2021 г. КЗЛД съгласува пакет от документи, изпратен от постоянния секретар на Министерството на външните работи на Република България, във връзка с подготовката на Проект на РМС за определяне на заместник

министър-председателя по управление на европейските средства за координатор по участието на България в Комитета по политика в областта на цифровата икономика на Организацията за икономическо сътрудничество и развитие (ОИСР) и неговите работни групи за одобряване на намерението на Република България за присъединяване към Препоръката на Съвета на ОИСР за изкуствения интелект, за одобряване на намерението на Република България за повишаване на статута на България в Комитета по политика в областта на цифровата икономика и за създаването на Междуведомствена работна група по цифровизация и изкуствен интелект към Междуведомствения координационен механизъм за присъединяване на Република България към ОИСР. С предложения проект на Решение на Министерския съвет е създадена Междуведомствена работна група по цифровизация и изкуствен интелект (МРГЦИИ) към Междуведомствения координационен механизъм за присъединяване на Република България към ОИСР, като председателят на Комисията за защита на личните данни е член в него. МРГЦИИ има за задачи да осигури активно и кохерентно участие на България в заседанията на Комитета и работните му органи, както и да извърши обстоен анализ на целесъобразността и възможностите за поетапно присъединяване на Република България към всички правни инструменти, които се разглеждат като част от условията за придобиване на статут на „асоцииран член“ в Комитета по политика в областта на цифровата икономика на ОИСР. Участието на България в Комитета по политика в областта на цифровата икономика на ОИСР, който е място за обмяна на опит, добри практики и изработване на глобални стандарти и препоръки за политики, ще има положителен ефект не само върху кандидатурата ни за членство в ОИСР, но и по отношение на способността на икономиката и обществото ни да се адаптират към новите реалности.

4. Преглед на националното законодателство за съответствие с правилата за защита на личните данни.

След стартиране прилагането на новата правна рамка в областта на защитата на личните данни, считано от май 2018 г., за Европейската комисия е въведено задължение за провеждане на периодична оценка и преглед на изпълнението им в държавите членки. През изминалите две години КЗЛД взема участие в серия двустранни разговори с представители на Европейската комисия, чиято цел е установяване на степента на съответствие на действащото в страната законодателство с изискванията за осъвременените правила за защита на личните данни. В хода на разговорите неведнократно е подчертано задължението на надзорните органи за защита на личните данни да наблюдават и осигуряват прилагането на Общия регламент относно защитата на данните по начин, който гарантира правна

сигурност и предвидимост, законосъобразност и добросъвестност. С цел гарантиране на всеобхватност на прегледа на българското законодателство през 2021 г. КЗЛД извършва анализ на действащата в Република България правна уредба, имаща отношение към обработването на лични данни и към променените изисквания в тази област. За пълнотата на анализа спомагат и множеството запитвания, жалби и сигнали, с които КЗЛД е сезирана в хода на своята дейност както по теми от обществен интерес, така и по въпроси, свързани с индивидуални казуси на администратори на лични данни и физически лица.

Въпреки че привеждането на националното законодателство в съответствие с правната рамка в областта за защита на данните от 2016 г. е постоянен процес, към края на 2021 г. КЗЛД успява да идентифицира няколко конкретни области на несъответствие, които условно могат да бъдат групирани, както следва:

1. необходимост от актуализация на законови и подзаконови актове по същество с цел отразяване на прякото действие на Регламент (ЕС) 2016/679 и променената с него правна рамка в областта на защитата на личните данни;

2. необходимост от правно-технически промени в редица нормативни актове с цел съобразяване с прякото действие на Регламент (ЕС) 2016/679 чрез въвеждане на общо препращане към съответните изисквания за защита на личните данни, а не посочване на Закона за защита на личните данни;

3. липса на регламентация в национален план на специални правила за обработване на лични данни в сектора на здравеопазването (подробен анализ по този въпрос е представен в т. 2 от настоящия раздел).

Направеният от КЗЛД анализ за съответствие на националното законодателство с изискванията на Европейската правна рамка в областта на защитата на личните данни не представлява изчерпателен списък на проблемните области, които се нуждаят от хармонизиране. От една страна, тази задача следва да се счита за постоянен процес и ангажимент на КЗЛД, от друга страна – е необходимо да се вземе предвид динамичният характер на законодателния процес както на европейско, така и на национално ниво.

Предвид изводите за все още съществуващо несъответствие на действащата правна уредба с изискванията за защита на личните данни, установени на европейско ниво, КЗЛД е счела за наложително да се обърне внимание на задълженията на публичните органи за съгласуване както на предложенията за нови нормативните актове, така и на предложенията за изменение и допълнение на вече съществуващи такива, когато с тях се засяга и режимът на обработване на лични данни, като се има предвид, че това задължение произтича от Регламент (ЕС) 2016/679, ЗЗЛД, Закона за нормативните актове и Устройствения правилник на Министерския съвет и неговата администрация. КЗЛД счита, че в рамките на общия

надзор за защита на личните данни и гарантиране на правата на субектите на данни тя разполага с достатъчно механизми за съдействие на публичните органи в този процес и за осигуряване прилагането на Регламент (ЕС) 2016/679 (акт с пряко приложение) в следните направления:

- съгласно чл. 36, пар. 4 от Регламент (ЕС) 2016/679 – да консултира по време на изготвянето на предложения за законодателни мерки, които да бъдат приети от националните парламенти, или на регулаторни мерки, основани на такива законодателни мерки, които се отнасят до обработването;
- съгласно чл. 36, пар. 5 от Регламент (ЕС) 2016/679 – без да се засяга чл. 36, пар. 1, правото на държавите членки може да изисква от администраторите да се консултират с надзорния орган и да получават предварително разрешение от него във връзка с обработването от администратор за изпълнението на задача, осъществявана от администратора в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве;
- съгласно чл. 12, ал. 2 от ЗЗЛД – освен в случаите по чл. 36, пар. 1 от Регламент (ЕС) 2016/679, предварителни консултации се извършват и когато се обработват лични данни в изпълнение на задача в обществен интерес, включително обработване във връзка със социалната закрила и общественото здраве. В този случай Комисията може да разреши обработването преди изтичането на срока по чл. 36, пар. 2 от Регламент (ЕС) 2016/679;
- съгласно чл. 57, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 – да дава становища в съответствие с правото на държавата членка на националния парламент, правителството и други институции и органи относно законодателните и административните мерки, свързани със защитата на правата и свободите на физическите лица по отношение на обработването;
- съгласно чл. 57, пар. 1, б. „и“ от Регламент (ЕС) 2016/679 – да наблюдава съответното развитие, по-специално, в областта на информационните и комуникационните технологии и търговските практики, дотолкова, доколкото то оказва влияние върху защитата на личните данни;
- съгласно чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 – да издава по собствена инициатива или при поискване становища до националния парламент, правителството на държавата членка или в съответствие с правото на държавата членка – до други институции и органи, както и до обществеността, по всякакви въпроси, свързани със защитата на лични данни;

• съгласно чл. 10, ал. 2, т. 1 от ЗЗЛД – да анализира и осъществява цялостен надзор и осигурява спазването на Регламент (ЕС) 2016/679, на ЗЗЛД и на нормативните актове в областта на защитата на лични данни освен в случаите по чл. 17;

• съгласно §45 от Преходните и Заключителни разпоредби към Закона за изменение и допълнение на ЗЗЛД (обн. – ДВ, бр. 17 от 2019 г.) – системите за автоматизирано обработване, използвани от компетентните органи по чл. 42, ал. 4 за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване, създадени преди 6 май 2016 г., се привеждат в съответствие с чл. 63, ал. 1 и 2 до 6 май 2023 г.

Предвид горното и с цел предприемане на мерки за гарантиране на правната сигурност на администраторите на лични данни и на правата на физическите лица при обработването на техни лични данни в края на отчетния период КЗЛД е решила да предостави резултатите от прегледа на законодателството 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 съответният нормативен акт, по отношение на който Комисията е констатирала несъответствия с правилата за защита на данните (22 бр. нормативни актове).

Като е заявила, че остава на разположение за съдействие в този процес и за неговото успешно финализиране, КЗЛД е подчертала важността на защитата на личните данни като основно право на Европейския съюз и необходимостта то да бъде адекватно гарантирано на нормативно ниво.

5. Запитвания на администратори по въпроси от областта на защитата на личните данни.

През отчетния период КЗЛД предоставя 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.

Забелязва се отчетлива тенденция на намаляване на броя, но не и за преустановяване на запитванията относно отпадналата през 2018 г. задължителна регистрация на администратори на лични данни. Същевременно запитванията на физическите лица, постъпили по телефона за консултации по прилагането на Регламент (ЕС) 2016/679 и на националното законодателство за защита на личните данни, изискват все по-голяма конкретика по отношение на разграничаване обработването на лични данни за чисто лични и домашни цели, условията за законосъобразно обработване на лични данни в условията на

съвременните технологични решения, както и предаването на лични данни към трети държави и международни организации.

В отчетния период бяха разгледани и различни казуси, по които голяма част от въпросите са насочени към законосъобразното предоставяне на данни в трети държави (т.нар. трансфери на данни). Наред с въпросите и последствията, възникнали по повод на решението на Съда на ЕС по случая „Шремс II“ и станали повод за редица дискусии и разяснения, КЗЛД е разгледала интересен казус, съчетаващ предизвикателствата както на трансферите, така и на отдалеченото полагане на труд в условията на пандемия.

Повдигнатият въпрос е дали е налице трансфер на лични данни, в случай че служител на работодател, ситуиран в България, полага труд от разстояние от трета държава и има достъп до системата с данни на работодателя си. Отговорът предполага детайлно изясняване на същността на трансферите, както и тяхното въздействие върху правата и свободите на субектите на данни. Изходната точка при разглеждането на такива казуси е, че предаването на лични данни в трети държави се осъществява само при условие че са спазени другите разпоредби на Регламент (ЕС) 2016/679 (спазване на принципите по чл. 5, наличие на основание за обработване по чл. 6, пар. 1 и/или по чл. 9, пар. 2, предприемане на технически и организационни мерки, извършване оценка на въздействието върху защитата на личните данни и т.н.) и само ако администраторът и обработващият лични данни спазват условията по Глава V. По конкретно поставения въпрос е взето предвид, че разгледаните правила (относно трансферите на данни) не се прилагат, в случай че служител на работодател, установен в България, полага труд от разстояние или е на служебно пътуване в трета държава и достъпва системите на работодателя си. Получател на данните в такъв случай е служителят, който в отношенията с работодателя си не може да има качеството нито на администратор, нито на обработващ, тъй като работи под неговите инструкции, разрешения или ограничения. Това обаче не изключва задълженията на работодателя да изпълнява всички изисквания на Регламент (ЕС) 2016/679, като в частност прилага подходящи технически и организационни мерки за защита на данните в съответствие с чл. 24 и 32 от същия правен акт. Добра практика в тези случаи е да се въведат ясни вътрешни правила, инструкции и процедури за работа от разстояние, като служителят следва да е запознат с рисковете при обработването, включително да е предупреден да не ползва несигурни публично достъпни мрежи.

През годината са разгледани и редица случаи на разработване на информационни системи, приложения и други технологични решения, основани на различни съвременни технологии, включително изкуствен интелект, в областта на медицината (проучвания, диагностика, дистанционно предоставяне на здравни услуги и т.н.), в областта на

платежните системи и т.н. КЗЛД полага сериозни усилия за изясняването на комплексния характер на обработването на лични данни през такива системи, ролите на участниците, въздействието върху правата и свободите на субектите на данни, както и необходимостта от въвеждането още на етапа на проектирането и по подразбиране на мерки за защита на данните. Очакванията са, че наред с развитието на законодателството в тази област ще нарасне интересът и ще се повиши търсенето на насоки и консултации от страна на разработчиците и ползвателите на тези нови технологични решения.

По повод въвеждането на „зелените“ сертификати като мярка в борбата срещу разпространението на *КОВИД-19* през отчетната година в КЗЛД са постъпили редица писма с въпроси кой има право да изисква личната карта на гражданите.

Съгласно националното ни законодателство личната карта е един от документите за самоличност на гражданите. Правна уредба на тези документи е регламентирана в Закона за българските лични документи (ЗБЛД). В документите за самоличност, в конкретния случай личната карта, се съдържат редица категории лични данни (като трите имена, единния граждански номер, постоянен адрес и други подобни), които са изчерпателно изброени в ЗБЛД. Целта на включването на нормативно предвидените категории лични данни в документите за самоличност е сигурната и недвусмислена идентификация на конкретното лице, която не може да се случи по друг начин освен чрез посочване на лични данни. Тоест по необходимост дадени категории лични данни се включват в съдържанието на документите за самоличност, за да могат те да изпълняват нормативно регламентираната им цел. В чл. 6 от ЗБЛД е предвидено, че гражданите са длъжни при поискване от компетентните длъжностни лица, определени със закон, да удостоверят своята самоличност. Следователно такива проверки могат да се извършват единствено от компетентни длъжностни лица, определени със закон (такива могат да бъдат органите на МВР, РЗИ и др.). Проверка на документите за самоличност могат да извършват и служители на дружествата, лицензирани от МВР като изпълнители на частна охранителна дейност (чл. 56, ал. 1, т. 1, б. „а“ от Закона за частната охранителна дейност). В този случай те осигуряват спазването на установения пропускателен режим за влизане и излизане от охранявания обект и вътрешния ред в него чрез проверка на документите за самоличност. Що се отнася до възможността лица, които не отговарят на изискванията на чл. 6 от ЗБЛД (напр. сервитьори, хостеси, хигиенисти и др. подобни) да извършват проверка на документа за самоличност, включително на притежателите на „зелени“ сертификати, с цел удостоверяване на тяхната самоличност, към настоящия момент такава правна възможност не е предвидена в българското законодателство.

Важно е да се подчертае, че самото представяне (показване) за проверка на документа за самоличност не попада в материалния обхват на ОРЗД, респ. не представлява обработване на лични данни. Такова би имало само ако при проверката на документите за самоличност се води запис (регистър с лични данни по смисъла на чл. 4, т. 6 от ОРЗД) или същите се обработват с автоматични средства. С промените в ЗЗЛД (изм. и доп. ДВ. бр. 17 от 26 февруари 2019 г.) се 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).

В КЗЛД постъпват и запитвания относно законосъобразността на дейности на администратор на лични данни в случаите, когато той адресира писмо (по имейл или пощата) до повече от едно физическо лице (напр. чрез вписването им в полета „до:“ или „копие до:“) и по този начин имената, имейлите и/или адресите за кореспонденция на тези физически лица станат видими за всяко едно от тях. Доколкото кореспонденцията и нейните адресати (физически лица) нямат отношение помежду си, такава практика не би съответствала на принципа за поверителност на данните, прогласен в чл. 5, пар. 1, б. „е“ от ОРЗД. Поначало в такива случаи може да се реализира неправомерно разкриване или достъп до лични данни.

Взаимодействието между правилата за защита на личните данни и тези за достъп до обществена информация за поредна година остават във фокуса на КЗЛД не само при изразяване на становища, но и в рамките на отговори по запитвания. И в тях се подчертава, че предмет на регламентация от ЗДОИ са обществените отношения, свързани с правото на достъп до обществена информация, както и с повторното използване на информация от обществения сектор. С оглед разпоредбата на чл. 2, ал. 5 от ЗДОИ обаче неговият режим не се прилага за достъпа до лични данни. Следва да се има предвид, че защитата на личните данни е и един от основните принципи, които следва да се съблюдават при осъществяване правото на достъп до обществена информация (арг. чл. 6, ал. 1, т. 5 от ЗДОИ). Видно от предметния обхват на ЗДОИ, същият урежда и повторното използване на информация от обществения сектор. Съгласно чл. 2, ал. 3 от ЗДОИ „информация от обществения сектор“ е всяка информация, обективирана върху материален носител, включително съхранена като документ, звукозапис или видеозапис, и събрана или създадена от организация от обществения сектор. Наличието на лични данни в информация от обществения сектор, която е поискана за повторно използване, в случаите, когато тази информация съставлява или е част от публично достъпен регистър, не може да е основание за отказ от предоставяне на информация от обществения сектор за повторно използване (чл. 41и, ал. 4 от ЗДОИ).

Регламент (ЕС) 2016/679 определя нормативните правила за защита на физическите лица във връзка с обработването на техни лични данни, в т.ч. и правото на достъп до тях, прогласено в чл. 15 от същия, и по ОРЗД субектът на данни може да иска достъп само до данните, свързани с него, и в този смисъл предоставянето на достъп до лични данни на трети лица въз основа на ОРЗД е недопустимо.

За поредна година КЗЛД разглежда питане, свързано с отправено искане от народен представител за предоставяне на документация, съдържаща лични данни. За да се определи дали е налице приложимо правно основание за извършване на предаването на исканите документи, следва да се разгледа и специалната нормативна уредба, регламентираща задачите и правомощията на народните представители. В този смисъл приложение в случая намира разпоредбата на чл. 138 от ПОДНС, според която държавните и местните органи и техните администрации са длъжни да оказват съдействие на народния представител и да му предоставят при поискване сведения и документи във връзка с изпълнение на правомощията му. На визираното право на народните представители да искат сведения и документи реферира тяхно задължение да пазят поверителността на информацията, получена при изпълнението на правомощията им (арг. чл. 145 от ПОДНС). Посочените разпоредби са следствие на конституционно установеното задължение на длъжностните лица и гражданите, когато бъдат поканени, да се явяват пред парламентарните комисии и да им предоставят исканите от тях сведения и документи (чл. 80 от КРБ). Следователно администраторите на лични данни са длъжни да предоставят на народния представител изисканите от тях документи, съдържащи лични данни, въз основа на чл. 138 от ПОДНС, който от своя страна представлява правно основание за законосъобразност на обработването им по чл. 6, пар. 1, б. „в“ от Регламент (ЕС) 2016/679 („обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора“).

Интересен казус представлява обработването на лични данни за нуждите на данъчното облагане при предоставяне на награди, чиято парична равностойност е по-висока от 100 лв. Комисията е сезирана от верига хранителни магазини, която при осъществяване на своята дейност и като част от рекламната си стратегия провежда игри със своите клиенти, обикновено на томболен принцип, в резултат на които връчва награди на спечелилите ги физически лица. Когато тези награди имат парична равностойност, по-висока от 100 лв., въз основа на чл. 55 във вр. с чл. 44а от Закона за данъците върху доходите на физическите лица (ЗДДФЛ) дружеството е длъжно да декларира и внася авансово дължимия данък върху наградите. За тази цел на основание на чл. 73 от ЗДДФЛ, като платец на доход, дружеството е длъжно да предостави на Националната агенция за приходите (НАП) информация за

изплатените доходи на наградените лица. Тя включва трите имена и ЕГН на наградените лица, както и данни за сумата на изплатения доход и дължимия данък. За дружеството обаче липсва законово основание да изисква копия на лични карти за осъществяване на съответната проверка предвид разпоредбата на чл. 25г от ЗЗЛД, тъй като в ЗДДФЛ не е предвидена възможност за събиране на копия от документи за самоличност. В практиката има редица случаи на грешно подадени имена и/или ЕГН. В тази връзка ЗДДФЛ въвежда за платеца на доходи административна санкция. Тъй като обаче способите за събиране на имена и ЕГН не са предвидени в ЗДДФЛ, а е налице законово основание за това по чл. 6, §1, б. „в“ от ОРЗД, за дружеството, в качеството му на администратор на личните данни, не са налице нормативни пречки при предоставяне на наградите да изисква от печелившите лица представяне на документ за самоличност с оглед снемане на необходимите данни (три имена и ЕГН) от служител на дружеството. Същото би могло да се постигне и в електронна среда (дистанционно), при условие че не се правят копия или видеозаписи на представения (за сверка) документ за самоличност. Дружеството обаче дължи предварителното и адекватно информиране (по чл. 13 или 14 от Регламент (ЕС) 2016/679) на лицата за тази операция по обработване на лични данни, тъй като е от изключително значение за гарантиране на техните права и интереси, свързани със защитата на личните им данни.

VI. УЧАСТИЕ В МЕХАНИЗМИТЕ ЗА СЪГЛАСУВАНОСТ И СЪТРУДНИЧЕСТВО В РАМКИТЕ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ЗА ЗАЩИТА НА ДАННИТЕ

1. Участие в заседанията на Европейския комитет по защита на данните и на експертните подгрупи към него.

Създаденият със започване прилагането на Регламент (ЕС) 2016/679 Европейски комитет по защита на данните (ЕКЗД) е независима европейска институция, която допринася за единното прилагане на правилата относно защитата на данните на територията на Европейския съюз, като насърчава сътрудничеството между органите за защита на данните на държавите – членки на ЕС, и държавите от Европейското икономическо пространство. Представители на КЗЛД продължават активно да участват във всички текущи процеси по изпълнение задачите на Комитета. Сред тях са и подготовката и участието на всяко едно от 15-те пленарни заседания на ЕКЗД, проведени през отчетния период – изцяло онлайн след февруари 2020 г., с изключение на присъствено проведеното през ноември 2021 г. пленарно заседание в гр. Брюксел.

С оглед осигуряване на непрекъснатост и устойчивост на дейността на Комитета продължава активното взаимодействие между експертите от националните органи по защита на данните в работните групи, подпомагащи ЕКЗД. Постигнатото пълно техническо съответствие с комуникационните системи на Комитета през предходния отчетен период позволява участие на заседанията по отделните работни групи без отделянето на определените от КЗЛД експерти от работното им място за дните на обсъжданията, обичайно провеждани в гр. Брюксел, Кралство Белгия. В резултат на проведените над 200 заседания на отделните експертни подгрупи през 2021 г. след обществено обсъждане са приети следните документи:

- Насоки 10/2020 относно ограниченията съгласно член 23 от ОРЗД;
- Насоки 07/2020 относно концепцията за администратор и обработващ лични данни в ОРЗД;
- Насоки 02/2021 относно виртуалните гласови асистенти;
- Насоки 8/2020 относно изпращането на персонализирано съдържание на потребителите на социални медии;
- Насоки 9/2020 относно относимо и обосновано възражение съгласно Регламент (ЕС) 2016/679;

• Насоки 1/2020 относно обработването на лични данни при свързаните превозни средства и приложенията, свързани с мобилността.

Сред останалите окончателно приети от ЕКЗД документи са:

• Преглед на ресурсите, предоставени от държавите членки на органите за защита на данните, и на правоприлагащите действия от страна на органите за защита на данните;

• Изявление 5/2021 относно Акта за управление на данните във връзка с настъпилите развития в законодателството;

• Изявление 04/2021 относно международни споразумения, включително предаването на данни към трети държави;

• Документ на Европейския комитет по защита на данните в отговор на искането от Европейската комисия за разяснения относно съгласуваното прилагане на ОРЗД с акцент върху научните изследвания в областта на здравеопазването;

• Съвместно становище 03/2021 на ЕКЗД и ЕНОЗД по предложението за Регламент на Европейския парламент и на Съвета относно европейска рамка за управление на данните (Акт за управление на данните);

• Съвместно становище 5/2021 на ЕКЗД и ЕНОЗД относно предложението за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект);

• Изявление 03/2021 относно Регламента за поверителност на електронните комуникации.

Следва да се отбележи, че експерти на КЗЛД участват в екипите по подготовка на документите като съдокладчици по последните два документа.

2. Обмен на информация през Информационната система за вътрешния пазар – статистика и анализ.

Информационната система на вътрешния пазар (ИСВП) е сигурен, многоезичен онлайн инструмент за осъществяване на обмен на информация между публичните администрации в държавите от Европейското икономическо пространство (ЕИП) и европейските институции и органи, занимаващи се с практическото прилагане на законодателството на Европейския съюз, чрез което се осъществяват и комуникацията и сътрудничеството между надзорните органи на държавите – членки на ЕС.

В ИСВП се осъществява управление на случаи в съответствие с процедури от чл. 56 до чл. 70 от Регламента, които обхващат: определяне на водещия надзорен орган (ВНО) и засегнати надзорни органи (ЗНО) като част от сътрудничеството „на едно гише“,

искане за местен случай, искане за взаимопомощ или за доброволна взаимопомощ, съвместни операции на надзорни органи, за становище на ЕКЗД или разрешаване на спорове от ЕКЗД, процедура по спешност (издаване на становище или решение на ЕКЗД) или писмени процедури.

Към 31.12.2021 г. в регистъра на случаите, поддържан в ИСВП, има 1886 активни случая на трансгранично сътрудничество, като:

- 1379 бр. са инициирани в резултат на получени жалби;
- 507 бр., произтичащи от други източници като инициатива – напр. разследвания и инициативи на национален надзорен орган, правно задължение, информация разпространена от средствата за масово осведомяване и др.

В резултат на гореспоменатите случаи са започнати действия по:

- 602 процедури по сътрудничество (чл. 61) за отчетния период, докато общият им брой от началото на функциониране на системата през 2018 г. е 7112;
- 862 процедури, базирани на обслужване „на едно гише“ (чл. 60), от които по 309 случая има изготвено окончателно решение;
- 98 искания за разглеждане на случая като национален (местен) по чл. 56, пар. 2;
- 1 процедура относно съвместна операция;
- 115 процедури, свързани с изразяването на становище от страна на ЕКЗД;
- 2 процедури по разрешаване на спорове и две окончателни решения по тях;
- приети са 4 временни мерки по чл. 66;
- 1 окончателно решение по чл. 66;
- 1 решение съгласно процедурата по спешност по чл. 66.

В допълнение общият брой на започнатите процедури от 2018 г. за идентифициране на водещ и заинтересовани органи за защита на данните е 2629, от които 93 са текущи, а 2536 – приключени.

През 2021 г. КЗЛД е сезирана с общо седем предложения да бъде конституирана като ВНО. След извършен анализ на представената документация по случаите, в това число фактите и събраните от проверки доказателства, Комисията е взела решение по четири случая да не се конституира като ВНО поради липсата на място на установяване на посочените дружества на територията на България, а в останалите три случая проверките за наличие на териториална компетентност все още текат. Най-честата хипотеза за невъзможността на КЗЛД да се конституира като ВНО е посочването като АЛД на фиктивно дружество с български адрес, за което след извършване от Комисията на предварителна проверка се установява, че не съществува или не може да бъде установено.

През отчетния период КЗЛД, като се е припознала в качеството си на ВНО, открива процедура по чл. 56 във връзка със случай, касаещ нарушение на сигурността на данните по чл. 33 от ОРЗД, изразяващ се в неоторизиран достъп до *Customer Relationship Manager* (*CRM*) акаунт на дружество. Засегнати са лични данни на граждани от Естония, Финландия, Литва, Латвия, Италия, Франция, Белгия, Австрия, Испания. След извършването на цялостна преценка на фактите и обстоятелства по случая и спазването на утвърдената в ИСВП процедура (публикуване на проект на решение, по което конституиралите се като ЗНО могат да правят коментари и предложения), КЗЛД налага имуществена санкция и официално предупреждение на съответния администратор на лични данни.

КЗЛД се е конституирала като ЗНО по общо 16 случая, тъй като е възникнало обосновано предположение, че могат да бъдат засегнати правата на български граждани. Пет от тях са били инициирани от българския надзорен орган.

Някои от по-интересните случаи са следните:

1. Компания, предлагаща фармацевтични и продукти за орална хигиена, в това число и дермокозметика, депозира уведомление за нарушение на сигурността на данните при дружеството-майка, ситуирано във Франция. На глобално ниво корпорацията е станала жертва на кибератака, осъществена чрез *ransomware „sodinokibi“*, принадлежащ на групата *Revil*. Нарушението е възникнало в мрежата на дружеството в САЩ. Софтуерът е криптирал част от файловете в *IT* инфраструктурата на компанията, посредством използването на *phishing*. Получени са легитимен достъп и повишени права върху системата, което води до улесненото вкарване на вируса. След това антивирусната програма на съответния компютър бива деинсталирана и той е криптиран. Самият вирус е разпространен чрез домейн контролър, използващ *SCCM Microsoft,* като така е достигнато и до засегнатия в България потребител. Очаква се произнасянето на ВНО.

2. Български гражданин сезира КЗЛД с жалба срещу компания, ситуирана в Кипър, предлагаща хостинг услуги на клиенти в различни държави от ЕС. Лицето упражнява правото си по чл. 17 от Регламента („правото да бъдеш забравен“) съгласно утвърдената процедура. Според него има няколко нарушения на приложимото законодателство: отговорът на администратора е изпратен след законоустановения срок; не е ясно кой точно го е изпратил; не е получен конкретен отговор на зададените въпроси; конкретната информация не му била предоставена, защото е конфиденциална и ирелевантна към искането му, както и се твърди от АЛД, че искането е изпълнено, а всяко последващо такова ще се счита за повтарящо се и прекомерно съгласно разпоредбата на чл. 12, пар. 5 от ОРЗД.

Становището на кипърския надзорен орган е, че администраторът е изпълнил искането на лицето във времевите рамки, предвидени в чл. 12 от Регламента. В допълнение

субектът на данните е депозирал няколко последователни искания към АЛД, на които са били предоставени конкретни отговори. Надзорният орган смята, че администраторът не е длъжен да дава информация, която е извън обхвата на чл. 15 от ОРЗД, като например предприети от него технически и организационни мерки за защита.

3. Българският надзорен орган се конституира като ЗНО по случай, открит от естонския надзорен орган, по повод на нарушение на сигурността на данните от страна на *Admiral Markets AS,* чиято основната дейност е свързана с предлагането на обучения и инвестиционни услуги на клиенти. Те съобщават за обаждания от трети лица, които уж предлагали услуги и инвестиционни възможности и работели за големи инвестиционни компании. Администраторът провежда разследване, с което установява, че един от компонентите на *CRM* на дружеството е компрометиран и е получен достъп до данни на клиенти на дружеството, които са били предадени на трети лица. Дружеството установява, че е бил използван автоматичен скрипт, който прави заявки за данни в системата. Предприети са адекватни мерки за смекчаване на последиците от нарушението на сигурността.

Надзорният орган на Естония се произнася с проект на решение, с което налага мярка „официално предупреждение“ по чл. 58, пар. 2, б. „б“ от Регламента. Изразените съображения са, че личните данни следва да се обработват по начин, осигуряващ подходяща сигурност на обработването, в това число защита от неоторизирано или незаконосъобразно обработване, като се имплементират подходящите технически и организационни мерки. От особена важност е администраторът да гарантира редовно сигурността на информационните системи (в това число техния постоянен мониторинг и ъпдейт). Прието е и окончателно решение със същия диспозитив, тъй като няма обосновани възражения от другите ЗНО.

През 2021 г. КЗЛД отговаря на 32 запитвания, постъпили от други органи за защита на данните, следвайки заложената процедура в ИСВП по чл. 61 от ОРЗД. Някои от поставените по-интересни въпроси са свързани с обработването на лични данни при управление на безпилотни самолети; нерегламентираният достъп до централизирани информационни системи, съдържащи лични данни; видеонаблюдението, извършвано от физическите лица чрез шпионката на външната врата; прилагането на правата на физическите лица и принципите за обработване на данните съгласно ОРЗД; операциите по обработване на лични данни за целите на националната сигурност; тълкуването на правото на физическото лице да подава жалба до надзорния орган за защита на данните при трансгранични случаи; ограничаването на достъпа на пациенти до техните здравни данни; извършването на видеонаблюдение на работното място с цел оценка на изпълнението на

задълженията; тълкуването на изключението, свързано с обработването на данни за лични или семейни нужди по отношение на онлайн съдържание; въвеждането на система, която да осъществява връзки между превозни средства с цел постигане на по-голяма пътна безопасност; разпореждането за предоставяне на информация по съдебно дело; обработването на лични данни на участниците в спортни събития; публикуването на съобщения, съдържащи лични данни в онлайн форуми; използването на биометрични данни за целите на идентификацията и тяхното съхраняване; обработването на информацията относно резултатите от тестването за *КОВИД-19* на служителите от техните работодатели и използването на система за автоматично разпознаване на регистрационни номера.

По отношение на писмените процедури за гласуване, проведени през 2021 г., следва да се отбележи, че КЗЛД гласува по 60 документа на ЕКЗД, като основната част от тях са свързани със задълженията на Комитета по:

- чл. 64, пар. 1, б. „б“ от ОРЗД – оценка на съответствието на проект на кодекс на поведение, негово изменение или допълнение с регламента;
- чл. 64, пар. 1, б. „в“ от ОРЗД – одобряване на изискванията за акредитиране на орган за наблюдение на кодекс за поведение съгласно чл. 41, пар. 3, респ. за акредитиране на сертифициращ орган съгласно чл. 43, пар. 3 от Регламента или на критериите за сертифициране, посочени в чл. 42, пар. 5 от ОРЗД;
- чл. 64, пар. 1, б „е“ – одобряване на задължителни фирмени правила по смисъла на чл. 47 от ОРЗД.

С оглед насърчаване обществената информираност, макар че липсва изрично задължение за превод на документи, свързани с механизма за сътрудничество и съгласуваност, традиционно КЗЛД подпомага ЕКЗД и в това отношение. В резултат на тази дейност българските граждани имат възможност своевременно да се запознаят с текста на съответния документ на български език, което спомага за тяхното по-добро информиране и възможности за вникване в приетите документи на ЕКЗД, които са от значение за всички заинтересовани лица в сферата на защитата на личните данни и неприкосновеността на личния живот.

За отчетния период са извършени 71 редакции на документи на ЕКЗД, като основната част от тях са представлявали насоки, становища, изявления и работни документи, които са част от основните инструменти на Комитета, свързани с неговите задачи съгласно чл. 70 от ОРЗД.

VII. МЕЖДУНАРОДНА ДЕЙНОСТ

През целия отчетен период приоритет остава участието във всички международни формати, обединяващи сродни органи по защита на данните, които са провеждали онлайн заседания или в рамките на които е обменена интензивна кореспонденция по актуални теми от сферата на защитата на личните данни. Прилагането на организационни мерки за преодоляване на съвременните предизвикателства, свързани с разпространението на *КОВИД-19,* е сред основните фактори за преизпълнението на количествените резултати на този показател. Обстоятелството, че всички заседания по международна линия са провеждани дистанционно, създава условия за активно участие в реално време в по-голям брой международни мероприятия от очаквания в 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, участия в заседания, подготвени позиции и подготвени отговори на чуждестранни запитвания – общо 538 бр.

1. Участие в механизма за координиран надзор на информационните системи на ЕС.

През отчетния период КЗЛД продължава да изпълнява в пълен обем дейностите по осигуряване пълноправното присъединяване на Република България към Шенген. Освен осъществяване инспекциите на националните звена на информационните системи на ЕС, както е посочено и в Раздел IV „Контролна дейност“, през 2021 г. КЗЛД реализира проверки на системите Европол, ШИС II, ВИС и ЕВРОДАК, представители на Комисията продължават своето активно участие в работата на съвместните надзорни органи и координационни групи по надзор на широкомащабните информационни системи на ЕС: Комитета за сътрудничество на Европол и Координационните надзорни групи на Шенгенската информационна система от второ поколение (ШИС II), Визовата информационна система (ВИС), ЕВРОДАК и Митническата информационна система. През 2021 г. са проведени общо 9 заседания на отделните формати. Резултатите от описаните в Раздел IV „Контролна дейност“ проверки са докладвани на заседанията на съвместните органи за надзор на съответните системи.

Сред общите теми на всички заседания е предстоящата промяна в осъществяването на координиран надзор и преминаването му към Комитета за координиран надзор в ЕКЗД. Акценти в работата на всички формати са докладването на одитните дейности на Европейския надзорен орган по защита на данните (ЕНОЗД) и дейностите по обработване на данни в различните системи от страна на Европейската агенция за оперативното

управление на широкомащабни информационни системи в пространството на свобода, сигурност и правосъдие през 2021 г., както и подготовката на предложение за съвместно писмо – становище от името на координационните групи за надзор на ШИС II и ВИС във връзка с Предложението за Регламент на Съвета относно създаването и функционирането на механизъм за оценка и наблюдение с цел проверка на прилагането на достиженията на правото от Шенген и за отмяна на Регламент (ЕС) №1053/2013.

По отношение на дейността на Съвместния надзорен орган на Европол КЗЛД участва във всички инициативи на съвместния орган: проект на становище относно предложението за изменение на Регламента за Европол, както и съдържанието на Работната програма на Съвета за периода 2021 – 2023 г.

Сред основните теми в дейността на Координационната надзорна група на ВИС, разглеждани през отчетния период, са предложението за общ план за инспекции, двугодишният отчет на Групата за периода 2019 – 2020 г., завършване подготовката и одобряване съдържанието на въпросника относно предварителното изтриване на данни от ВИС. КЗЛД обобщава и изпраща информация по отношение на националното развитие в двугодишния период до 2020 г. и във връзка с отговорите от въпросника по темата в рамките на 2021 г.

Акценти в дейността на Координационната надзорна група на ЕВРОДАК продължават да са подготовката на единен документ относно структурирано докладване на националните одити на системата ЕВРОДАК, както и подготовката на становище относно Новия пакт за миграцията и убежището на ЕС, които са част от подготвяната работна програма на Групата. За пръв път е представен окончателният вариант за брошурата относно правото на информация на субектите на данни, достъпна на всички национални езици на държавите – членки на ЕС. Същата е пряк резултат от сътрудничеството на Групата с Агенцията на Европейския съюз за основните права.

През отчетния период Координационната група за надзор на ШИС II започва подготовката на становище относно законодателното предложение на ЕК и продължава обсъжданията по отношение на организацията на мисиите по оценка на Шенген с оглед постигането на устойчивост на участието и ангажираността на националните експерти в процеса по проверка и оценка. Продължават дискусиите по отношение на възможните модели за събиране на статистически данни за заявките за достъп и резултатите от тях, както и по разработването на информационни материали относно изменената правна рамка за ШИС.

По отношение на Координационната група по надзор на МИС в рамките на настоящата година е завършена подготовката и са одобрени 2 основни документа:

въпросник относно обучението за защита на данните на служителите от институциите с достъп до МИС, както и Отчетът за дейността на Координационната група за надзор на МИС за периода 2018 – 2019 г. КЗЛД представя в рамките на предварително определения срок отговорите на въпросите по отношение на състоянието на системата и обучението на служителите в Република България.

През отчетния период продължава утвърждаването на Комитета за координиран надзор (ККН) към ЕКЗД, чиято основна цел е да осигури координиран надзор над широкомащабните информационни системи, функциониращи на територията на ЕС, които се използват от органи, служби и агенции на ЕС в съответствие с член 62 от Регламента (ЕС) 2018/1725 или с друг правен акт на ЕС за създаване на конкретната система.

Комитетът за координиран надзор е създаден в рамките на ЕКЗД и се състои от представители на националните органи за защита на данните на всяка държава – членка на ЕС и ЕНОЗД. Участници могат да бъдат и националните органи за защита на данните на държави извън ЕС, които попадат в Шенгенското пространство.

В дейностите на ККН, които засягат конкретна широкомащабна система или институция на ЕС, могат да участват представителите на националните органи за защита на данните, в случай че съответната им държава прилага правния акт на ЕС за създаване на широкомащабната система или европейска институция. Комитетът функционира автономно и приема свой процедурен правилник, методи на работа и двугодишна работна програма. На всеки две години ККН изготвя доклад от дейността си, който се предлага на ЕКЗД за представяне на Европейския парламент, Съвета, Комисията и други адресати, когато това е изрично изискано в правния акт на ЕС за създаване на широкомащабната система или органа, подлежащи на координиран надзор.

Към настоящия момент ККН осъществява координация и надзор в рамките на обработването на лични данни в Информационната система за вътрешен пазар на ЕС, системата за съдебно сътрудничество по наказателноправни въпроси ЕВРОЮСТ, както и обработването на лични данни при осъществяваните на действия от страна на Европейската прокуратура. Обработването на лични данни в следните широкомащабни системи и агенции на ЕС също ще попадне в обхвата на координиращите дейности на ККН, след като правният акт на ЕС, в който това е предвидено, започне да се прилага:

- Шенгенската информационна система от второ поколение;
- Агенция на Европейския съюз за сътрудничество в областта на правоприлагането (Европол);
- Система за влизане/излизане (СВИ);
- Европейската система за информация и разрешение за пътуване (*ETIAS*);

• Европейската информационна система за съдимост за лица, граждани на трети страни (*ECRIS-TCN*);

• Визова информационна система;

• Европейска база данни за дактилоскопия в областта на убежището;

• Митническа информационна система.

България е сред държавите, в които има повече от един надзорен орган по защита на данните (КЛЗД, която осъществява общ надзор, и ИВСС, който осъществява специализиран надзор по см. на чл. 17 от ЗЗЛД), поради което участието в работата на ККН става посредством т.нар. „съвместно представителство“ с право на един глас.

През отчетния период са проведени две онлайн заседания на ККН. Предмет на обсъжданията на заседанието през май 2021 г., които имат отношение към дейността на КЗЛД, са въпроси, свързани с:

1. Информационната система на вътрешния пазар: публикуване на списък с контакти на компетентните в национален план надзорни органи, проучване в национален план на практическото приложение на нормативните изисквания за функциониране на Информационната система на вътрешния пазар от гледна точка на защитата на личните данни: общ преглед; права на субектите на данни; достъп до системата от страна на надзорния орган по защита на данните;

2. Организацията на работа на ККН: поддържане на интернет страница, разкриване/публикуване на документи за нуждите на обществеността, разглеждане на искания за достъп до документи и подготовка за предстоящото включване в предмета на координирания надзор на допълнителни широкомащабни информационни системи.

Акцент на заседанието на ККН през декември е поставен върху обобщената справка и анализ от извършеното преди това национално проучване, свързано с ИСВП, и концептуален анализ с предложения за бъдещото функциониране на ККН с оглед предстоящото разширяване на неговия надзор над ШИС и Европол и свързаното с това правоприемство на надзорната дейност на Координационната група за надзор на ШИС II и Съвместния надзорен орган на Европол.

2. Участия в Комитета по чл. 93 от Регламент (ЕС) 2016/679.

Европейската комисия се подпомага от комитет. Този комитет е структура по смисъла на Регламент (ЕС) №182/2011 относно за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Европейската комисия. През годината са проведени 8 дистанционни заседания. Сред основните теми са:

• предложението за решение за изпълнение на Европейската комисия относно адекватното ниво на защита на личните данни по Регламент (ЕС) 2016/679 от Южна Корея;

• двете предложения за решения за изпълнение на Европейската комисия относно стандартни договорни клаузи между администратори и обработващи данни, намиращи се в ЕС (съгласно член 28 от ОРЗД), и относно стандартни договорни клаузи за трансфер на лични данни към трети държави (съгласно член 46 от ОРЗД);

• предложения за решенията за изпълнение относно адекватното ниво на защита на личните данни от Обединеното кралство по Регламент (ЕС) 2016/679 и относно адекватното ниво на защита на личните данни от Обединеното кралство по Директива (ЕС) 2016/680.

3. Участия в заседанията на Експертната подгрупа по Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 към Европейската комисия.

Експертната подгрупа по Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 към Европейската комисия е постоянна работна група, която се председателства от представител на ЕК и чиято задача е осигуряването на експертиза в областта на защитата на личните данни, доколкото този процес ще подпомогне ЕК във вземането/предлагането на решения, основани на общото мнение на общността на специалистите с експертни познания в защитата на данните от националните надзорни органи. През годината са осъществени 2 дистанционни заседания. Сред обсъжданите теми през отчетния период са:

• Дискусия за разграничаване на обхвата на Директива (ЕС) 2016/680 и ОРЗД;

• Дискусия относно правото на ефективни съдебни средства за защита срещу надзорен орган (член 53 от Директива (ЕС) 2016/680);

• Дискусия за съвместяването на правото на защита на данните с правото на свобода на изразяване (член 85 от ОРЗД);

• Дискусия относно правото на ефективна съдебна защита срещу надзорен орган (член 78 от ОРЗД);

• Транспониране на Директива (ЕС) 2016/680 в частта ѝ за правото на ефективно вътрешноправно средство за защита (чл. 53 от Директивата);

• Транспониране на Директива (ЕС) 2016/680 и прилагане на Регламент (ЕС) 2016/679 в частта им относно надзора над съдилищата, действащи в качеството си на органи на съдебната власт (чл. 45 от Директивата, чл. 55 и Раздел 8 от Регламента).

Акцентът в обсъжданията през отчетния период са Директива 2016/680 и нейното взаимодействие и прилагане паралелно с Регламент 2016/679, както и наличните ефективни правни средства за защита по силата на правната рамка по транспонирането ѝ. По

отношение на Регламент 2016/679 дискусията е посветена на обработването на лични данни с цел упражняване свобода на изразяване и наличните ефективни правни средства за защита при прилагане на същия регламент.

С оглед разнородните подходи в различните правни системи на държавите членки и с цел ефективен обмен на опит между тях ЕК предлага да разпространи конкретен въпросник по обсъжданите теми, който е попълнен и предоставен от страна на КЗЛД в срок. Теми за бъдеща дискусия са обсъждания във връзка с трансферите към трети държави по чл. 39 от Директива (ЕС) 2016/680, както и общата тема за „застрашената независимост“ на надзорните органи при разширяване на компетенциите с Регламента и Директивата.

4. Участия в заседанията на Работна група „Защита на данните“ към Съвета на ЕС.

Работната група „Защита на данните“ към Съвета на ЕС се занимава с въпроси, свързани с прилагането на законодателството и политиките за обмен на информация и защита на лични данни в областта на правоприлагането. Освен това тя си сътрудничи с Европол, особено по отношение на стратегията за управление на информацията (*IMS*) за рационализиране на трансграничния обмен на информация. Групата разглежда законодателните предложения на Европейската комисия в нейната област на експертиза, които се изпращат към Съвета на министрите. Работната група се състои от експерти от всяка държава – членка на ЕС, и се председателства от делегата на държавата, която изпълнява ротационното шестмесечно председателство на Съвета на ЕС. След разглеждане предложенията се предават на Съвета по правосъдие и вътрешни работи (ПВР).

През отчетния период са осъществени 6 заседания, като сред обсъжданите теми са:

- Предложение на Съвета за приемане на правила за изпълнение относно длъжностното лице по защита на данните, приложението на Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета, ограничения в правата на субектите на данни в контекста на изпълнението на задачите на длъжностното лице по защита на данните и за отмяна на Решение на Съвета 2004/644/ЕК;
- Обсъждане на предложението за Позиция на Съвета на ЕС по прегледа на прилагането на Директива (ЕС) 2016/680;
- Решения за изпълнение на ЕК относно адекватното ниво на защита на данните;
- Съвместен преглед на Споразумението САЩ – ЕС – *Umbrella Agreement EU – US*;

• Преговори по Втори допълнителен протокол на Конвенцията на Съвета на Европа от Будапеща;

• Проект на решения за изпълнение на Комисията относно стандартни договорни клаузи между администратори и обработващи данни, намиращи се в ЕС (съгласно член 28 от ОРЗД), и относно стандартни договорни клаузи за трансфер на лични данни към трети държави (съгласно член 46 от ОРЗД);

• Актуална информация относно международните трансфери на данни – представяне от службите на Европейската комисия;

• Представяне на приоритетите на френското председателство на Съвета на ЕС;

• Процес на подписване на модернизираната Конвенция 108 на Съвета на Европа.

5. Участие в заседанията на Изпълнителното бюро на Конвенция 108 към Съвета на Европа.

С Конвенция №108 на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни се създава Консултативен комитет на Конвенцията за защита на лицата по отношение на автоматизираната обработка на лични данни. Той се състои от представители на страните по Конвенцията и наблюдатели от други държави, международни организации и неправителствени организации. Консултативният комитет отговаря за тълкуването на разпоредбите на Конвенцията и осигурява улесняване и подобряване на нейното прилагане. Също така изготвя доклади, насоки и ръководни принципи по актуални теми, свързани с приложното поле на Конвенция 108. В рамките на отчетния период Комитетът заседава на пленарна сесия два пъти, а Изпълнителното бюрото към Консултативния комитет – три пъти. Към края на ноември 2021 г. 43 страни са подписали Изменения протокол и 15 страни са ратифицирали Протокола (*CETS №223*) за изменение на Конвенцията за защита на лицата при автоматизирана обработка на лични данни.

През отчетния период са финализирани Вторият допълнителен протокол към Конвенцията от Будапеща за престъпления в кибернетичното пространство, за засилено сътрудничество и разкриване на електронни доказателства, Механизмът за оценка и последващи действия съгласно Конвенция 108+, както и Насоките за обработване на лични данни за целите на политическите кампании. Следва да се отбележи, че българските предложения за изменение и допълнение на последните са приети в цялост и са отразени в окончателния текст на документа. Сред приетите документи е и предложението за Работна програма на Комитета за периода 2022 – 2025 г.

На 17 ноември 2021 г. Комитетът на министрите към Съвета на Европа официално приема текста на Втория допълнителен протокол към Конвенцията от Будапеща за престъпления в кибернетичното пространство, за засилено сътрудничество и разкриване на електронни доказателства. Към настоящия момент по инициатива на Европейската комисия текат процедури №2021/0382/NLE и №2021/0383/NLE, съответно за Предложение за Решение на Съвета на ЕС за упълномощаване на държавите членки да подпишат в интерес на Европейския съюз Втория допълнителен протокол към Конвенцията и Предложение за Решение на Съвета на ЕС за упълномощаване на държавите членки да ратифицират в интерес на Европейския съюз Втория допълнителен протокол към Конвенцията.

Този протокол е резултат от дългогодишни усилени и сложни преговори, но във финалната си версия наред с всичко останало представлява и надежден инструмент за трансфер на лични данни към трети държави, ратифицирали Конвенцията, чрез споразумения, които предоставят подходящи гаранции за защитата на личните данни в сферата на предотвратяването, разкриването и наказателното преследване на престъпления (изискване по смисъла на чл. 37 от Директива (ЕС) 2016/680).

6. Участие в международни форуми по защита на данните.

На 28 януари 2021 г. експерти от КЗЛД участват в две международни мероприятия по случай Деня за защита на личните данни – 28 януари: конференция на германските органи за защита на данните на федерално и местно ниво, посветена на 40-ата годишнина от приемането на Конвенция 108/81/СЕ, с наименование „Предизвикателства при международния трансфер на данни от гледна точка на Конвенцията 108+ и ОРЗД“ и дигитална международна конференция на Хърватския надзорен орган под надслов „Цифрова трансформация и защита на данните в свят на пандемия“.

Германските колеги представят теми, свързани с различните аспекти от прилагането на Конвенция 108+: международните трансфери на данни от гледна точка на надзорните органи, най-вече във връзка с решението на Съда на ЕС по делото *Schrems II*; практиката на Европейския съд по правата на човека и на Съда на Европейския съюз (включително взаимодействието между чл. 8 и чл. 10 от Хартата за основните права на ЕС); както и предимствата на Конвенцията, като международно правно обвързващ документ в сферата на защита на данните.

Участниците в хърватската дигитална конференция разглеждат основни въпроси, свързани със защитата на данните и бързо развиващата се дигитална среда. Други теми на форума са способността на МСП да посрещнат новите предизвикателства, сериозните последици от пандемията върху сектор „Туризъм“, развитието на Конвенция 108 и

приложението ѝ по време на глобална пандемия, както и прилагането на нейните правила от държавите – членки на ЕС. Икономическото отражение на кризата и бързо развиващата се дигитална среда върху бизнеса и защитата на данните, ползите от данните отвъд бизнес средата (включително като основа за доверието на субектите към администраторите на лични данни), значението на оценка на въздействието върху защитата на личните данни, стандартните договорни клаузи и решението на Съда на Европейския съюз – *Schrems II*, също са сред темите на международната конференция.

В периода 18 – 22 октомври 2021 г. се провежда 43-тото издание на Глобалната асамблея по въпросите на неприкосновеността. Следвайки правилата на Асамблеята, програмата е разделена на открита и закрита сесия. По време на закритата сесия са приети Резолюция за стратегическото развитие на Асамблеята за периода 2021 – 2023 г., Резолюция относно споделянето на данни за обществени цели, Резолюция за цифровите права на децата, Резолюция относно правителствения достъп до данни, както и Резолюция за бъдещето развитие на Асамблеята и нейния Секретариат.

Предвид неприсъственото осъществяване на събитието е организирано предварително гласуване за приемане на отчетните документи на 11-те работни групи към Глобалната асамблея по въпросите на неприкосновеността, чието съдържание е подкрепено от КЗЛД. За член на Изпълнителния комитет на организацията е избран представител на Мароканската национална комисия за контрол и защита на личните данни. За председател на Изпълнителния комитет на Асамблеята е избран ръководителят на Мексиканския национален институт по прозрачност, достъп до информация и защита на личните данни. С приетата Резолюция за бъдещето развитие на Асамблеята и нейния Секретариат се продължава процесът по въвеждане на такса за членовете на организацията, като точният размер на таксата ще бъде определен на по-късен етап и в съответствие с приетия график (Пътна карта за осигуряване финансирането на Секретариата на Асамблеята (2022 – 2026)).

На 16 ноември 2021 г. представител на КЗЛД участва в международната конференция под надслов „Лични данни – бъдеща перспектива“ по повод 20-ата годишнина от създаването на Латвийския орган за защита на данните. Сред темите на конференцията са обработването на личните данни от „умни“ устройства, лицево разпознаване и идентификацията за финансови цели, новите технологии за обработване на лични данни в трети държави, необходимостта и пропорционалността като основни принципи, които следва да се съблюдават с оглед гарантиране на защитата на личните данни на лицата във връзка с прилагането на Директивата за борбата срещу изпирането на пари. Участниците обсъждат въпроси, свързани с незаконно получените финансови средства, подходи, основани на оценката на риска, както и предаването на лични данни към трети държави.

В периода 16 – 17 ноември 2021 г. представители на КЗЛД участват в годишното издание на *European case handling workshop* (*ECHW*), посветено на споделянето на национален опит при разглеждането на жалби, осъществяването на надзорна дейност и разследвания, както и при предоставянето на насоки към администраторите по прилагането на законодателството в сферата на защита на личните данни. По време на двудневната програма предмет на обсъждане са стратегиите и моделите, изградени от надзорните органи по защита на личните данни на Италия, Исландия, Гибралтар, Германия, Обединеното кралство, Нидерландия, Ирландия и остров Ман.

Като основни причини за нарушенията на сигурността на личните данни са определени изгубено устройство, непреднамерено публикуване на информация, неоторизираният достъп, както и пробивите на сигурността на предлаганите от администратора или обработващия лични данни услуги. Обсъдени са конкретни срокове за изпълнение на стъпките по разследване на жалби, като основната цел е не налагането на глоби/имуществени санкции, а корекция в процесите по обработване на администраторите. Като ефективен модел е представен така наречения *batching* метод за скъсяване времето, необходимо за разглеждане на броя жалби и уеднаквяване решенията, взети от надзорния орган.

В края на отчетния период на 16 и 17 декември 2021 г. представители на КЗЛД участват в Конференцията на органите за защита на данните в Централна и Източна Европа. Основните акценти в осъществените промени и постижения на надзорните органи за защита на данните на Централна и Източна Европа са свързани с промяна на структурите на надзорните органи с цел да бъдат обхванати задълженията им, произтичащи от Регламент (ЕС) 2016/679, както и подходите за преодоляване предизвикателства, свързани с обработването на данни в условията на *КОВИД-19*. Първият дискусионен панел в програмата „Механизми за отчетност“ е модериран от служител на КЗЛД. Представителите на надзорните органи за защита на данните на Литва, Република България и Полша представят теми, свързани със сътрудничеството между надзорните органи и длъжностните лица по защита на данните; приложението на кодексите за поведение, както и принципа на отчетността като законодателен механизъм за защита на правата на субектите на данни.

През отчетната 2021 г. се наблюдава постоянно дистанционно участие на представители на КЗЛД в работата на Експертната група за по-безопасен интернет за деца (*Safer Internet for Children Expert Group*) към Генерална дирекция „Съобщителни мрежи, технологии и съдържание“ на Европейската комисия. Групата подпомага обмена на най-добри практики по отношение на прилагането на конкретни разпоредби, свързани с децата, в съществуващи правни актове, включващи мерки за защита на непълнолетните от вредно

съдържание в Директивата за аудио-визуалните и медийни услуги и правила за изискване на родителско съгласие за достъп до данните на децата, обхванати от ОРЗД от държавите – членки на ЕС, Исландия и Норвегия.

Работата по актуализирането на Европейската стратегия за по-добър интернет за децата (стратегия *BIK*) започва през 2021 г., като за подготовката на прегледа на Стратегията са проведени поредица от консултации под надслов *#DigitalDecade4YOUTh* в целия ЕС. В съответствие с принципите, планирани в рамките на Цифровото десетилетие, новата стратегия *BIK* продължава да защитава децата онлайн, като ги подпомага да се възползват от предимствата, предлагани от цифровите технологии, и същевременно ги защитава от онлайн заплахи. Това се осъществява чрез прилагането на съществуващата правна рамка като Директивата за аудио-визуалните медийни услуги (*AVMSD*), Общия регламент за защита на данните (*GDPR*) и предложената законодателна инициатива за цифровите услуги (*DSA*).

През 2021 г. в продължение на изпълнение на поставените цели Експертната подгрупа за обмен на най-добри практики обръща внимание на няколко нормативни документа, касаещи децата и възможностите, които се откриват за регулиране и предоставяне на децата на по-безопасна онлайн среда, а именно: Предложението за Регламент за определяне на хармонизирани правила относно изкуствения интелект (Акт за изкуствения интелект) и Предложението за Регламент относно единния пазар на цифрови услуги (Законодателен акт за цифровите услуги) и за изменение на Директива 2000/31/ЕО и Стратегията на ЕС за правата на детето. Основната цел на Стратегията е да бъдат предоставени условия за възможно най-добър живот на децата в ЕС и по целия свят, като предлага конкретни мерки за защита, насърчаване и изпълнение на правата на децата в днешния постоянно променящ се свят.

През изтеклата година КЗЛД взема участие и в дейността на Международната работна група по защита на личните данни в телекомуникациите (позната още като Берлинска група), основана през 1983 г. в рамките на Международната конференция на защита на личните данни и неприкосновеността на личния живот по инициатива на Берлинския комисар по защита на данните, който председателства Групата до началото на 2021 г. Основната задача на групата е да информира гражданите за тяхната защита на данните и правата за свобода на информацията и да ги подкрепя в тяхното отстояване. Групата включва представители от органите за защита на данните и международни организации от целия свят, занимаващи се с въпросите на неприкосновеността на личния живот. Тя приема становища и препоръки – включително в контекста на законодателни процедури, както и изготвя експертни становища и доклади. Част от нейната дейност е и

участието в национални, европейски и международни органи, конференции и работни групи.

На проведеното през март 2021 г. заседание е представен националният опит на КЗЛД в периода от предходното заседание в края на 2019 г. Българският представител запознава участниците с дейностите на КЗЛД, свързани с прилагането на ефективни надзорни механизми, извънредно нарасналия брой на уведомления за нарушенията на сигурността и главните причини за тях, както и дейностите на КЗЛД по прилагане на мерки за повишаване на осведомеността и предоставяне на разяснения за съвременната законодателна рамка за защитата на личните данни.

Участниците споделят информация за дейности на национално ниво по отношение на преодоляването на последствията от разпространението на *КОВИД-19*. Сред обсъдените теми са сензорните мрежи (*sensor networks*), гласово контролираните устройства (*voice-controlled devices*), „умните градове“, лицевото разпознаване, блокчейн технологията, както и квантовата изчислителна техника и сигурност.

7. Дейност на председателя на КЗЛД в качеството му на заместник-председател на ЕКЗД.

Отчетният период е един от най-успешните периоди за утвърждаване ролята на ЕКЗД и повишаване на разпознаваемостта на последователните му усилия за единното прилагане на правилата относно защитата на данните навсякъде в Европейския съюз и за насърчаване сътрудничеството между органите за защита на данните на държавите членки. В качеството си на заместник-председател на ЕКЗД, през 2021 г. председателят на КЗЛД взема участие в редица събития.

На 23 юни 2021 г. Венцислав Караджов участва в дискусия на тема „Следващите стъпки за споделяне на данни и приоритети за прилагане на нови практики – неприкосновеност, правоприлагане и споделяне на данни в международен план“ (*The next steps for data sharing, and priorities for implementing the new code of practice – privacy, enforcement, and sharing data internationally*), част от поредното издание на *Westminster eForum policy conference, Next steps for UK data protection*.

На 14 юли 2021 г. членовете на ЕП провеждат дискусия, посветена на приложенията за социалните мрежи, позволяващи създаването на кратки забавни и танцови видеозаписи. По време на обсъжданията в Комисията по граждански свободи, правосъдие и вътрешни работи (*LIBE*) на Европейския парламент Европейският комитет е представен от председателя на КЗЛД. Заедно със заместник-началника на отдел „Защита на данните“, Генерална дирекция „Правосъдие и потребители“ на ЕК, председателят на Комисията

защитава експертна позиция относно приложението на разпоредбите на законодателството за защита на неприкосновеността на личния живот и личните данни на европейските граждани на територията на ЕС.

На 10 септември 2021 г. по време на 19-ата конференция по киберсигурност *INFOSEK* (*19th cyber security conference INFOSEK*) в гр. Нова горица, Словения, председателят на КЗЛД представя теми, свързани с дейността на ЕКЗД и последователното прилагане на правилата за защита на данните в ЕИП, пред експерти по информационна сигурност, управление на непрекъснатостта на бизнеса, цифровата криминалистика, нормативно съответствие, сигурността на компютърната система и приложенията, както и облачните системи. Специален акцент е поставен върху това как стратегията и работната програма на ЕКЗД подпомагат създаването на последователно разбиране на ключовите концепции и процеси в ОРЗД и механизма за сътрудничество и съгласуваност.

Дванадесет дни по-късно, на 22 септември 2021 г., по време на 6-ия Международен конгрес по информационно право (*6th International Information Law Congress*) в гр. Измир, Турция, председателят на КЗЛД представя теми, свързани със защитата на личните данни в контекста на изкуствения интелект и блоковата технология (блокчейн).

На 12 октомври 2021 г. се провежда *RAID 2021: Panel Briefing*, гр. Париж, Франция, която събира на едно място представители на държавния сектор, бизнеса и академичните среди от ЕС, Китай и САЩ, търсещи подходящите отговори на глобалните предизвикателства, свързани с развитието на технологиите, изкуствения интелект, интернет и обработването на данни. Акцент в представянето на председателя на КЗЛД е Съвместното становище 5/2021 на ЕКЗД и ЕНОЗД относно предложението за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект).

В края на отчетния период ЕКЗД е представен от Венцислав Караджов в последния за годината международен форум за защита на личните данни, организиран от *Thomson Reuters* на 9 декември 2021 г. в Испания, на който председателят на КЗЛД запознава участниците със стратегическите цели и задачи на ЕКЗД.

VIII. ПОДПОМАГАНЕ ИЗПЪЛНЕНИЕТО НА ЦЕЛИТЕ НА КЗЛД ЧРЕЗ РЕАЛИЗАЦИЯ НА ПРОЕКТИ С НАЦИОНАЛНО И МЕЖДУНАРОДНО ФИНАНСИРАНЕ

1. „Осигуряване на най-висока степен на защита на неприкосновеността на личния живот и личните данни чрез иновативни инструменти за малки и средни предприятия и граждани – *SMEDATA*“.

Изпълнението на инициирания в края на 2017 г. в партньорство със Съюза на юристите в Република България, „Апис Европа“, *EY* – България, Италианския орган по защита на данните, университета *Roma Tre* и Европейската асоциация на жените юристи – клон България, проект завърши успешно в рамките на предварително планирания срок – 30 ноември 2020 г.

Следвайки развитието на епидемиологичната обстановка, инструментът за самооценка на малки и средни предприятия е представен на 28 януари 2021 г., Деня за защита на личните данни, с оглед постигането на максимална публичност и интерес от обществото. Това е интернет базиран софтуер, който дава възможност на представители на малките и средните предприятия да оценят своята готовност, както и съответствието на процесите си по обработване на лични данни с разпоредбите на ОРЗД. Същият е разделен на две основи части (стълба): самооценка и разяснения. Всеки от тях се състои от три еднакви раздела: въведение, основен раздел и допълнителни материали за четене.

Разделът „Самооценка“ съдържа набор от последователни, логически свързани въпроси, за да се демонстрира взаимосвързаността между обикновените бизнес операции и обработването на лични данни. Освен това структурата на въпросите представя важността на защитата на личните данни не само с оглед спазването на правилата на ОРЗД, но и предвид възможни загуби за администраторите/обработващите, свързани с търговската репутация, взаимоотношенията с клиенти, както и паричния поток. Разделът „Разяснения“ съдържа 16 теми, представящи основните задължения на администраторите на лични данни, правата на физическите лица и специфични случаи на обработване на лични данни в контекста на обичайната дейност на МСП заедно с методология за обучение и допълнителни материали за четене.

Инструментът за самооценка и разяснения предоставя критерии за качество на мерките за повишаване на осведомеността, позволяващи на малките и средните предприятия (МСП) да демонстрират разумна увереност чрез последващ избор на допълнителни подходи за повишаване на осведомеността сред техния персонал или клиенти – граждани, както и на вътрешни механизми за тяхното прилагане. Същият е

достъпен както от интернет страницата на проекта, така и от институционалната интернет страница на КЗЛД.

2. „Осигуряване на най-висока степен на защита на неприкосновеността на личния живот и личните данни чрез иновативни инструменти за малки и средни предприятия и граждани – *SMEDATA II*“.

Проектът *SMEDATA II* цели осигуряването на ефективното прилагане на ОРЗД чрез информираност, мултиплициращо обучение и изграждане на устойчив капацитет в малките и средните предприятия. Сред планираните дейности са организирането на серия от събития за повишаване на осведомеността и обучение в България и Италия, надграждане на мобилното приложение „*GDPR* в твоя джоб“. Всички проектни дейности са разработени, за да разпространяват не само информация за целите и резултатите от проекта, но също така и новости в областта на защитата на личните данни от значение за МСП и гражданите.

През отчетния период са завършени над 1/3 от планираните дейности по проекта, както и над 1/3 от тях са в процес на изпълнение. Сред основните дейности през отчетния период е надграждането на получилото ежегодната награда на БАИТ в началото на 2020 г. мобилно приложение „*GDPR* в твоя джоб“, предоставящо разяснения и насоки по прилагане на правната рамка по защита на личните данни за малките и средните предприятия и гражданите. Съдържанието му вече е достъпно на 5 езика – български, английски, италиански, френски и немски, като потребителите имат непосредствен достъп до законодателството и съдебната практика в областта на защитата на личните данни в България, Италия, Франция и на федерално ниво в Германия. През отчетния период приложението е допълнено с информация за националното законодателство на Франция и Германия, както и езикови версии на немски и френски език. До настоящия момент мобилното приложение е инсталирано на над 5900 устройства. Допълнително удобство създава и неговата разработена версия за настолни компютри.

Сред останалите осъществени дейности по проекта през отчетния период са подготовката на осъвременено обучително съдържание за представители на МСП, както и техническо обновяване на интернет страницата на проекта – *smedata.eu*, което дава възможност на физически лица с намалено зрение да достъпват информацията на сайта.

Комисията за защита на личните данни е водещ партньор – координатор на проектните дейности. В проектния консорциум участват Съюзът на юристите в България, „Апис Европа“, адвокатското дружество *EY* – България, университетът *Roma Tre* и Европейската асоциация на жените юристи – клон България. Общият бюджет за всички

партньори по проекта е 423 055,38 лв. (216 304,78 евро), като е предвидено изпълнението му да приключи в края на юни 2022 г.

3. *AI-Trans: Increasing AI Transparency Through Digital Alternative Learning of Privacy Training*.

По инициатива на КЗЛД в началото на 2019 г. е подготвено и подадено проектно предложение с наименование *AI-Trans: Increasing AI Transparency Through Digital Alternative Learning of Privacy Training* по програма „Еразъм +“. Предложението е одобрено за финансиране през юли 2019 г.

Проектът има за цел да създаде иновативно обучително съдържание въз основа на вече създадено устойчиво и дългосрочно стратегическо партньорство между национални надзорни органи, академични среди и организации на гражданското общество. Той осигурява знания и развитие на уменията, свързани с поверителността и защитата на личните данни във връзка с новите технологии, и по-специално, с изкуствения интелект (*AI*) и интернет на свързаните устройства (*IoT*). Проектът е пръв по рода си, обединяващ национални органи по защита на данните, университети и организация на гражданското общество от 4 държави – Италия, Полша, България и Молдова.

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

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

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

В рамките на проекта са разработени 8 тематични модула, свързани със защитата на личните данни в контекста на съвременните предизвикателства – интернет на свързаните устройства и изкуствения интелект, като през отчетната 2021 г. са завършени

интелектуалните продукти по проекта. Акцент следва да бъде поставен върху Методология за организиране и провеждане на обучение относно интернет на свързаните устройства, 8 онлайн обучителни модула относно *AI* и *IoT*, сред които:

- Технически концепции за *IoT* и въведение в основните проблеми на защитата на данните и защитата на потребителите;
- Роботи за домашни грижи – Право и етика на *AI* и *IoT*;
- Умни уреди за дома – Право и етика на *AI* и *IoT*;
- Медицински, здравни и фитнес устройства за носене – изкуствен интелект и защита на личната информация;
- Умни играчки – Право и етика на *AI* и *IoT*;
- Етика и проблеми със защитата на личните данни в социалните медии в ерата на изкуствения интелект;
- Тъмни модели (*Dark patterns*) – аспекти на електронната търговия и тяхното потенциално подобрение в *IoT/AI* среда;
- Практически насоки относно правата за защита на данните, въпросите на прозрачността, минимални стандарти за сигурност и др.

Третият основен интелектуален продукт по проекта е Кодексът на най-добри практики за ДЛЗД на организации, ориентирани към поверителността. Всички интелектуални продукти са достъпни на онлайн платформата за предоставяне на разяснения и повишаване на информираността на обществото – *eopen.cpdp.bg*.

През отчетния период са реализирани 5 събития за разпространение на резултатите (2 в България и по едно в Полша, Италия и Молдова), както и петдневно онлайн краткосрочно обучение за екипите на организациите – партньори по проекта. В края на ноември 2021 г. е осъществена и втората международна среща на партньорите по проекта, на която са одобрени окончателните версии на интелектуалните продукти, както и планът за подготовката на окончателния отчет за проектното изпълнение.

Окончателно разходваните средства по бюджета на проекта са 184 682,18 лв. (94 426,50 евро). Продължителността на изпълнение на проектните дейности е 27 месеца до края на ноември 2021 г.

4. Подготовка на проектни предложения – програма „Еразъм+“, програма „Граждани, равенство, права и ценности“.

През отчетния период са подготвени 3 проектни предложения по различни програми на Европейския съюз, чието кандидатстване се осъществява през второто, третото и

четвъртото тримесечие на 2021 г. Сред изцяло разработените от администрацията на КЗЛД е и проектно предложение с наименование *DATA4TOURISM – Ensuring the Highest Degree of Privacy and Personal Data Protection through Sector-specific Innovative Tools for SMEs and Citizens*. Проектният формуляр за кандидатстване е завършен в края на отчетния период и успешно подаден в началото на декември 2021 г. Следва да се отбележи, че се затвърждава процесът по подготовка на проектни предложения изцяло от администрацията на КЗЛД без външна консултантска помощ. В допълнение отчетлива е тенденцията Комисията да е водещ партньор в проектните консорциуми за реализирането на одобрените за финансиране проектни инициативи, които не се ограничават на територията на Република България.

IX. КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ – НАБЛЮДАВАЩ ОРГАН ОТНОСНО СИГУРНОСТТА НА ДАННИТЕ СЪГЛАСНО ЗЕС

1. Статистика и анализ на исканията за достъп до трафични данни.

КЗЛД е надзорен орган във връзка с разпоредбите на Закона за електронните съобщения (ЗЕС) относно задържането и достъпа до трафични данни. В изпълнение на разпоредбите на чл. 261а, ал. 5 от ЗЕС КЗЛД ежегодно до 31 май предоставя на Народното събрание и на Европейската комисия обобщена статистическа информация относно случаите на предоставяне на трафични данни на компетентните органи за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления. Тя се изготвя въз основа на постъпилите данни за предходната година от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, относно:

- случаите, при които са били предоставени данни на компетентните органи;
- времето, изтекло от началната дата на съхранението до датата, на която компетентните органи са поискали предаването на данните;
- случаите, при които не е могло да се отговори на искането за данни.

На база предоставената през 2020 г. информация от 114 предприятия, предоставящи обществени електронни съобщителни услуги, през 2021 г. КЗЛД е предоставила следните статистически данни на Народното събрание и Европейската комисия:

- Общият брой на исканията за достъп до трафични данни е **37 853**.
- Случаите, при които са били предоставени данни на компетентните органи по чл. 250б, ал. 1 и чл. 250в, ал. 4 от ЗЕС, са общо **37 525**.
- Времето, изтекло от началната дата на съхранението до датата, на която компетентните органи са поискали предаването на данните, е основно до 3 (три) месеца – в 61% от случаите (фиг. 12).

Случаите, при които не е могло да се отговори на искането за предоставяне на трафични данни, са 328.

Фиг. 12

2. Статистика на получените протоколи за унищожени трафични данни.

В изпълнение на задълженията си по чл. 251ж, ал. 1 от ЗЕС КЗЛД поддържа регистър на получените протоколи от предприятията за унищожените данни с оглед упражняване на ефективен текущ и последващ контрол. Статистическата информация относно получените през отчетната година протоколи е представена на фиг. 13.

Фиг. 13

Броят на предприятията, които изпълняват задължението си за ежемесечно предоставяне на протоколи по чл. 251ж, ал. 1 от ЗЕС за унищожените данни през отчетната година, средно е 74 на месец.

X. РЕАЛИЗИРАНЕ НА ПОЛИТИКИ ЗА ПУБЛИЧНОСТ И ПОВИШАВАНЕ НА ОБЩЕСТВЕНАТА ИНФОРМИРАНОСТ И РАЗБИРАНЕ НА РИСКОВЕТЕ, ПРАВИЛАТА, ГАРАНЦИИТЕ И ПРАВАТА, СВЪРЗАНИ С ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ. ИНСТИТУЦИОНАЛНО ВЗАИМОДЕЙСТВИЕ

1. Анализ на съвременните заплахи и предизвикателства пред защитата на личните данни.

С оглед изпълнение на целите и приоритетите за 2021 г. на КЗЛД, залегнали в Глава XII от „Годишния отчет на КЗЛД за 2020 г.“, се предвиди продължаване на анализа на съвременните заплахи и предизвикателства пред защитата на личните данни. Извършен е анализ на практиката на други надзорни органи и на основните тенденции за развитие в сферата на защитата на личните данни. Този подход спомага за уеднаквяване практиките по прилагането на Регламент (ЕС) 2016/679 в рамките на ЕС, което е и една от основните му цели и дава насоки за бъдещо развитие на българския надзорен орган. Направените проучвания позволяват да се прилага чуждият опит, като се отчитат спецификите на националното ни законодателство.

В изпълнение на тази цел през 2021 г. са извършени три анализа на следните теми:

1. „Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване“;

2. „Големи бази данни (*Big Data*) и свързаната с тях възможност за профилиране;

3. „Правата на децата и младите хора при работа в дигитални платформи. Защита и укрепване на правата на децата и младите хора.“

В изложението по-долу са представени основните акценти от анализите и техните изводи.

Анализ „Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване“

Съществен елемент от анализа са терминологичното изясняване на ключовите понятия „изкуствен интелект“ и „лицево разпознаване“ и очертаване на тяхната същност и съдържание.

Изкуственият интелект (ИИ) е набор от технологии, които съчетават данни, алгоритми и изчислителна мощ, и има потенциал да трансформира основни сектори на индустрията, услугите и обществото като цяло. Според възприетата дефиниция системите с изкуствен интелект са софтуерни (и евентуално хардуерни) системи, проектирани от

хората, които при зададена сложна цел действат във физическото или цифровото измерение, възприемайки средата си чрез събиране на данни, интерпретиране на събраните структурирани или неструктурирани данни, разсъждавайки върху знанието или обработвайки информацията, извлечена от тези данни, в резултат на което вземат решения за най-добрите действия, които водят до постигане на поставената цел.

Теорията на изкуствения интелект се основава на хипотезата, че основно човешко качество като интелигентността може да бъде описано с достоверна точност, така че да бъде симулирано от машина. Затова изкуственият интелект може да бъде дефиниран като способността на една машина да демонстрира способности, присъщи за хората – да разсъждава, да се учи, да планира или да твори. Говорим за ИИ, когато технически системи наблюдават околната си среда, получават данни (които са подготвени от другиго или които набират сами), преработват ги и извършват действия, свързани с постигането на конкретна цел.

Изкуственият интелект е наука за концепциите, методите и средствата за създаване на интелигентни компютърни програми, както и измерване и изследване на естествения интелект чрез компютърни системи с цел техното подобряване.

Лицевото разпознаване представлява технология, способна да съпостави човешко лице от цифрово изображение или видеокадър с база данни от лица. Технологията обикновено се използва за удостоверяване автентичността на потребителите при използване на услуги чрез точно определяне и измерване на черти на лицето от дадено изображение или видеокадър. Задачата на системите за лицево разпознаване е да идентифицират човешко лице, което е триизмерно и променя външния си вид, въз основа на неговото двуизмерно изображение.

За да изпълнят тази изчислителна задача, системите за лицево разпознаване изпълняват четири стъпки. В първата стъпка се сегментира лицето от фона на изображението. Във втората стъпка сегментираното изображение на лицето се подравнява, за да отчетат позата на лицето, размерът на изображението и фотографските свойства. Целта на процеса на подравняване е да даде възможност за точната локализация на чертите на лицето в третата стъпка, в която се извличат характеристиките на лицето. Така установеният вектор на характеристиките на лицето след това, в четвъртата стъпка, се съпоставя с база данни от лица и се идентифицира.

В основата на съвременните системите за видеонаблюдение се използват алгоритми и процеси на изкуствения интелект, които създават условия за автоматизирано вземане на решения с важни последици за субектите на данни. Такова е лицевото разпознаване. От създаването си системите за лицево разпознаване намират широко приложение в

технологиите, една от които са системите за видеонаблюдение, които масово навлизат във всички сфери на живота и непрекъснато се използват поради тяхната достъпност и приложимост. Доскоро системите за видеонаблюдение са били приоритет за специални обекти, банкови офиси и големи предприятия, но днес те се използват за охрана на училища, жилищни комплекси, болници, хотели, офиси, магазини и др.

По отношение на създаването и използването на ИИ в различни отрасли основно се открояват три групи сектори, а именно:

- **Развиващи изкуствен интелект** (*такива са съвременните информационно-комуникационните технологии/софтуер, роботиката и научните изследвания*);
- **Консуматори на изкуствен интелект** (*това са всички проявления на съвременния начин на живот, като напр. производство, логистика, цифрови платформи, електронна търговия, селско стопанство, публична администрация, здравеопазване, интелигентни градове, транспорт, финанси и др.*);
- **Създаващи условия за развитието и внедряването на изкуствен интелект** (*правна рамка и образование*).

В анализа специално внимание е отделено на ползите и рисковете от развитието на изкуствения интелект и новите технологии за лицево разпознаване.

Динамичното развитие на технологиите и все по-широкото използване на различни алгоритми за изкуствен интелект, лицево разпознаване и др. създават възможности за безпрецедентно по обем и дълбочина навлизане в личното пространство и личната неприкосновеност на физическите лица. Използването на технологиите на изкуствен интелект крие редица потенциални рискове като непрозрачност на процеса на вземане на решения, нарушаване на личното пространство и употреба на тези технологии за извършване на незаконосъобразни действия. ИИ може да доведе до предубеждения и по този начин до различни форми на дискриминация, основана на пол, раса, цвят на кожата, етнически или социален произход, генетични характеристики, език, религия или убеждения, политически или други мнения, принадлежност към национално малцинство, имотно състояние, рождение, увреждане, възраст или сексуална ориентация.

Откроени са седем ключови изисквания, които приложенията с ИИ трябва да спазват, за да се смятат за надеждни:

Човешки фактор и надзор

Системите с ИИ да не накърняват автономността на човека и да не причиняват други неблагоприятни последствия.

Техническа стабилност и безопасност

Физическата и психическата безопасност на системите с ИИ да бъде проверима на всеки етап от всички засегнати страни.

Управление на данните и неприкосновеност на личния живот

Данните да са изчистени от неточности или грешки и да не отразяват социални предубеждения.

Обяснимост и прозрачност

Да се регистрират и документират както решенията, взети от системите с ИИ, така и целият процес, който е довел до тези решения.

Многообразие, недискриминация и справедливост

Да се гарантира универсален дизайн за равноправен достъп на лицата с увреждания.

Обществено и екологично благополучие

Да се следи социалното въздействие на ИИ, както и устойчивостта и екологичната отговорност на системите с ИИ.

Отчетност

Да се гарантират отговорност и отчетност за системите с ИИ и техните резултати, да се свеждат до минимум потенциалните отрицателни въздействия.

Въз основа на натрупания опит в световен мащаб Комисията за защита на личните данни формулира няколко основни извода и препоръки по отношение на съвременните

заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване:

- В системите с ИИ трябва да се избягват предубеждения, водещи до дискриминация, и не трябва да се възпроизвеждат дискриминационни процеси. Тези рискове следва да бъдат взети предвид при разработването на технологии с ИИ, както и при работата с доставчиците на технологии с ИИ, за да се предприемат мерки за преодоляване на все още съществуващите пропуски, които улесняват дискриминацията.

- Мрежите от взаимосвързани ИИ следва да бъдат защитени и да се предприемат сериозни мерки за предотвратяване на нарушения на сигурността, изтичане на данни, заразяване на данни, кибератаки и злоупотреба с лични данни. Това ще изисква съответните институции както на равнище Европейския съюз, така и на национално равнище да работят заедно и в сътрудничество с крайните потребители на тези технологии. Държавите членки следва да гарантират зачитането на ценностите на ЕС и зачитането на основните права по всяко време, когато разработват и внедряват технологии с ИИ, за да гарантират сигурността и устойчивостта на цифровите си инфраструктури.

- Възможността, осигурявана от тези технологии, за използването на лични данни с цел категоризиране и насочване към определени лица, откриване на уязвимите страни на отделни лица или извличане на полза от точни предвидими знания трябва да бъде неутрализирана чрез ефективно прилагане на принципите за защита на данните и неприкосновеността на личния живот, като например свеждане на данните до минимум, правото на възражение във връзка с профилирането и контрола върху ползването на данните, правото на получаване на обяснение за решение, основаващо се на автоматизирана обработка, и защита на неприкосновеността на личния живот още на етапа на проектиране на дадена технология, както и чрез прилагане на принципите на пропорционалност, необходимост и ограничение въз основа на строго определени цели в съответствие с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

- Всяко обработване на лични данни, извършвано в контекста на разработването, внедряването и използването на ИИ и свързаните с него технологии, включително лични данни, извлечени от нелични данни, и биометрични данни, да се извършва в съответствие с Регламент (ЕС) 2016/679.

- Да се насърчават научноизследователските проекти, насочени към намиране на решения, основаващи се на ИИ и свързаните с него технологии, които имат за цел насърчаване на социалното приобщаване, демокрацията, плурализма, солидарността, справедливостта, равенството и сътрудничеството.

• Всяка нова регулаторна рамка за ИИ, състояща се от правни задължения и етични принципи за разработването, внедряването и използването на изкуствения интелект и свързаните с него технологии, следва да зачита човешкото достойнство, самостоятелността и самоопределянето на личността, да предотвратява вреди, да насърчава справедливостта, приобщаването и прозрачността, да премахва предубедеността и дискриминацията, включително по отношение на малцинствените групи, и да зачита и спазва принципите за ограничаване на отрицателните външни ефекти на използваната технология, за обяснимост на технологиите и гарантиране, че технологиите съществуват, за да служат на хората, а не да ги заменят или да вземат решения вместо тях, като крайната цел е увеличаване на благоденствието на всеки отделен човек.

• ИИ и свързаните с него технологии в областта на правоприлагането и граничния контрол биха могли да подобрят обществената безопасност и сигурност, но също така се нуждаят от всеобхватен и строг обществен контрол и от възможно най-високо равнище на прозрачност по отношение на оценката на риска за отделните приложения, както и от общ преглед за използването на изкуствения интелект, роботиката и свързаните с тях технологии в областта на правоприлагането и граничния контрол. Тези технологии крият значителни рискове, които трябва да бъдат обмислени подобаващо, като се отчитат възможните неблагоприятни последици за физическите лица, по-специално, във връзка с техните права за неприкосновеност на личния живот, защита на личните данни и недискриминация.

• В контекста на широкоразпространената дезинформационна война, подклаждана по-специално от неевропейски участници, технологиите с ИИ могат да окажат неблагоприятно въздействие в етичен план чрез експлоатиране на предубеденост в данните и алгоритмите или чрез преднамерено променяне на данните на ИИ от страна на трета държава и те биха могли да бъдат изложени също така на други форми на опасна и зловредна манипулация, извършвана по непредвидими начини и водеща до неизмерими последици. Затова е налице все по-належаща необходимост да се продължи с инвестициите в областта на научните изследвания, анализа, иновациите и трансграничния и междусекторен трансфер на знания с цел разработване на технологии с изкуствен интелект, които да са независими от всякакъв вид профилиране, предубеденост и дискриминация и които да могат да допринасят ефективно за борбата с фалшивите новини и дезинформацията, като същевременно се зачитат неприкосновеността на личните данни и правната рамка на Съюза.

• ИИ не следва никога да замества хората, като решенията, които се основават единствено на автоматизирана обработка и произвеждат правно действие по отношение на

физически лица или засягат тези лица в значителна степен, трябва винаги да включват съдържателно оценяване и преценка, извършена от човек.

• Всички технологии с ИИ и свързаните с него технологии, включително софтуерът, алгоритмите и данните, използвани или генерирани от такива технологии, които са разработвани, внедрявани и използвани в ЕС, следва изцяло да зачитат правата на гражданите на неприкосновеност на личния живот и защита на личните данни.

• Използването и събирането на биометрични данни с цел дистанционна идентификация на обществени места като биометрично разпознаване или разпознаване на лица носят специфични рискове за основните права и се внедряват или използват единствено от публичните органи на държавите членки за цели от съществен обществен интерес. Тези органи следва да гарантират, че това внедряване или използване е оповестено публично, пропорционално и целенасочено, ограничено до конкретни цели и места, а също така и по времетраене в съответствие с правото на Съюза и националното право, по-специално, Регламент (ЕС) 2016/679.

Въпреки че Регламент (ЕС) 2016/679 съдържа ефективни решения за правното регулиране на изкуствения интелект и в частност в случаите на обработка на лични данни чрез автоматизирано вземане на решения (*член 22*), КЗЛД данни силно препоръчва да се следят тенденциите в европейски план относно границите, в рамките на които е допустимо обработване на лични данни в този контекст. Във връзка с това е необходимо е да се отчитат препоръките, становищата и предложенията на Европейската комисия, Европейския парламент, ЕКЗД и ЕНОЗД:

• за налагане на мораториум върху масовото наблюдение чрез системи за изкуствен интелект;

• за недопускане на автоматизираното лицево разпознаване на обществени места или за целите на граничния контрол;

• за строги гаранции за физическите лица, когато инструментите на изкуствения интелект се използват в правоприлагането, особено в случаите с прогнозиране на извършители на престъпления;

• за определяне на хармонизирани правила относно изкуствения интелект и за насърчаване разглеждането на проблемите с използването на системи с ИИ, включително използването им от институциите, органите и агенциите на ЕС;

• за изграждане на регулаторна рамка, основаваща се на „етика по подразбиране“ и „етика при проектирането“, която да гарантира, че всеки пуснат в действие ИИ изцяло зачита и спазва законодателството в областта на защитата на личните данни;

• за прилагане на подход, основан на риска, уеднаквен с правната рамка на ЕС в областта на защитата на личните данни, съобразно който се търсят пресечната точка и балансът между развитието на технологиите и правата на човека (*необходимост и пропорционалност*);

• за оценка и намаляване на обществения риск за групите от физически лица;

• за обща забрана върху използването на ИИ за автоматично разпознаване на човешки черти на обществено достъпни места и на някои други употреби на ИИ, които могат да доведат до несправедлива дискриминация, например разпознаване на лица, походка, пръстови отпечатъци, ДНК, глас, натискане на клавиши и други биометрични или поведенчески данни, в какъвто и да било контекст поради изключително високия риск, свързан с дистанционната биометрична идентификация на лица на обществено достъпни места;

• за забрана върху използването на биометрични данни в рамките на системи с ИИ за категоризиране на отделни лица в групи въз основа на етническа принадлежност, пол, политическа или сексуална ориентация или на други основания, при които има забрана на дискриминация;

• за забрана върху използването на ИИ за всякакъв вид социална оценка и за съставяне на изводи за емоциите на физически лица (освен в много специфични случаи, например по здравословни причини, когато разпознаването на емоциите е важно).

За КЗЛД от съществено значение е ролята на повишаването на обществената информираност не само относно заплахите, но и относно възможностите, които виртуалното пространство създава пред субектите на данни. КЗЛД споделя разбирането, че за да защити информационните права в цифровата ера, тя, като надзорен орган, трябва да стане по-ефективна в предвиждането, тълкуването и влиянието на подобен напредък в начина на използване на данните. Необходимо е организирането на повече събития, които дават възможност за обмяна на експертни знания и опит в постигането на по-висока степен на защита на неприкосновеността на личния живот, обмен на идеи за законодателни и практически промени в областта на дигитализацията и обществото им оповестяване. КЗЛД, в качеството си на надзорен орган за защита на данните, следва да инициира дискусии по тези въпроси за повлияване на приемането на високи стандарти за защита на данните в Р България. Темите, върху които е необходимо да се обърне сериозно внимание, включват: поверителност и конкуренция, бъдещето в онлайн проследяването, изкуствен интелект в съответствие със защитата на данните, средства за защита в дигиталната ера,

иновации, свързани с пандемията – стрес тест за правата на субектите на данни и достъпа на властите до личните данни.

При отчитане на етичните граници на използването на изкуствения интелект КЗЛД ще продължи да следи процеса по правното му регулиране като едно от най-сериозните предизвикателства пред правната система на ЕС и националните правни системи на държавите членки.

Анализ „Големи бази данни (*Big Data*) и свързаната с тях възможност за профилиране“

Бързото технологично развитие, широкото използване на компютрите, интернет и цифровите технологии, глобализацията създават нови предизвикателства пред защитата на личните данни. В ерата на цифровия свят, в който живеем днес, всяка дейност оставя цифрова следа, която може да бъде събрана, обработена и оценена или анализирана. С новите информационни и комуникационни технологии се събират, записват и анализират все повече данни.

В анализа си относно съдържанието на концепцията за „големите бази данни“ КЗЛД посочва, че за пръв път през 2001 г. *Laney* споменава трите *V*-та (*Volume, Variety, Velocity*), които са в основата на дефиницията на понятието *big data*. Обемът (*Volume*) се отнася до огромния физически обем на масивите от данни, скоростта на нарастване (*Velocity*) – до актуалността, скоростта на обновяване, обработка и получаване на резултат в реално време, а многообразието (*Variety*) е свързано с различните източници и форми на представяне на данните.

„Големи информационни масиви“ („Големи бази данни“, *Big Data*) е модерен термин, който може да се отнася до няколко понятия в зависимост от контекста. Той най-общо включва „нарастващата технологична способност за събиране, обработване и извличане на нова и прогнозна информация от голям обем, скорост и разнообразие от данни“. Следователно понятието „големи информационни масиви“ обхваща едновременно самите данни и анализа на данните.

Източниците на данните са най-различни по вид и включват хора и техни лични данни, електронни устройства, машини или датчици, информация за климата, спътникови изображения, цифрови снимки и видеоматериали или *GPS* сигнали. Данните могат да се генерират от хора чрез мобилни приложения, в интернет, през социалните мрежи или плащания, данни на публичната администрация и др.

„Интернет свързаните устройства/интернет на вещите/интернет на предметите“ (*Internet of Things, IoT*) през последните години се утвърди като един от основните нови

източници на големи данни. Метаданните също могат да образуват големите данни. Големи данни се получават също в производството, здравеопазването, образованието и други обществени сфери, като ежедневно обемът на съхраняваните в компютърните системи данни расте експоненциално.

Големите масиви от данни са толкова широкообхватни и сложни, че изискват нови технологии за обработка като изкуствения интелект.

Въз основа на анализа на ползите и рисковете, свързани с големите информационни масиви, се констатира, че действителното и потенциалното въздействие на обработката на огромни количества данни оказват влияние и засягат правата и свободите на хората, включително неприкосновеността на личния им живот. Затова предизвикателствата и рисковете, свързани с големите масиви от данни, налагат по-ефективна защита на данните.

Съвременните техники за обработване на данни са в състояние да обхванат големи масиви от данни, да импортират бързо нови данни, да осигуряват обработване в реално време на информацията при кратки срокове за реагиране и да предоставят възможност за множество и едновременни искания, като могат да анализират различни видове информация (снимки, текстове или номера).

Възможността за анализ и обработване на големи информационни масиви по структуриран начин осигурява нови средства за профилиране и целева реклама.

Анализът на големи информационни масиви може да разкрие закономерности между различните източници и масиви от данни, давайки възможност за осигуряване на полезна информация в различни области. Анализът на информацията в реално време може да бъде използван за подобряване на въведените системи.

Събирането и обработването на лични данни в една глобализирана икономика означават нарастване на броя на трансграничните потоци от данни. Това обработване може да доведе до значителни и видими ползи в ежедневието: интернет търсачките улесняват достъпа до значителни обеми информация и знания, услугите за социални мрежи дават възможност на хората в целия свят да общуват, да изразяват мнението си и да мобилизират подкрепа за социални, екологични и политически каузи, а дружествата и потребителите се възползват от ефективни и ефикасни маркетингови техники, които стимулират икономиката. Технологиите и обработването на лични данни също така представляват незаменими инструменти за държавните органи в борбата им срещу престъпността и тероризма.

Големите информационни масиви обаче носят и рискове, които обикновено са свързани с три техни характеристики: обем, скорост и разнообразие на обработваните данни. Рисковете за защитата на данните и неприкосновеността на личния живот, свързани

с големите информационни масиви, са подчертани в становища на Европейския надзорен орган по защита на данните (ЕНОЗД) и на Работната група по член 29, в резолюции на Европейския парламент и в документи по политиката на Съвета на Европа. Те може да включват неправомерна употреба на големите информационни масиви от лица с достъп до масивите от информация посредством манипулиране, дискриминация или потискане на отделни лица или на конкретни групи в обществото.

Големите информационни масиви създават значителни рискове, а именно във връзка със защитата на основните права като правото на неприкосновеност на личния живот и защитата и сигурността на данните, а също и свободата на изразяване на мнение и недопускането на дискриминация. Техниките за псевдонимизация и криптиране може да смекчат рисковете, които са свързани с анализа на големи информационни масиви.

В определени случаи използването на големи информационни масиви включва и обучаването на устройства с изкуствен интелект като невронни мрежи и статистически модели с цел предвиждане на определени събития или поведение. Често данните за обучението са със съмнително качество и не са неутрални.

Развитието на комуникационните технологии и повсеместното използване на електронни устройства, устройства за наблюдение, социални медии, уеб взаимодействия и мрежи, включително устройства, които съобщават информация без намесата на човека, водят до развитието на масивни, нарастващи набори от данни, които чрез съвременни техники за обработка и анализ предоставят безпрецедентен поглед върху човешкото поведение, личния живот и обществото.

Чувствителна информация за лица може да се изведе и от нечувствителни данни, което размива границата между чувствителни и нечувствителни данни.

Цифровата грамотност и повишаването на осведомеността за цифровите права, неприкосновеността на личния живот и защитата на данните сред гражданите, включително и сред децата, както и повишаване на разбирането относно това къде и как потоците от данни се събират са от изключително значение.

Степента, в която може да бъде засегната неприкосновеността на личния живот и личните данни, е невъзможно да се измери точно.

Технологичният напредък и възможностите за анализи на големи информационни масиви, изкуственият интелект и машинното самообучение улесняват създаването на профили и вземането на автоматизирани решения, които имат потенциал да окажат значително въздействие върху правата и свободите на физическите лица.

Широкоразпространената достъпност на лични данни в интернет (физическите лица все по-често оставят лична информация, която е публично достъпна и в световен мащаб) и

от интернет свързани устройства (*IoT*), както и възможността да се установяват корелации и да се създават връзки могат да позволят определяне, анализ и предвиждане на личностни или поведенчески аспекти на даден човек и на неговите интереси и навици.

В контекста на интернет на предметите/вещите големият обем лични данни, генерирани от различните взаимосвързани устройства, също поражда рискове за неприкосновеността на личния живот и защитата на данните. Поради множеството свързани устройства невинаги е ясно кой може да събира, да има достъп до и да използва данните, събрани от базираните на интернет на предметите устройства.

В тази връзка рисковете, правилата, гаранциите и правата по отношение на обработването на техните лични данни трябва да бъдат изяснени на физическите лица.

Свързаните чрез интернет на предметите устройства и множеството операции по обработване и засегнати данни също могат да бъдат предизвикателство за изискването за ясно и информирано съгласие за обработването на данни, когато това обработване се основава на съгласие. Хората често не разбират техническото функциониране на това обработване и следователно последиците от своето съгласие.

Друг важен повод за безпокойство е сигурността, като се има предвид, че свързаните устройства са особено уязвими към рисковете за сигурността. Свързаните устройства имат различни нива на сигурност.

От гледна точка на защитата на данните основните проблеми са свързани, от една страна, с обема и разнообразието на обработваните лични данни и от друга страна, със самото обработване и резултатите от него.

Големите информационни масиви и изкуственият интелект повдигат редица въпроси относно идентифицирането на администраторите и обработващите лични данни, както и относно тяхната отговорност: Кой е собственикът на данните, когато се събира и обработва такова голямо количество данни? Кой е администраторът, когато данните се обработват от машини и софтуер? Какви са конкретните отговорности на всяко действащо лице при обработването? и За какви цели могат да се използват големите информационни масиви?

Въпросът за отговорността в контекста на изкуствения интелект ще стане още по-сложен, когато изкуственият интелект вземе решение въз основа на обработка на данни, разработена от самия него.

Изкуственият интелект и автоматизираното вземане на решения повдигат въпроси за това кой носи отговорност за нарушенията, които засягат неприкосновеността на личния живот на субекта на данните, когато сложността и обемът на обработваните данни не може да бъдат определени със сигурност.

Големите информационни масиви поставят предизвикателство и пред принципа за точност на данните, тъй като свързаните с тях приложения обикновено събират данни от различни източници, без възможност да се проверява и/или поддържа точността на събираните данни.

Сложността и липсата на прозрачност по отношение на анализа на големи информационни масиви може да изискват преосмисляне на идеите за контрол на личните данни от страна на лицата.

Съгласието на субектите на данните и на лицата при обработването на големи информационни масиви също представлява предизвикателство за законодателството в областта на защитата на данните.

Контролът от страна на лицата върху обработването на техните лични данни и тяхната осведоменост по тези въпроси са от решаващо значение при анализа на големи информационни масиви: без това те няма да имат ясна представа кой е администраторът или обработващият лични данни и няма да могат да упражняват ефективно своите права.

Псевдонимизацията, анонимизиране или криптиране на личните данни са подходящи предпазни мерки за намаляване на рисковете за съответните субекти на данни, когато личните данни се използват в приложения за големи информационни масиви.

При всички случаи, независимо от избрания бизнес модел организациите, които обработват големи обеми лични данни, трябва да спазват приложимото законодателство в областта на защитата на данните.

Въпреки своите многобройни ползи цифровата ера създава и предизвикателства пред неприкосновеността на личния живот и защитата на данните, тъй като огромни количества лична информация се събират и обработват по все по-сложни и непрозрачни начини.

Предизвикателствата пред големите данни включват тяхното регистриране, съхранение, анализ, търсене в тях, споделяне, трансфер, визуализация, правене на запитване/заявка в тях, обновяване, сигурност и видове източници за работа с тях. Важно е да се определят ясни правила и процедури за работа с големи бази данни, съдържащи лични данни на физически лица, в целия процес по тяхното обработване – събирането, получаването, съхранението, предоставянето и унищожаването им, като се предвидят възможности за минимизиране на рисковете за лицата при евентуално изтичане на такава информация. Обработката на големи данни изисква нов подход, базиран на изкуствения интелект (*AI*), в който връзката между големите данни и *AI* се осъществява от високоскоростни мрежи.

Защитата на данните е неразделно свързана с технологичните, социалните и политическите промени. Те влияят пряко на процесите по обработване на данните и предопределят бъдещите заплахи и предизвикателства пред защита на личните данни.

В резултат от направения анализ КЗЛД дава следните насоки към администраторите на лични данни и физическите лица за изпълнение на техните задължения и упражняване на техните права:

Задължения на администраторите на лични данни

Съгласно Регламент (ЕС) 2016/679 в контекста на обработването на големи бази данни администраторите на лични данни са задължени да:

- Уведомят субектите на данни за съществуването на автоматизирано вземане на решения, включително профилиране *(член 12),* като уведомлението съдържа и съществена информация относно използваната логика при профилирането и предвидените последствия от това обработване за лицата *(член 13, параграф 2, буква „е“)*;
- Предприемат подходящи мерки, за да гарантира правата, свободите и законните интереси на субектите на данни. Това включва най-малко правото на човешка намеса от страна на администратора и възможността субектът на данните да изрази гледната си точка и да оспори решение, което се основава на автоматизирано обработване на личните му данни *(член 22, параграф 3)*;
- Изрично да предоставят подробности относно правото на възражение *(член 21, параграф 1 и 2)* на вниманието на субекта на данни и да ги представи по ясен начин и отделно от всяка друга информация *(член 21, параграф 4)*;
- Спазват принципа за свеждане на данните до минимум, както и изискванията за ограничение на целите и принципите за ограничение на съхранението;
- Личните данни в контекста на профилирането следва да бъдат обработвани добросъвестно, законосъобразно, пропорционално и за конкретни и легитимни цели;
- Предприемат мерки да коригират факторите, които водят до неточности в личните данни;
- Въведат надеждни мерки за постоянна проверка и гарантиране, че повторно използваните или получените по косвен път данни са точни и актуални;
- Демонстрират, че субектите на данни разбират с какво точно се съгласяват, и също така да помнят, че съгласието невинаги представлява подходящо основание за обработване;

• При наличие на легитимен интерес трябва да се извърши балансиране, за да се оцени дали пред интересите на администратора преимущество имат интересите или основните права и свободи на субекта на данните;

• Ограничат рисковете или грешките, които профилирането може да предизвика;

• Периодично да оценяват качеството на използваните данни и алгоритми;

• Гарантират, че профилирането и автоматизираното вземане на индивидуални решения (независимо дали включва профилиране или не) не се използват по начини, които оказват необосновано въздействие върху правата на физическите лица;

• Ако от профилирането се извличат чувствителни предпочитания и характеристики, администраторът следва да гарантира, че: 1. обработването не е несъвместимо с първоначалната цел, 2. е определил законосъобразно основание за обработването на специалните категории данни, както и 3. е информирал субекта на данни относно обработването;

• Извършват анализ на риска и оценка на въздействието върху защитата на данните;

• Определят видовете потребители в информационните системи;

• Утвърдят правила за отделните потребители на информационните системи, функционалните им задължения и процедурите за тяхната дейност, в които достатъчно ясно да са разписани принципите на взаимодействие на отделните потребители;

• Утвърдят правила за обработка на личните данни за всяка една от поддържаните информационни системи;

• Утвърдят правила и процедури за защита на личните данни, в т.ч. информационната/киберсигурност;

• Утвърдят вътрешни правила за обучение и тренировка на служителите за действия в случаи на незаконосъобразно обработване на лични данни;

• Поддържат журнални записи (*log файлове*) на действията на потребителите на информационните системи;

• Имат налична документация къде и как на етапа на проектиране на информационните системи е приложен чл. 25 от Регламент (ЕС) 2016/679 (защита на данните на етапа на проектиране и по подразбиране);

• Утвърдят политики и процедури за защита на личните данни, които гарантират спазването на Регламент (ЕС) 2016/679 и ЗЗЛД, при наемане на облачни услуги и тяхното управление по отношение на достъп/преносимост/възстановяване/унищожаване на данни, в т.ч. извършване на анализ на риска при използването на външен доставчик.

Права на физическите лица

Съгласно Регламент (ЕС) 2016/679 в контекста на обработването на големи бази данни физическите лица имат следните права:

- Да не бъдат обект на решение, което ги засяга в значителна степен и се основава единствено на автоматизирано обработване, без да се вземат предвид техните гледни точки *(Модернизирана конвенция №108, член 9, параграф 1, буква „а“);*
- Да предявяват искове срещу администратора, който е създал профила, и срещу администратора, който е взел автоматизирано решение относно субект на данни (със или без човешка намеса), ако тези две образувания са различни;
- Правото на достъп до личните данни, обработвани от администратора чрез автоматизирано вземане на решения, остава незасегнато *(член 15)*;
- Да получат подробности относно лични данни, които се използват за профилиране, включително категориите данни, които се използват за създаване на профил;
- Да упражнят правата си на коригиране, изтриване и ограничаване на обработването. Администраторът на данни може да бъде освободен от задължението да съобщава на субекта на данните за всяко извършено коригиране или изтриване на неговите лични данни и когато такова уведомяване „е невъзможно или изисква несъразмерно големи усилия“ *(Регламент (ЕС) 2016/679, член 19)*;
- Да оспорват решения, които се основават единствено на автоматизирано обработване. Те не могат да упражняват това право, ако автоматизираното решение е разрешено в закон, който е приложим спрямо администратора и в който се предвиждат и подходящи мерки за защита на правата, свободите и законните интереси на субектите на данни;
- Да бъдат уведомени за причините за извършваното обработване *(Модернизирана конвенция №108, член 9, параграф 1, буква „в“)*;
- Да бъдат информирани от администратора и при определени обстоятелства имат право да възразят срещу „профилирането“, независимо дали се извършва изцяло автоматизирано вземане на индивидуални решения, основано на профилиране;
- Да могат да оспорват евентуални неточности в използваните от администратора на лични данни и релевантността на прилагания към тях профил *(Обяснителен доклад към модернизираната Конвенция №108, параграф 75)*;
- Да възразят срещу обработването (включващо профилиране) на основания, свързани с неговата конкретна ситуация;

• Да възразят срещу обработване на техните лични данни за целите на директния маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг.

Цифровата грамотност и повишаването на осведомеността за цифровите права, неприкосновеността на личния живот и защитата на данните сред гражданите и сред децата, както и повишаването на разбирането относно това къде и как потоците от данни се събират (т.е. извличане на данни от интернет, съчетаване на стрийминг данни с данни от социални мрежи и свързани устройства и обединяването им в нов поток от данни) са от изключително значение. Контролът от страна на лицата върху обработването на техните лични данни и осведомеността им по тези въпроси са от решаващо значение при анализа на големи информационни масиви: без това те няма да имат ясна представа кой е администраторът или обработващият лични данни и няма да могат да упражняват ефективно своите права. Във връзка с това КЗЛД следва да насочи усилията си в извършването на постоянен анализ на потенциалните въздействия на големите информационни масиви и интернет свързаните устройства върху етиката и морала. Целта на подобен подход са намирането на баланса между реализацията на ползите от технологиите за обществото и гарантирането на правата и свободите на хората, в т.ч. правото на защита на техните лични данни. КЗЛД би могла да бъде полезна с консултации и насоки към администраторите при определянето на ясни правила и процедури за работа с големи бази данни, съдържащи лични данни на физически лица, в целия процес по тяхното обработване с цел минимизиране на рисковете за лицата при евентуално разкриване на такава информация. Това съдействие от КЗЛД може да се получи в рамките на производството по провеждане на предварителна консултация на основание чл. 36 от Регламент (ЕС) 2016/679 във връзка с чл. 58 – 61 от Правилника на КЗЛД и на нейната администрация, вкл. по инициатива на Комисията, когато обработването е за изпълнението на задача в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве.

Анализ на тема „Правата на децата и младите хора при работа в дигитални платформи. Защита и укрепване на правата на децата и младите хора“.

Целта на анализа е да предостави задълбочено основните принципни положения при обработването на лични данни на деца и защита на техните права при работа в дигитални платформи. Обърнато е внимание, че приложимостта на общите норми за защитата на личните данни (Регламент (ЕС) 2016/679 като *lex generalis*) следва да 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 анализа е поставен акцент върху основни положения при обработване на имената, изображенията и други лични данни, предоставяни от деца в цифровата среда. Разгледана е възможността за даване на съгласие за обработване на данни при ползването на дигитални услуги и възможните подходи за проверка на възрастта на потребителите деца с цел недопускане достъпа на деца до онлайн услуги, на които те нямат право. Обърнато е специално внимание на оценката на риска, която трябва да се извърши от администратора на лични данни, както и изискванията, свързани със своевременното изтриване на предоставената от децата и младите хора информация. Разгледани са добри практики и примери за онлайн инструментите за защита на лични данни, контрол на възрастта, както и споделянето на личните данни с трети лица, данни за геолокация, както и възможности за родителски контрол, забрана за профилиране и т.н.

Водеща линия на анализа е, че всички действия, отнасящи се до деца в дигитална среда (както и *offline*), следва да се подчиняват на общовалидния принцип за най-добрия (най-висшия) интерес на детето, тъй като той е от първостепенно значение. Концепцията за най-добрия интерес на детето произтича от разпоредбата на чл. 3 от Конвенцията на ООН за правата на детето. Съгласно посочената разпоредба висшите интереси на детето са първостепенно съображение във всички действия, отнасящи се до децата, независимо дали са предприети от обществени или частни институции за социално подпомагане, от съдилищата, административните или законодателните органи. Най-добрият интерес на детето трябва да се вземе предвид при всички мерки и решения, отнасящи се до децата. Конвенцията на ООН за правата на детето съдържа универсални разпоредби, насочени към защита на нуждите на детето по отношение на сигурност, здраве, благополучие, семейни отношения, както и физическо, психологическо и емоционално развитие, идентичност, свобода на словото и почтеност за формиране на собствено мнение и правото да бъде чуто.

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 на най-добрия интерес на детето.

В този смисъл обработването на лични данни на дете при предоставянето му на дадена услуга онлайн в никакъв случай не трябва да води до нарушаване на принципа за най-висшия интерес на детето. При преценка кой е най-добрият интерес на детето трябва да бъдат положени всички усилия за намиране на баланса, респ. за съгласуване на правото

на защита на детето с другите му права, по-специално, с правото на свобода на изразяване и информация**,** както и правото на участие (в различни инициативи).

Особено внимание се обръща на различните нива на зрялост на детето и адаптирането на дигиталната среда към тази особеност, тъй като различните деца достигат различни нива на зрялост на различна възраст, включително тези на деца с увреждания или в уязвими ситуации. Политиките и практиките, насочени към тези деца във връзка с достъпа до цифрова среда, трябва да отговарят на съответните им нужди. Да се отчитат индивидуалните способности на децата за постепенно развитие също означава например, че политиките за изпълнение на правата на подрастващите да могат/да трябва да се различават значително от тези, предназначени за по-малки деца. В този смисъл изрично се подчертава забраната за дискриминация.

Важно място в анализа намира равнопоставеността на защитата на свободата на изразяване и правото на информация на младите хора, от една страна, и защитата на личните данни – от друга, при съобразяване с възрастовите им особености. Важно е децата да бъдат оставени да изразяват своето мнение, доколкото разполагат с капацитет за това и при отчитане на техния най-добър интерес. Достига се до извода, че доставчиците на онлайн услуги трябва да познават своята аудитория и да предприемат подходящи стъпки, за да идентифицират своите потребители, да гарантират, че услугите, насочени към, предназначени или които е вероятно да бъдат достъпени от деца, прилагат ефективно на практика специфични мерки за защита на данните, конкретно насочени за деца.

В анализа си КЗЛД обръща внимание и на профилирането, когато то засяга деца. По принцип профилирането е вредно за децата и затова то трябва да бъде изключено по подразбиране, освен ако не е от същностно значение и условие за предоставяне на услугата или има убедителна причина да бъде включено (напр. при наличие на надделяващ обществен интерес, при условие че са налице подходящи гаранции, предвидени от закона). Пример за допустимо профилиране е профилирането с цел гарантиране на възрастта на потребителите деца. Следва да се има предвид обаче, че всяко профилиране, използвано за целите на верифициране на възрастта, не трябва да създава рискове, които са по-високи от рисковете, за които се използва верифицирането на възраст. Ако профилирането е необходимо условие за предоставяне на дадена онлайн услуга, може да е възможно да се използва споразумението за услуга като допустимо правно основание за извършването му. Профилирането с единствена цел „защита на децата“ може да се основава на баланс на интересите като правно основание, като се отчита, че е в най-добрия интерес на детето. В други често срещани случаи се изисква съгласие за профилиране, тъй като то се счита за много чувствително по отношение на неприкосновеността на лицата и в повечето ситуации

е трудно да се обоснове профилирането от гл.т. на Конвенцията на ООН за правата на детето и правилата за защита на данните.

Обработването на данни в дигитална среда следва да взема предвид принципите за защита на данните на етапа на проектирането и по подразбиране, като същите имат особено важно значение, когато става въпрос за работа с деца и млади хора с характерните им възрастови особености и ниво на зрялост. В контекста на личните данни на деца всички аспекти на обработването, вкл. чрез съответните продукти и системи, трябва да бъдат проектирани по начин, който отчита, че децата имат право на специална защита, че трябва да се чувстват в безопасност, когато използват услуги онлайн, и че тяхното право на неприкосновеност следва да се зачита.

Предоставянето на информация и прозрачността при обработването на лични данни на деца в дигитална среда се подчиняват на изискванията за яснота, разбираемост и липса на манипулативни действия, насочени към децата. Децата и младите хора имат права в областта на защитата на личните данни, като към възможностите за тяхното упражняване следва да са насочени всички усилия на доставчиците на дигитални услуги, предназначени за тях.

Ако администратор иска да използва личните данни на деца и младежи за маркетингови цели (няма абсолютна забрана за тази дейност), той трябва да е сигурен не само, че спазва приложимите разпоредби в тази област, но и че взема предвид това, което се счита за най-добрия интерес на детето.

Използването на лични данни на непълнолетни за маркетингови цели може да бъде необходимо за изпращане на реклама по имейл (директна реклама) или за насочване на персонализирани реклами към деца и младежи в платформите, които посещават. Онлайн маркетингът се среща в много формати като банери, рекламни слотове на видеосподеляне на платформи или игри и други неща, които децата често използват. Има и маркетинг, вграден в социалните медии.

Преди да бъдат използвани личните данни на деца и младежи за маркетингови цели, Общият регламент относно защитата на данните изисква от администратора да разполага с правно основание за такова обработване. Правното основание, което най-често се използва за обработване на лични данни за маркетингови цели, е, когато е необходимо за целите на легитимните интереси на администратора. В този случай обаче анализът на баланса между законните интересите на администратора и интересите, основните права и свободи на децата и младежите задължително трябва да отчита концепцията за „най-добрия интерес на детето“.

Децата са по-малко наясно с рисковете, но в същото време заслужават специална защита в съответствие с действащите законови изисквания. Поради тази причина е важно навреме да се извършва балансът между техните права, свободи и интереси и тези на администратор и да се предпазват децата от рискове, които те може да не могат да оценят и за които може да не са наясно. Това е особено вярно при използването на лични данни на децата за маркетингови цели, за създаване на потребителски профили и в услуги, насочени директно към деца.

В анализа се отделя внимание и на актуални теми като използването на дизайнерски техники, които да повлияят на изборите, направени от децата и младите хора (цифрово побутване, *nudging*), както и свързаните играчки и устройства, предназначени за деца и млади хора („интернет свързани устройства“).

Анализът се фокусира и върху някои особени аспекти на взаимодействието на младите хора с дигиталните платформи като необходимостта от защита от вредното медийно влияние, използването на данните за маркетингови цели, борбата със заплахите и речта на омразата. Основният извод, който извежда Комисията, е, че дигиталната технология при обработването на лични данни сама по себе си не съставлява голямата част от проблема, проблемът е как се използва тя. Важен принцип, който трябва за се прилага при възпитанието на децата и младите хора за работа в дигитална среда, е, че това, което е недопустимо *offline*, е недопустимо и *online*.

Като взема предвид Препоръка за децата в цифровата среда на Организацията за икономическо сътрудничество и развитие, както и добрите практики на сродните си надзорни органи от Швеция и Франция, КЗЛД представя следните препоръки към заинтересованите страни:

1. **Към разработчиците и доставчиците на цифрови услуги** с цел осигуряване на безопасна и полезна цифрова среда за децата, чиито лични данни те обработват:

– 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, вкл. задаване на по-строги настройки за поверителност по подразбиране, при зачитане на най-добрия интерес на детето;

– Да засилят правото на информация и другите права на децата на етапа на проектирането (по дизайн), както и да гарантират ефективно и прозрачно предоставяне на информация за това как ще бъдат използвани техните лични данни. Информацията трябва

да бъде адаптирана към децата винаги когато те са целевата група на дадена услуга в дигитална среда;

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

– Да демонстрират и доказват управление и отчетност.

2. **Към родителите** с цел насърчаване на родителския контрол в дигитална среда по начин, който зачита неприкосновеността и най-добрите интереси на детето и който отговаря на правилата за защита на данните, и по-специално на:

– принципа на пропорционалност, като се вземат предвид интересите, възрастта и степента на зрялост на детето и избягване на използването на натрапчиви функции като постоянно проследяване;

– принципа на прозрачност спрямо детето чрез ясно обяснение кои родителски контроли се използват;

– принципа на сигурност на данните на детето, за да се гарантира, че трети страни нямат достъп до информация за детето (например данни за геолокация на детето).

– да предоставят подкрепа на децата си, когато те лично упражняват своите права в областта на защитата на личните данни, както и да упражняват тези права от тяхно име;

– да получат подкрепа по линия на цифрово образование/обучение, за да знаят достатъчно за наличните начини за защита на правата на децата си онлайн.

3. **Към децата и младите хора:**

– да бъдат стимулирани да се интересуват, да четат и да узнаят минимално необходимото за това какво са лични данни, кой и как борави с тях и защо, за да научат, че имат права и да са наясно, че обработването на техни лични данни е свързано с определени рискове и евентуални негативни последици;

– да бъдат насърчавани автономно да упражняват правата си по отношение на социални мрежи, игри и платформи за споделяне на видео;

– да споделят със своите родители и учители за проблеми и притеснения, които срещат онлайн.

В своята бъдеща надзорна дейност КЗЛД е необходимо да следи за спазването на водещите принципни положения, които изграждат концепцията за защита на личните данни на децата, изложени по-горе, при зачитане на завишените изисквания, произтичащи от приложимата специална международноправна и националноправна уредба. Навременният контрол върху спазването им от страна на администраторите и обработващите е важна

предпоставка за законосъобразност на обработването и гарантирано упражняване на правата на децата в областта на защитата на личните данни. За тази цел КЗЛД следва да засили контролната си дейност под формата на секторни анализи и/или секторни проверки на администратори и обработващи, чието обработване е насочено към деца. Специфичен фокус на този контрол може да бъде обработването на лични данни на деца, структурирани в големи бази данни. Друг задължителен елемент от контрола следва да бъде изпълнението на задължението за извършване на оценка на въздействието при обработване на лични данни на деца при пряко предлагане на услуги на информационното общество, каквото изискване произтича за администраторите в изпълнение на чл. 35, пар. 4 от Регламент (ЕС) 2016/679 във връзка с т. 7 от Списъка на видовете операции по обработване на лични данни, за които се изисква извършване на оценка на въздействието върху защитата на данните, приет от КЗЛД. Наред с това е необходима поетапна и систематична информационно-образователна 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.

2. Сътрудничество с държавни органи, неправителствени организации и частни организации.

По редица въпроси от обществен интерес, имащи отношение към обработването и защитата на личните данни, през отчетния период КЗЛД осъществява ползотворно сътрудничество, вкл. в оперативен порядък, с множество държавни органи, сред които Инспектората 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 транспорта, информационните технологии и съобщенията и Комисията за регулиране на съобщенията. От особено значение за дейността на КЗЛД през отчетния период е приемането на актуализирани съвместни Указания с Централната избирателна комисия относно защитата и обработването на лични данни в изборния процес – израз на постоянното междуинституционално сътрудничество между КЗЛД и ЦИК. Тези Указания, първоначално приети в навечерието на изборите за Европейски парламент през 2019 г., са прегледани и осъвременени с оглед актуализирането на изборните правила през последните години и обществените потребности в контекста на изборите за Народно събрание, насрочени, а впоследствие произведени през април 2021 г.

За осъществяване на стратегическата цел „Усъвършенствани процеси по откритост и прозрачност“ е подписано споразумение със сдружение „Национална асоциация за защита

на потребителите“ с цел извършване на проучване и съдействие при констатирани нарушения и порочни практики по отношение на потребителите при ползването на услуги на доставчици на съдържание онлайн чрез така наречените „бисквитки“. Проведена е и консултативна среща с Асоциацията на европейските журналисти – България, за проучване на възможностите за евентуалното ѝ бъдещо присъединяване към инициативата.

Продължава регулярното взаимодействие с Министерството на правосъдието. Като традиционно добра и ефективна е работата в рамките на Работна група 33 – „Сътрудничество в областта на правосъдието и защита на данните“ към Съвета по европейски въпроси (СЕВ) към Министерския съвет. Дейностите в този формат дават възможност за взаимопомощ и съдействие по редица документи (рамкови позиции, позиции по преюдициални запитвания, анализ и информация за различни формати и участия на представители на съответната институция и др.). От съществено значение е и усилената работа по предложения от Министерството на правосъдието Закон за защита на лицата, подаващи сигнали или оповестяващи публично информация за нарушения, с който се въвеждат изискванията на Директива (ЕС) 2019/1937 на Европейския парламент и на Съвета от 23 октомври 2019 г. относно защитата на лицата, които подават сигнали за нарушения на правото на Съюза (ОВ, L 305/17 от 26 ноември 2019 г.).

Поради продължаващата работа на общоевропейско ниво по регламенти относно цифровата икономика и пазари и неприкосновеността на личния живот в цифровата среда (по Регламента за електронната неприкосновеност и Директивата за временни дерогации, по Акта за управление на данните, както и рамкови позиции по привеждане на инструментите на ЕС в областта на наказателното право в съответствие с правилата на ЕС за защита на личните данни – Рамково решение 2002/465/ПВР и Директива 2014/41/ЕО), активно е и участието (изразяването на позиции) в 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).

Традиционно е засилено сътрудничество на КЗЛД с МВР. През изтеклата година освен обичайното изразяване на становища по документи, предоставени за съгласуване на вниманието на КЗЛД, във формален и неформален порядък двете институции са си съдействали по редица правни въпроси от взаимен интерес (сключване на споразумения, рамкови позиции във формат Работна група 23 „Сътрудничество в областта на вътрешните работи“ към СЕВ, както и споделени участие в заседания на Работна група „Защита на данните към Съвета на ЕС в случаите, когато темите на заседанията представляват интерес

за представители на МВР). Не на последно място, продължава изключително доброто сътрудничество с длъжностното лице по защита на данните на МВР, което предпоставя и зачитането на единни и завишени стандарти на защита на данните на субектите, чиито данни се обработват от МВР.

Важен партньор на КЗЛД през отчетния период остава Министерството на образованието и науката. В духа на дългогодишно сътрудничество и в изпълнение на стратегическите си цели КЗЛД е предложила и поела ангажимент да разработи обучителни материали за защитата на данните на деца с фокус върху различни таргет групи – преподаватели, родители и самите деца в ученическа възраст. Материалите ще бъдат предоставени на МОН и съответно разпространени в рамките на 2022 г. като част от юбилейните събития на КЗЛД по повод 20-ата годишнина от създаването на институцията.

През изминалата година експерти от КЗЛД са участвали активно в дейността на Работна група 17 „Телекомуникации и информационни технологии“ към СЕВ, която е пряко свързана с функциите на Работната група по телекомуникации и информационно общество (РГ ТИО) към Съвета на Европейския съюз, като допринесоха с бележки, коментари и предложения по следните законодателни досиета на ЕС, касаещи защитата на данните, а именно:

1. Предложение за Регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (т.нар. *ePrivacy Regulation*) – работата по което продължава и през 2022 г.;

2. Предложение за Регламент на Европейския парламент и на Съвета относно европейска рамка за управление на данните (т.нар. Акт за управление на данните) – на 30 ноември 2021 г. европейските съзаконодатели в лицето на Съвета и Европейския парламент постигат предварително споразумение по досието. Важно е да се подчертае, че предложените от КЗЛД бележки по него са приети и съответно обективирани в окончателната му редакция;

3. Предложение за Регламент на Европейския парламент и на Съвета за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект) и за изменение на някои законодателни актове на Съюза;

4. Предложение за Регламент на Европейския парламент и на Съвета за изменение на Регламент (ЕС) №910/2014 по отношение на създаването на рамка за европейска цифрова самоличност (*eIDAS*);

5. Предложение за Директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148.

Представители на КЗЛД участват и в подгрупа към Работна група №3 „Право на установяване и свободно предоставяне на услуги“ към СЕВ във връзка с досие 2020/0361 (COD) относно предложение за Регламент на Европейския парламент и на Съвета за Единния пазар за цифрови услуги (Законодателен акт за цифровите услуги) и за изменение на директива 2000/31/ЕО. Българската страна подкрепя възприетия в предложението асиметричен подход, с който се определят специфични правила и задължения, съобразени с различните категории доставчици, вида на предоставяните от тях цифрови услуги и мащаба на тяхната дейност, както и предвиденото разделение на отговорностите в борбата срещу незаконното съдържание онлайн между доставчиците, получателите на услуги и публичните органи. Всички съществени български коментари и предложения са намерили своето отражение в предлаганите компромисни текстове на председателството, като например извоюването на изключение за микро- и малките предприятия от задължението за публикуване на уведомленията за причините за премахване на съдържание, което би представлявало съществена административна тежест за стартиращите и най-малките компании. Българската страна ще продължава да следи за потенциално въздействие на отделните предлагани компромисни разпоредби и търсене на най-благоприятните за българските потребители и предприятия формулировки.

Във връзка с представено на 15.12.2020 г. от Европейската комисия ново законодателно предложение за Регламент на Европейския парламент и на Съвета относно достъпни и справедливи пазари в цифровия сектор (законодателен акт за цифровите пазари) е създадена междуведомствена подгрупа към Работна група №5 „Конкуренция“ към СЕВ за работа по досие 2020/0374 с цитирания по-горе предмет, в работата на която КЗЛД също така участва чрез своите представители в нея. Законодателното предложение е от особена важност за развитието на цифровите пазари както в ЕС, така и в България. В този смисъл България, изразявайки позиции и коментари както по първоначално предложените от ЕК текстове, така и по компромисни текстове на председателството и предложения от отделните делегации, следи за постигане на оптимални за българските потребители, както и за малките и средните предприятия разпоредби, постигане на хармонизирана практика за прилагане с минимални административни тежести за държавите членки, както и за създаване на правна сигурност за целите на стабилно и предвидимо развитие на цифровите пазари в ЕС.

Участието през отчетния период в Работна група към Министерството на финансите относно работата по законодателния пакет на ЕК за мерките срещу изпирането на пари и финансирането на тероризма, което ще продължи и през 2022 г., се свързва с коментари и предложения единствено в рамките на компетентността на надзорния орган, като

експертите се придържат към принципни позиции по повод съответното прилагане на законодателството в областта на защитата на данните. Предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма (*AML/CFT*), от една страна, и защитата на личните данни и личната неприкосновеност, от друга, представляват дейности, които се извършват с цел да се защитят важни обществени интереси, залегнали в правото на Европейския съюз. От гледната точка на надзорен орган по защита на личните данни се застъпват няколко принципни положения при обработването на лични данни за целите на *AML/CFT*, от които не следва да се отстъпва, включително при последващото транспониране на бъдещата Шеста *AML*-директива и въвеждането на мерките за изпълнение на въпросните регламенти.

И през изтеклата 2021 г. се запазва тенденцията за изключително ползотворно сътрудничество между КЗЛД и Инспектората към Висшия съдебен съвет. То се развива както текущо по линия на провеждането на надзорната дейност в областта на защитата на личните данни в национален план, които често налагат съвместен анализ и работа по „гранични“ случаи на компетентност на съответния орган, но и във все по-ефективната работа и съвместното участие в работата на работни групи и комитети към ЕС, включително съобразно обсъждания въпрос, във формати на работни групи на Съвета на ЕС. И през отчетната 2021 г. представители на двете институции продължават участието си в Комитета за координиран надзор към ЕКЗД, създаден в съответствие с чл. 62 от Регламент (ЕС) 2018/1725.

В духа на добро междуинституционално взаимодействие през 2021 г. КРС и КЗЛД издават съвместни Указания по чл. 249, ал. 4 от ЗЕС относно условията, методиката и сроковете за предоставяне на информация между предприятията, предоставящи обществени електронни съобщителни услуги, за наличието на неплатени задължения на крайния ползвател с оглед нововъведената възможност в ЗЕС предприятията, предоставящи обществени електронни съобщителни услуги (наричани по-нататък „Предприятия/та“), да поискат от други предприятия, предоставящи същите услуги, информация относно наличието на неплатени задължения на крайния ползвател към тях, когато при сключване на договор се предоставя и крайно устройство. Указанията са съобразени и с предвидените в ЗЕС права и задължения за предприятията, като същите не водят до разширително тълкуване на неговите норми, което е допълнителна гаранция за правата на субектите на данни. Съвместните указания способстват за гарантиране защитата на крайните ползватели (физически лица) при обработване на личните им данни, което от своя страна ще доведе и до подобряване на правната сигурност и предвидимост в търговския оборот. Указанията са

приети от двата органа и впоследствие обнародвани в Държавен вестник, брой 109 от 21.12.2021 г.

В изпълнение на сключения през 2020 г. договор за сътрудничество между Икономическия университет – Варна (ИУ – Варна), и КЗЛД на 31.03.2021 г. експерти от администрацията на КЗЛД провеждат обучение под формата на „среща-дискусия“ със студенти и преподаватели от катедра „Правни науки“ на ИУ – Варна. Темата на срещата е посветена на „Компетентността на КЗЛД и Инспектората към Висшия съдебен съвет“. Тя е част от обучението по дисциплината „Достъп и защита на информацията“, което предполага теоретична и практическа правна подготовка на студентите от специалност „Съдебна администрация“ с оглед потребността от непрекъснато развиване и усъвършенстване на правните знания в изучаваната материя. В началото на октомври 2021 г. чрез видеоконферентна връзка е проведена кръгла маса на тема „Защитата на личните данни и дигитализацията – предизвикателства и перспективи“. Събитието е организирано съвместно от Научноизследователския институт и катедра „Правни науки“ на Икономически университет – Варна. Във форума участват представители на КЗЛД, на Института за държавата и правото на Българска академия на науките, на академичната общност на Икономическия университет – Варна, и други университети (ВУТП, УНСС, ТУ – Варна, Шуменския университет „Епископ Константин Преславски“), както и представители на юридическата практика (Административен съд Варна). Представителите на КЗЛД изнасят два доклада на тема „Защита на данните по подразбиране и на етапа на проектиране в епохата на дигитализацията“ и „Нарушения на сигурността на данните и дигитализацията“. Кръглата маса поставя на полето на полемиката практическите предизвикателства на най-актуалните аспекти на ефективната защита на личните данни в дигитална среда. Представените доклади провокират интересни и ползотворни дискусии относно предизвикателствата, свързани със защитата на личните данни в дигиталното общество.

В началото на отчетния период в рамките на ползотворното сътрудничество с г-жа Ирина Дунчева – журналист, блогър по въпросите на защитата на личните данни и носител на Грамота за цялостен журналистически принос през 2020 г. за повишаване на информираността в областта на защитата на данните, връчена от КЗЛД, е организирано и проведено обучение за журналисти на тема „Задължения на администраторите и обработващите лични данни“.

През отчетната 2021 година КЗЛД взема участие в поредица от семинари, организирани от адвокатска кантора „Боянов и Ко“, по две много актуални теми в областта на защитата на личните данни за 2021 г.: Обработването на лични данни за ваксинационния

статус от работодателите и Предизвикателствата, свързани с трансферите на лични данни след Решението на Съда на Европейския съюз по т.нар. дело „Шремс 2“ (дело C-311/18 (*Schrems II*) и Препоръки 01/2020 на Европейския комитет по защита на данните за допълнителните мерки по отношение на трансферите, които да осигурят съответствие с европейското ниво на защита на личните данни. Експертите от КЗЛД са отговорили на възникналите казуси вследствие на нарасналия обществен интерес, дали са допълнителни разяснения и насоки по принципни въпроси и са споделили добри практики за постигане на законосъобразно обработване на личните данни в обсъждания контекст.

И през изминалата година, водена от политиката си за партньорство, КЗЛД активно търси и развива партньорства със сродни надзорни органи, академичните среди, бизнеса и неправителствения сектор. Примери за последните са Сдружение „Национална асоциация за защита на потребителите“ и фондация „ЛИБРе“. С последната е изпълнен успешно проект по програмата „Еразъм+“ и се разработват нови проектни предложение от интерес за целевите групи на двете организации. Посредством подготовката на проектни предложения и изпълнението на одобрени за финансиране проекти през 2021 г. КЗЛД е реализирала партньорски отношения по линия на проектната дейност с държавни институции и сродни органи, частни организации, неправителствения сектор и академичните среди от Република България, Гърция, Кипър и Полша.

3. Утвърждаване на фигурата на ДЛЗД.

3.1. Регистър на подадените от АЛД/ОЛД уведомления за ДЛЗД.

Длъжностното лице по защита на данните (ДЛЗД) е нова фигура съгласно Регламент (ЕС) 2016/679. На основание чл. 37 от Регламент (ЕС) 2016/679 АЛД и ОЛД определят ДЛЗД, публикуват данните за контакт с длъжностното лице и ги съобщават на надзорния орган. В чл. 25б от ЗЗЛД това задължение е конкретизирано, като са посочени изискуемите за регистрация данни, а чл. 15, ал. 1, т. 1 от ЗЗЛД постановява воденето на специален публичен регистър – „Регистър за администраторите/обработващите лични данни, определили ДЗЛД“, чрез който данните за контакт с ДЗЛД да бъдат събрани на едно място и да бъдат достъпни за всеки, който има нужда от тази информация.

Данните в регистъра се набират от подадените уведомления чрез попълване на утвърдения образец на Уведомление, публикуван на сайта на КЗЛД и подаден по един от следните начини:

1. Чрез Специализираната автоматизираната информационна система на КЗЛД от сайта на КЗЛД (рубрика „Публични регистри“). За целта АЛД/ОЛД трябва да разполага с

квалифициран електронен подпис, с който се идентифицира в системата и получава достъп за извършване на необходимите операции: въвеждане, коригиране или изтриване на данните от уведомлението.

2. На имейла на КЗЛД – *kzld@cpdp.bg*. В този случай Уведомлението трябва да бъде попълнено и съответният електронен файл да бъде подписан с квалифициран електронен подпис (КЕП).

3. Чрез Системата за сигурно електронно връчване, поддържана от Държавна агенция „Електронно управление“. В този случай Уведомлението трябва да бъде попълнено и съответният електронен файл да бъде изпратен чрез тази система.

4. Лично в деловодството на КЗЛД или по пощата на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров“ №2, Комисия за защита на личните данни. В този случай се подава попълнено, подписано и подпечатано Уведомление на хартиен носител.

В образеца се нанасят данните на АЛД/ОЛД в посочените полета и информацията за ДЛЗД, а така също необходимите данни за контакт с ДЗЛД. В раздел „Публични данни за контакт с ДЗЛД“ се попълват онези канали за комуникация, които АДЛ/ОЛД са преценили за релевантни, и те ще са видими в публичния регистър.

Достъпът до публичния регистър е свободен и всеки може да намери информация за АЛД/ОЛД, определили ДЗЛД, за името на ДЗЛД или за данните за контакт с длъжностното лице.

През отчетния период подадените уведомления от АЛД и ОЛД за определяне на ДЛЗД се диференцират съгласно основанието, както следва:

- обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции (133 от общо подадени уведомления за отчетния период);
- основните дейности на АЛД или ОЛД се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни (154 от общо подадени уведомления за календарната година);
- основните дейности на АЛД или ОЛД се състоят в мащабно обработване на специалните категории данни съгласно чл. 9 и на лични данни, свързани с присъди и нарушения, по чл. 10 от Регламент (ЕС) 2016/679 (31 от общо подадени уведомления за календарната година).

Извън гореизброените хипотези, при които определянето на ДЛЗД е задължително, всеки АЛД или ОЛД може по своя преценка да определи такъв служител. От тази възможност са се възползвали 155 от администраторите, подали уведомления за определяне на ДЛЗД през 2021 г.

Фиг. 14

През 2021 г. до КЗЛД са подали уведомления за определено ДЛЗД 761 АЛД или ОЛД, с което общият брой на подадените уведомления е 6241.

За същия период публикуваните АЛД или ОЛД, определили ДЛЗД в публичния регистър, са 358 бр., с което общият им брой става 5075.

3.2. Пропуски при подаването на уведомления за ДЛЗД и често задавани въпроси.

Въпреки че в приетите и публикувани на страницата на КЗЛЗ „Указания относно изпълнението на задължението на администраторите и обработващите лични данни за уведомяване на КЗЛД при определяне на длъжностно лице по защита на данните“ (пълният текст на указанията е публикуван на сайта на КЗЛД в рубриката „Длъжностно лице по защита на данните“) освен друго е обърнато внимание на изискването на Регламента ДЛЗД да е лице, различно от администратора/обработващия, както и от лицата, които определят целите и средствата за обработването на лични данни при съответния администратор/обработващ, продължава постъпването на уведомления, в които ръководителят (управителят) се е самоопределил за длъжностно лице по защита на данните.

В такива случаи – 171 бр. за 2021 г., Комисията връща писмо с разяснения и указания по преценка да се подаде ново уведомление с коректно посочени данни. Това са близо 30% от общия брой подадени уведомления за периода, което говори за необходимостта от продължаване на действията на КЗЛД за предоставяне на разяснения и указания за постигане на съответствие с изискванията на Регламента във връзка с определянето на ДЗЛД.

Тази продължаваща тенденция на подаване на такива уведомления навежда на извода, че част от администраторите подхождат формално към прилагането на Регламента и бъркат уведомяването за определяне на ДЗЛД със стария и отменен режим на регистрация като администратори на лични данни. В КЗЛД все още пристигат и такива искания – 11 бр., въпреки отмяната на регистрирането на АЛД от 25.05.2018 г., т.е. вече от четири години.

3.3. Необходимост от промяна във възприемането на длъжностното лице по защита на данните.

Анализирайки практиката на КЗЛД при произнасяне по жалби и сигнали през 2021 г., отново се отчита, че както и през миналата година АЛД продължават да не се обръщат към своите ДЛЗД или поне не прилагат становища от същите в производствата пред Комисията. Ролята на ДЛЗД е от изключително значение за правилното разбиране, а оттам и прилагане на Регламент (ЕС) 2016/679 и ЗЗЛД от АЛД/ОЛД и нейното подценяване е сериозен пропуск от страна на последните в това отношение. Самата фигура на ДЛЗД е съществен елемент в правната рамка за защита на личните данни и правилното функциониране на едно ДЛЗД е сигурен знак за задълбоченото разбиране и прилагане на Регламента от АЛД/ОЛД.

В този смисъл КЗЛД ще продължи да следи за реалното функциониране на фигурата на ДЛЗД като важен и принципен момент от действията на един АЛД/ОЛД при изпълнението на задължението за точното прилагане на Регламента. Институционалната и моралната подкрепа, които всеки АЛД/ОЛД следва да оказва за повишаване авторитета и значението на ДЛЗД в своята структура, ще затвърдят професионалната репутация на ДЛЗД и ще накарат самите служители на АЛД/ОЛД да променят отношението и практиката си по неглижиране на функционирането на ДЛЗД, и ще повишат тяхната ангажираност по въпросите, свързани със защитата на личните данни, в ежедневната им дейност.

4. Повишаване на обществената информираност.

4.1. Институционалният сайт на КЗЛД е основен инструмент за реализирането на информационната дейност на КЗЛД. Информационно-разяснителните дейности на КЗЛД са

с постоянен характер и тяхната цел е посланията да достигнат до максимално широк кръг заинтересовани лица – граждани, АЛД/ОЛД, други институции. Информацията на сайта се поддържа тематично, а не по целеви групи, тъй като невинаги е еднозначна целевата група за определена информация. Продължава поддържането на сайта в три езикови версии – на български, английски и френски език.

Утвърдена практика е КЗЛД по достъпен и разбираем начин да разяснява на обществото основните положения от правната рамка в ЕС в областта на личните данни, както и националното законодателство в тази сфера. За тази цел през 2021 г. на сайта се публикуват насоки, указания, разяснения и т.н., като целта е в максимална степен да се обхванат различните категории потребители на тази информация – граждани, администратори, потребители с различна степен на познания и ориентиране в сферата на опазване сигурността на личните данни и гарантиране правата на гражданите.

Поддържат се два основни информационно-разяснителни раздела – „Насоки“ и „Полезна информация“, в които информацията е разделена по тип. В „Насоки“ се публикуват изисквания, указания и насоки, а в „Полезна информация“ – информация с разяснителен характер по актуални теми от висок обществен интерес. През 2021 г. продължава допълването на съдържанието с нови приети насоки и изявления на ЕКЗД, информационно-разяснителни материали по Регламент 2016/679, отпратки към полезни инструменти и приложения, разработени по проекти с участието на КЗЛД. През юни 2021 г. са публикувани съвети към администраторите и обработващите лични данни за защита на данните в киберпространството. През септември 2021 г. са публикувани вътрешни документи относно надзорната дейност на Комисията – Инструкция за практическото осъществяване на надзорната дейност, Методика за оценка на риска и Въпросник за извършване на проверки. През ноември 2021 г. са публикувани указания относно действията на администраторите на лични данни при настъпване на нарушение на сигурността на личните данни.

Във връзка с повишаване на обществената информираност по въпроси в областта на защитата на личните данни в началото на отчетния период са предприети действия по актуализиране на информацията на интернет сайта, предоставяна на администраторите на личните данни и физическите лица, относно международното сътрудничество и Шенгенското пространство. Разясненията по отношение на предаването на лични данни към трети държави и международни организации са изцяло обновени и реорганизирани в самостоятелен информационен раздел „Предаване на данни към трети държави и международни организации“. В този раздел е предоставена информация относно Решенията на Европейската комисия относно адекватното ниво на защита на данните и относно

стандартните договорни клаузи за трансфер на лични данни към трети страни, режима на обработване и трансфер на данни чрез използване на задължителни фирмени правила, други възможности за трансфер на данни, споразуменията за обработване и трансфер на данни на пътниците от авиопревозвачите, програмата за проследяване финансирането на тероризма. С оглед на демонстриране на прозрачност и отчетност всички информационни материали в трите секции са датирани, за да може да се проследяват промените, ако такива настъпят.

Тъй като работата на КЗЛД във връзка с постигането на пълноправно членство на България в Шенгенското пространство е приоритетна задача и през 2021 г., специално внимание е отделено на актуализирането на раздела „Шенгенско пространство“. Акцентът в предоставената информация е върху правната рамка, упражняването на правата на физическите лица и защитата на личните данни в Шенгенската информационна система – ръководства за упражняване на права; информация за данните, които се съдържат в Шенгенската информационна система от второ поколение (ШИС II) и сроковете за тяхното съхранение; контрола при обработването на данните и функционирането на националната част на ШИС (НШИС), образци на искания относно информация в ШИС II. Предоставени са данни за контакт с органи, компетентни за въвеждане, актуализиране и заличаване на националните сигнали в ШИС II. Предоставени са редица допълнителни материали относно Шенгенското пространство, Националната шенгенска информационна система (НШИС) и Национална визова информационна система (НВИС). Публикувани са и 4 информационни брошури – три на Европейската комисия и една на КЗЛД.

През отчетната година е изцяло преработен информационният раздел „Международно сътрудничество“.

И през 2021 г. се поддържа разделът „Новини“, като в него се предоставя актуална информация за събития и инициативи на национално и наднационално ниво. Публикуват се информация и съответни препратки към приети решения, становища, насоки, документи с информационно-разяснителен характер на КЗЛД и на други органи и институции (Европейския комитет по защита на данните, Европейската комисия, Съда на ЕС и др.).

През отчетния период продължава изпълнението на стратегическата цел за усъвършенстване на процеса за откритост и прозрачност, във връзка с което в раздел „Практика“ се отразява практиката на КЗЛД с акцент върху становища от обществен интерес и анонимизирани решения по жалби. Оповестяват се някои решения на КЗЛД, като целта е отразяване произнасянето на Комисията по различни казуси. Публикуват се и решения от съдебната практика на КЗЛД – решения на ВАС и административни съдилища.

През 2021 г. продължава осигуряването на прозрачност относно институцията чрез регулярно и своевременно отразяване на сайта на информация, подлежаща на публикуване

в съответствие със законови изисквания – финансова информация, информация за предоставянето на административни услуги, за осигуряване на достъп до обществена информация, за проектната дейност на КЗЛД и т.н. Осъществена е публичност до 2 регистъра и 1 списък по ЗПКОНПИ, които се поддържат актуални.

В периода януари-май 2021 г. чрез сайта на КЗЛД е проведено онлайн анонимно проучване сред АЛД/ОЛД от публичния сектор. Резултатите от проучването са анализирани и публикувани в брой №6 на Информационния бюлетин на КЗЛД.

4.2. Информационният бюлетин на КЗЛД е друго основно средство за постигане на обществена информираност, който има собствен ISSN 2367-7759. През 2021 г. са издадени шест бюлетина. Бюлетинът се издава в електронен вид на всеки 2 месеца и се публикува на институционалния сайт, с което е достъпен за всеки посетител на сайта. Едновременно с това има възможност за абониране, в резултат на което абонатите получават известие, че поредният брой на бюлетина вече е публикуван, както и съответен линк. По инициатива на КЗЛД в списъка на получателите на информационния бюлетин са включени длъжностни лица по защита на данните, както и съсловни и браншови органи и организации. Предоставена е и възможност за отписване както на абонатите, така и на тези получатели, включени в списъка по инициатива на КЗЛД. Към края на 2021 г. общият брой на получателите на бюлетина е 3830 души, от които 1130 са абонати.

В бюлетина се предоставят материали, отразяващи дейността и инициативите на КЗЛД, заседанията на ЕКЗД, приети от ЕКЗД документи (становища, изявления), решения на Съда на ЕС. Предоставя се информация относно разглеждания на ниво ЕС цялостен пакет документи, свързан със защитата на данните и свободното движение както на лични, така и на нелични данни.

И през 2021 г. в бюлетина се отразяват събития, инициативи и разработки в областта на защитата на личните данни в национален, европейски и световен мащаб. За изминалата година такива материали в национален мащаб са: „КЗЛД публикува указания и разяснения относно определянето на длъжностно лице по защита на данните и последващо уведомяване на Комисията“; „КЗЛД публикува съвети към администраторите и обработващите лични данни за защита на данните в киберпространството“; „КЗЛД одобри формуляр за подаване на уведомление за нарушение на сигурността на личните данни“; „КЗЛД публикува свои вътрешни правила относно извършване на надзорната ѝ дейност“; „КЗЛД проведе обучение на тема „Какво да правим при изтичане на информация?“; „КЗЛД и КРС изготвиха проект на съвместни указания“; „Съвместни указания на ЦИК и КЗЛД относно обработването и защитата на личните данни в изборния процес“; „Участие на

КЗЛД в кръгла маса на тема „Защитата на личните данни и дигитализацията – предизвикателства и перспективи“; „Инструмент за самооценка на малки и средни предприятия за съответствието им с Общия регламент относно защитата на данните“; „Продължава надграждането на мобилното приложение „*GDPR* в твоя джоб“ и др.

В наднационален мащаб такива материали са „Европейската комисия предлага мерки за насърчаване на споделянето на данни и за подкрепа на европейските пространства на данни“; „Предложение на ЕК за създаване на Цифров зелен сертификат“; „Европейската комисия предлага надеждна и сигурна цифрова самоличност за всички европейци“; „Европейската комисия представи нова стратегия за Шенгенското пространство“; „Европейската комисията предлага създаването на съвместно киберзвено за засилване на способността за реагиране в случай на мащабни инциденти по сигурността“; „ЕС се стреми да улеснява обмена на данни: Съветът на ЕС постигна съгласие по позицията си относно Акта за управление на данните“; „Органите за защита на данните и неприкосновеността на страните от Г-7 поеха ангажименти за сътрудничество“ и др.

Публикувани са резюмета на съвместни становища на ЕКЗД и ЕНОЗД.

И през 2021 г. продължава публикуването на решения и становища на КЗЛД, както и обща статистика за контролната дейност. Решения по жалби се публикуват с цел осигуряване на прозрачност за обществеността относно практиката на КЗЛД при разглеждане на жалби. Всички публикувани решения на КЗЛД са с псевдонимизирани лични данни на физическите лица и по-голямата част от имената на юридическите лица. По отношение на контролната дейност през 2021 г. регулярно се оповестява статистика за извършени проверки, разгледани искания, упражнени корективни правомощия на КЗЛД. През 2021 г. почти всеки бюлетин предоставя подробна информация за текущото изпълнение на международни проекти, в които участва КЗЛД.

4.3. През 2021 г. е разработен цялостен обучителен материал *„Действия на администраторите на лични данни при настъпване на нарушение на сигурността на личните данни – чл. 33 и чл. 34 от Регламент (ЕС) 2016/679“*. В него са описани подробно последователността на действия, които следва да се предприемат от АЛД/ОЛД при настъпване на нарушение на сигурността на личните данни; кога се изисква уведомяване на надзорния орган и кога на засегнатите субекти на данни в съответствие с чл. 34 от Регламент (ЕС) 2016/679; какво е минималното съдържание на уведомлението. Разяснено е и какви технически и организационни мерки за минимизиране вероятността от настъпване на нарушение следва да се предприемат, както и какви технически и организационни мерки да се предприемат за преодоляване на последиците от евентуално такова нарушение на

сигурността, както и какво и как следва да се документира от АЛД/ОЛД при нарушение на сигурността на данните. Материалът е достъпен на интернет страницата на Комисията в раздел „Полезна информация“.

От втората половина на 2021 г. на интернет страницата на Комисията е наличен и формуляр за „Уведомление за нарушаване на сигурността на данните на основание чл. 33 от Регламент (ЕС) 2016/679 или на основание чл. 67 от ЗЗЛД“. Използването на същия не е задължително условие, а е по-скоро с препоръчителен характер с оглед избягване на евентуални пропуски от АЛД/ОЛД при подаване до КЗЛД на уведомлението по чл. 33 от Регламента и последващи искания за допълнителна информация от страна на Комисията.

Поради възникналата епидемична обстановка в страната през отчетната година са преустановени всички обучения и мероприятия за повишаване на осведомеността по въпроси в областта на защитата на личните данни, които в предходни години КЗЛД е провеждала на територията на цялата страна. Независимо от това през отчетния период Комисията подготвя и провежда 2 специализирани обучения в областта на защитата на личните данни за журналисти и за студенти. В допълнение през октомври 2021 г. чрез дистанционна платформа с предварително регистрирани участници КЗЛД провежда специализирано онлайн обучение на тема „*Какво да правим при изтичане на информация*“. Изнесени са презентации от експерти на Комисията и са разгледани действията на всички участници в системата за защита на личните данни при настъпване на нарушение на сигурността на данните – администратори, обработващи, КЗЛД, физически лица. В последвалата дискусия от онлайн участниците са зададени множество въпроси с практически казуси, на които са представени подробни разяснения.

В началото на отчетния период по случай Деня за защита на личните данни – 28 януари, КЗЛД обявява станал традиция студентски конкурс за есе на тема „Личните данни и свободата в дигиталното общество“. През 2021 г. конкурсът се организира от катедра „Правни науки“ при Икономическия университет – Варна, и Комисията за защита на личните данни. Той е обявен в изпълнение на Договор за сътрудничество между Икономическия университет – Варна, и КЗЛД. Право на участие е дадено на студенти от този университет. При обявяването на конкурса е посочено, че процесът на обучение в различни специалности на университета провокира различни гледни точки и проекции на възприятия относно социалните, икономическите и обществените модели, взаимовръзки и отношения. Тези различни гледни точки са и чудесен повод за споделяне, среща и провокиране на различен тип творческо мислене.

Конкурсът за есе дава възможност на студентите да представят аргументирано своите разбирания по темата – как възприемат свободата в дигиталния свят и какво е

мястото на защитата на личните данни в този контекст. В рамките на срока за кандидатстване са получени есета на студенти от различни курсове и специалности в университета. На 13 април 2021 г. чрез конферентна връзка е проведена заключителната част на конкурса, на която участниците, класирани на първите три места, представят своите идеи пред конкурсната комисия в рамките на 10 минути с предварително създадена презентация и изложение. Студентските есета са публикувани в сайта на Икономическия университет – Варна, на страницата на катедра „Правни науки“, както и в специален раздел на брой 3 (90) на бюлетина на КЗЛД.

5. Медийна политика и отразяване на събития, свързани с дейността на КЗЛД.

През 2021 г. КЗЛД продължава своята последователна политика по развитие и устойчива позитивна институционална публичност, на прозрачност и откритост при осъществяването на своята дейност, на ползотворно партньорство и взаимодействие с други държавни органи, с представители на гражданското общество и със средствата за масова комуникация.

5.1. Ден за защита на личните данни.

И тази година КЗЛД за 15-и пореден път отбеляза 28 януари – Деня за защита на личните данни, с редица събития и мероприятия. Основната цел на това честване са повишаване на информираността и насърчаване на инициативите и добрите практики за разбиране правата, правилата, рисковете и гаранциите, свързани с обработването и защитата на личните данни.

Датата 28 януари 2021 г. е юбилейна за правото на защита на личните данни. На 28 януари 1981 г., точно преди 40 години, става факт Конвенция 108 на Съвета на Европа за защита на лицата при автоматизирана обработка на лични данни. Конвенцията е първият международен акт за защита на личните данни на физическите лица и въвежда правните принципи и норми, възприети и прилагани и към днешна дата от ЕС и държавите членки. Инициативата за обявяването на 28 януари за Ден за защита на личните данни е на Съвета на Европа, но понастоящем той се отбелязва в редица държави в целия свят, въпреки че е възникнал като „европейски“. През 2018 г. Конвенция 108 е модернизирана с оглед развитието на информационните и комуникационните технологии и предизвикателствата, които възникват пред неприкосновеността.

По повод празника КЗЛД организира в зала „Заседателна“ на КЗЛД традиционната „Приемна за администратори на лични данни и граждани“, в която експерти от администрацията приемат граждани, администратори на лични данни и длъжностни лица

по защита на данните и отговарят на въпросите им, свързани както с прилагането на Закона за защита на личните данни, така и с поставени конкретни казуси.

Председателят на КЗЛД Венцислав Караджов връчва за пета поредна година „Награда за журналистика“ по повод 28 януари – Ден за защита на личните данни. Комисията награждава Ирина Дунчева за най-голям журналистически принос през 2020 г. за популяризиране дейността на КЗЛД и правата на гражданите за неприкосновеност и защита на личните данни. Институцията благодари на Ирина Дунчева за активното, обективно и добронамерено отразяване в блога си на обществено значими теми, свързани както с дейността на КЗЛД, така и относно възможностите за защита на личните данни и информация в европейски и световен мащаб.

Ежегодната „Награда за журналистика“ (грамота и медал на КЗЛД) е учредена на 28 януари 2016 г. и се дава за публикации, предавания и обществено значими прояви на журналист/медия, които са отразявали редовно дейността на институцията през предходната календарна година.

Друго събитие по случай Деня за защита на личните данни е обявяването на станалия традиционен студентски конкурс за есе на тема „Личните данни и свободата в дигиталното общество“. През 2021 г. конкурсът се организира от катедра „Правни науки“ при Икономическия университет – Варна, и Комисията за защита на личните данни. Той е обявен в изпълнение на договор за сътрудничество между Икономическия университет – Варна, и КЗЛД. Право на участие е дадено на студенти от този университет. При обявяването на конкурса е посочено, че процесът на обучение в различни специалности на университета провокира различни гледни точки и проекции на възприятия относно социалните, икономическите и обществените модели, взаимовръзки и отношения. Тези различни гледни точки са и чудесен повод за споделяне, среща и провокиране на различен тип творческо мислене.

Конкурсът за есе дава възможност на студентите да представят аргументирано своите разбирания по темата – как възприемат свободата в дигиталния свят и какво е мястото на защитата на личните данни в този контекст. В рамките на срока за кандидатстване са получени есета на студенти от различни курсове и специалности в университета. На 13 април 2021 г. чрез конферентна връзка е проведена заключителната част на конкурса, на която участниците, класирани на първите три места, представят своите идеи пред конкурсната комисия в рамките на 10 минути с предварително създадени презентация и изложение. Студентските есета са публикувани в сайта на Икономическия университет – Варна, на страницата на катедра „Правни науки“, както и в специален раздел на брой 3 (90) на бюлетина на КЗЛД.

На 28 януари 2021 г. чрез сайта на КЗЛД е предоставен достъп до дигитален Инструмент за самооценка на малки и средни предприятия за съответствието им с Общия регламент относно защитата на данните. Инструментът е разработен по проект *SMEDATA* – „Осигуряване на най-висока степен на защита на неприкосновеността на личния живот и личните данни чрез иновативни инструменти за малки и средни предприятия и граждани“. Инструментът е достъпен от сайта на КЗЛД.

Също по повод на Деня за защита на личните данни е инициирано проучване (анкета), насочено към администраторите на лични данни от частния сектор, като целта е да се получи информация относно готовността им да ползват специфични трудови умения на лица в неравностойно положение, като привлекат в своите екипи лица с такива умения, които да участват при управлението на процесите по обработване на лични данни. Събраната информация е използвана за обосноваване необходимостта от конкретни действия от страна на националния надзорен орган за създаване на възможност за социално включване и кариерно развитие на безработни лица и хора в неравностойно положение чрез индивидуален подход, основан на най-добрите практики за демонстриране на съответствие с правната рамка на ЕС за защита на данните.

Анкетата е проведена в периода между 28 януари 2021 г. и 10 май 2021 г. Целевата група са администратори и обработващи лични данни в частния сектор, тъй като съществуват редица нормативни изисквания пред публичния сектор за наемане на лица със специфични потребности. След анализиране на резултатите от анкетата като основен се налага изводът, че броят на администраторите на лични данни, категоризирани като малки и средни предприятия, които биха наели служител или външен експерт със специфични потребности, примерно намалена трудоспособност, варира между 11 184 и 20 046 предприятия.

В резултат на извършения анализ събраната информация е надградена чрез създаване на профил, описващ „идеалния“ служител, който да подпомага процесите по обработване на личните данни в МСП, както и да участва при демонстриране на съответствие на тези операции по обработване с разпоредбите на Регламент (ЕС) 2016/679. На участниците в изследването е предоставена възможност да споделят своето виждане относно уменията, които следва да притежава служителят/лицето, изпълняващо дейностите, свързани с обработването на лични данни, в съответствие с принципите и правилата на ОРЗД.

5.2. Медийна политика.

КЗЛД продължава успешно реализирането на своята последователна политика по развитие и устойчива позитивна институционална публичност, на прозрачност и откритост в осъществяването на своята дейност.

През годините Комисията изгради добри практики за комуникация с медиите с ясната цел за постигане на единни, ясно установени и съвременни стандарти в медийната комуникация за повишаване на информираността на обществото и осигуряване на публичност и откритост на своята дейност, свързана със защита на личните данни на физическите лица.

През 2021 г. инициативите в посока опазване неприкосновеността на личния живот са подкрепени и чрез поддържането на устойчиви и ползотворни връзки с представители на медиите в страната. Дейността на институцията намира място в множество публикации в печатните медии. Електронните агенции и електронните медии също отразяват редовно дейността на институцията. КЗЛД отговаря на актуални обществени въпроси и интервюта по различни теми през годината в Българската национална телевизия, Българското национално радио, Агенция „Монитор“, в. „Монитор“, предаването „Бизнес старт“ по *Bloomberg TV Bulgaria, Bulgaria ON AIR,* Правен сайт „Де факто“, в. „Сега“, в. „Труд“, и др.

От КЗЛД се предоставя своевременно информация на журналисти по тяхно писмено или устно искане, което води до публикуването на значителен брой информационни материали и журналистически разследвания, които засягат разнообразни аспекти на защитата на личните данни. Чрез постоянната комуникация с медиите и множеството реализирани изяви до населението у нас достига ценна и практична информация, което е част от цялостната политика на институцията към публичност, прозрачност и открит диалог с българското общество.

Поради продължаващата сложна епидемична обстановка през изминалата година постъпват сравнително по-малко искания и запитвания за интервюта по актуални обществени въпроси и различни теми, свързани с дейността на КЗЛД, в сравнение с предходните години. Постъпилите запитвания от журналисти касаят основно постъпилите жалби и сигнали, извършените проверки/одити, издадените АУАН и НП и упражняването на корективните правомощия по чл. 58, §2 от Регламента (ЕС) 2016/679. В осъществените интервюта с председателя на Комисията Венцислав Караджов през отчетния период са обсъдени темите за видеонаблюдение, обработване на лични данни в частния сектор, опазване на личните данни и други.

XI. АДМИНИСТРАТИВЕН КАПАЦИТЕТ И ФИНАНСОВИ РЕСУРСИ

1. Административен капацитет.

Общата численост на персонала към 31.12.2022 г. е 81 щатни бройки. Недостигът на достатъчно финансови и човешки ресурси, които да гарантират адекватно, навременно и качествено изпълнение на надзорните ѝ функции е приоритетен въпрос, за който Комисията предприема действия през 2021 г. чрез обявяването на конкурси и процедури по мобилност за общо 13 свободни позиции. За целия отчетен период са проведени 18 конкурса и процедури за мобилност, като други три конкурса са започнати и неприключени към 31.12.2021 г. За целите на успешното приключване на конкурсите са извършени промени в щатното разписание на КЗЛД, като свободни щатни бройки „старши експерт“ са преобразувани в „младши експерт“. Това решение е довело до интерес на кандидати за позиции, за които не се изисква професионален опит (за разлика от длъжността „старши експерт“), което има за резултат успешно реализиране на множество назначения в администрацията на КЗЛД.

Към 31.12.2021 г. в КЗЛД работят 54 служители по служебно правоотношение и 18 по трудово правоотношение (в това число председателят и членовете на КЗЛД).

През 2021 г. са назначени 11 служители, от които 9 по служебно правоотношение и двама по трудово правоотношение. Един служител е назначен чрез мобилност в държавната администрация по чл. 81а от Закона за държавния служител.

През отчетния период в ранг са повишени 20 служители.

През 2021 г. чрез процедура по мобилност в държавната администрация са напуснали трима служители на КЗЛД.

Поради въведените ограничения и мерки за неразпространение на пандемията от КОВИД-19 през отчетния период не се провеждат обучения за повишаване на административния капацитет на служителите на КЗЛД. Независимо от това по линия на обучения в т.нар. „Лятна академия за млади лидери от държавната администрация“ на Института по публична администрация (ИПА) през 2021 г. двама служители от специализираната администрация на КЗЛД вземат участие в специализиран краткосрочен курс през отчетния период, както и в дискусионен формат за изработване на предложение за съдържание на Стратегията за развитие на държавната администрация след 2021 г.

Представител на администрацията на Комисията е първият запознал експерти от държавната администрация с дейността на КЗЛД в стартиралата през отчетния период инициатива на ИПА за ежемесечни онлайн срещи на вече разрасналата се мрежа на младите лидери в администрацията.

Във връзка с отправена покана от Народното събрание на Република България по повод изпълнението на проект №BG05SFOP001-2.013-0001 с наименование „Повишаване на ефективността при въвеждането на директивите и мерките по прилагането на актовете на Европейския съюз в българските закони“, дейност „Обучения на служителите от администрацията на Народното събрание и от централната администрация, с които да се повишат компетентността и експертизата на администрацията, ангажирана с процеса на въвеждане на директивите и мерките по прилагането на актовете на ЕС в българските закони“, четирима служители на КЗЛД са взели участие в предложените обучения по следните три теми:

1. Преглед и анализ на действащи процедури и правила в НС, свързани с изработването и разглеждането на законопроектите, с които се въвежда право на ЕС. Идентифициране на основни недостатъци;

2. Проверка за съответствието на законите с изискванията на Закона за нормативните актове, Указ №883 за прилагане на ЗНА, Правилника за организацията и дейността на НС, актовете на ЕС, включително Наредбата за обхвата и методологията за извършване на оценка на въздействието и на методологията, приложение към ПОДНС;

3. Практически задачи и тестове, свързани с изработване на законопроекти по време на обучението, анализиране по време на обучението на законопроекти и на приети закони с идентифициране на проблемите чрез конкретни примери за добро и лошо законодателство.

По покана от Дипломатическия институт към министъра на външните работи на Република България по повод изпълнението на проект №BG05SFOP001-2.015-0002 с наименование „Провеждане на специализирани обучения за служители от държавната администрация“ служители на КЗЛД вземат участие в обучения, организирани от Дипломатическия институт към Министерството на външните работи – курс „Публична дипломация“ и курс „Комуникационни и презентационни умения в международна среда“.

Курсът се провежда в рамките на два дни, през които се разглеждат приликите и разликите между конвенционалната и публичната дипломация. Особен акцент в обучението е поставен върху публичната дипломация, осъществявана в ЕС, както и на способите за провеждане на т.нар. „дигитална дипломация“. В резултат на проведения курс взелите участие в него служители от администрацията на КЗЛД са повишили квалификацията и уменията си, нужни при участието им в различни формати на експертни работни групи както на национално, така и на европейско равнище.

2. Административно обслужване.

В изпълнение на изискванията на Наредбата за административното обслужване потребителите на административните услуги осъществяват контакт с КЗЛД чрез Звеното за административно обслужване. Дейността по административно обслужване се осъществява при пълно изпълнение на Вътрешните правила за административното обслужване и Хартата на клиента, които имат за цел повишаване качеството на административните услуги, насърчаване участието на гражданите и служителите при обсъждане на услугите, начина им на предоставяне, необходимото качество и стандартите за изпълнение. Дейността на Звеното за административно обслужване се осъществява от четирима служители в условия на непрекъсваем работен процес в рамките на работния ден.

През отчетния период служителите от Звеното за административно обслужване са обработили общо 19 601 бр. документи – писма, молби, заявления, жалби, вътрешни документи и др., от и към граждани, администратори и държавни институции. Системата за документооборот обработва всички документи, постъпили в Звеното за административно обслужване, като със създадените правила за сканиране на вход и изход прозрачността в работата на администрацията е абсолютно гарантирана.

За измерване удовлетвореността на потребителите през отчетния период са отчетени преобладаващата част от задължителните методи за обратна връзка съгласно изискванията на чл. 24, ал. 2 и ал. 3 от Наредбата за административното обслужване, а именно: извършване на анкетни проучвания; провеждане на консултации със служителите; анализ на сигнали, предложения, жалби и похвали; анализ на медийни публикации.

Изключително малка част от потребителите на административни услуги проявяват активност да дават целенасочена оценка на предоставяното от КЗЛД административно обслужване въпреки обстоятелството, че достъпът до средствата за обратна връзка е свободен. Независимо от това въз основа на информацията от преките впечатления на служителите, ангажирани с административното обслужване, и от служителите, които на ротационен принцип обслужват телефона за устни експертни консултации по законодателството за защита на данните и за бързи справки по постъпили жалби, сигнали и въпроси, може да се направи извод, че КЗЛД спазва всички изисквания за законосъобразно, добросъвестно и безпристрастно административно обслужване.

Анализът на КЗЛД показва, че повод за изразяване на недоволство от работата на институцията от страна на съответните външни заинтересовани лица са сроковете за разглеждане на подадените от тях жалби и сигнали. Макар и единични случаи, основните оплаквания са свързани изцяло с времетраенето на производствата пред КЗЛД, които понякога (в случаите на сложна фактическа и правна обстановка) продължават повече от

година – година и половина. Причините за това забавяне са от обективен характер и са предимно от външно естество: завишен брой сезирания на КЗЛД, усложнена и тромава процедура по АПК по отношение на редовното връчване на книжа на страните в административните производства, отказ от съдействие на КЗЛД при събиране на доказателства (в т.ч. при осъществяване на проверки на място), необходимост от съдействие на други органи за служебно събиране на доказателства.

Друг повод за недоволство е физическата невъзможност на експертите, които дават устни консултации по Регламент (ЕС) 2016/679 по телефон, да приемат всички телефонни обаждания. В допълнение през отчетния период поради извършване на строителни работи в района на сградата на КЗЛД (изграждане на улица) периодично настъпват аварийни ситуации – спиране на електрозахранване, прекъсване на комуникационни кабели и т.н. В резултат на това възникват затруднения в комуникациите с институцията – стационарни телефони, електронна поща, институционален сайт, достъп до електронни услуги. Невъзможността за осъществяване на консултации по телефон или контакт с институцията в такива случаи е провокирала допълнително напрежение у гражданите и администраторите, тъй като телефонът е най-бързият и предпочитан от тях начин на комуникация с надзорния орган.

КЗЛД нееднократно е имала възможност да посочи, че след стартиране прилагането на новата правна рамка по защита на данните (считано от 25 май 2018 г.) обемът от работа се е увеличил многократно. Засиленото текучество на персонал през целия мандат на настоящия състав на КЗЛД – особено осезаема тенденция след 25 май 2018 г., е друг много сериозен негативен фактор, който също оказва влияние върху срочността на изпълняваните дейности. Изключително сериозната натовареност на администрацията на Комисията очаквано води и до забавяне в сроковете за разглеждане и приключване на отделните административни преписки поради физическа невъзможност за тяхното навременно отработване.

3. Анализ на постъпилите в КЗЛД заявления за достъп до обществена информация и искания за повторно използване на информация.

В качеството си на задължен субект по ЗДОИ информация, на сайта на КЗЛД се поддържа раздел „Достъп до информация“, в който е включена нормативно изискуемата информация, както следва;

– Процедура по разглеждане на заявленията за достъп до обществена информация и предоставяне на информация за повторно използване;

– Описание на звеното за приемане на заявления за предоставяне на достъп до обществена информация и информация за повторно ползване;

– Разходи за предоставяне на достъп до обществена информация и информация за повторно ползване;

– Ред за достъп до публичните регистри на КЗЛД;

– Описание на информационните масиви и ресурси, използвани в администрацията на КЗЛД;

– Списък на издадените актове и текстове на издадените нормативни и общи административни актове;

– Списък на категориите информация, подлежаща на публикуване в интернет, както и форматите, в които е достъпна;

– Годишен отчет за постъпилите заявления за достъп до обществена информация и за повторно ползване на информация от обществения сектор, който включва и данни за направените откази и причините за това.

В таблицата по-долу е представена обобщена информация относно постъпили и разгледани заявления за достъп до обществена информация през 2021 г.

Общ брой постъпили заявления за достъп до обществена информация:	28
- От граждани на Република България	26
- От чужденци	0
- От медии	1
- От НПО	1
- От частноправни субекти	0
Общ брой решения по заявления за предоставяне на достъп до обществена информация:	16
- Предоставяне на пълен достъп до обществена информация	14
- Предоставяне на частичен достъп до обществена информация	1
- Предоставяне на достъп при надделяващ обществен интерес	0
- Отказ за предоставяне на достъп до обществена информация	1
Уведомление за липса на исканата обществена информация	0
Препращане на заявлението, когато КЗЛД не разполага с исканата информация, но знае за нейното местонахождение	3
Предоставяне на информация по реда на административното обслужване или по реда на АПК	8
Заявления, които не отговарят на чл. 25 във вр. с чл. 2, ал. 1 от ЗДОИ	0

Общ брой на постъпили искания за предоставяне на информация за повторно ползване	1

На всички граждани и организации, заявили достъп до обществена информация, е предоставена такава през 2021 г. в законовия срок. С едно изключение с всички решения е предоставен пълен достъп до обществена информация. Решението за предоставяне на частичен достъп е взето във връзка със заявление за предоставяне на цялата административнонаказателна преписка за налагане на имуществена санкция на НАП за нарушение на чл. 32, §1, б. „б“ от Регламент (ЕС) 2016/679. На заявителя е предоставена само информацията, която притежава характеристиките на обществена такава, без да се предоставят копия от самите писмени доказателства, събрани в хода на административнонаказателното производство, въз основа на които е наложено и съответното административно наказание.

Решението за отказ от достъп до обществена информация е взето във връзка със заявление за предоставяне на информация от административни актове на КЗЛД, като при разглеждането му информацията е определена като такава, която не попада в обхвата на чл. 2, ал. 1 от ЗДОИ. Комисията е счела, че изисканата информация е свързана с надзорната дейност на административния орган, т.е. информацията е служебна, по конкретен казус, не е с обществен характер, а засяга частни интереси. Срещу Решението за отказ обаче е постъпила жалба в АССГ, като решението на съда е за връщане на преписката в КЗЛД за ново произнасяне. След като взема предвид съдебното решение, КЗЛД се произнася с ново Решение за достъп до обществена информация, като в този случай вече е предоставен пълен достъп до исканата информация при стриктно спазване на указанията на съда.

С оглед предмета на заявленията за достъп до обществена информация същите се отнасят до: достъп до изготвените и приети правила, уреждащи достъп до материали по преписките, съответно реда за получаване на копие от документи, съгласно чл. 87, ал. 4 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация; достъп до резултатите от проведената анкета, насочена към длъжностните лица по защита на данните в публичния сектор; достъп до регистъра на администраторите и обработващите лични данни, които са определили лица за защита на данните, който се поддържа от КЗЛД на основание чл. 15, ал. 1 от ЗЗЛД; броя на проведените конкурси за служители в КЗЛД и подадени жалби за нарушения на конкурсната процедура; списък на категориите информация, подлежаща на публикуване в интернет, както и форматите, в които тази информация е достъпна. Постановените откази за предоставяне на информация

са свързани с обстоятелството, че исканата информация не притежава характеристиките на обществена информация по смисъла на чл. 2, ал. 1 от ЗДОИ.

4. Състояние на внедрените информационни и комуникационни системи в КЗЛД през 2021 г.

През отчетния период чрез Системата за управление на документи и работни потоци в КЗЛД и контрол на решенията в синхрон със Системата за електронен документооборот и Системата за сигурно електронно връчване е осигурена бърза и надеждна кореспонденция както между държавните органи, така и между всички участници в нея (физически и юридически лица). Това води както до по-качествено обслужване на гражданите, така и до значително намаляване на документите на хартиен носител и ускоряване на информационните потоци.

През 2021 г. са извършени редица дейности за подобряване информационната и комуникационната инфраструктура на КЗЛД, както следва:

– закупени са 10 броя нови компютърни конфигурации;

– закупени са 5 броя нови преносими компютри;

– закупени са два броя *UPS*;

– закупени са 2 броя сървъри;

– закупени са 6 броя *access switch*;

– закупени са 20 броя многофункционални устройства – принтер/скенер.

Чрез тези мерки КЗЛД е осигурила възможността за създаване на организация за работа на служителите ѝ от разстояние в домашна среда и провеждане на заседанията на Комисията, вкл. от разстояние при необходимост, с цел ограничаване на разпространението на *КОВИД-19* при спазване на изискванията на чл. 6а, ал. 1 от Закона за мерките и действията по време на извънредното положение.

Своевременно са подновени договорите за поддръжка на информационните системи, критични за дейностите и процесите в КЗЛД. Доставка и инсталиране на сървърни и персонални сертификати се извършват регулярно съгласно сроковете им за подновяване.

Профилактиката и ремонтът на техническите средства се извършват в максимално къси срокове съгласно утвърдените процедури.

През отчетния период КЗЛД е продължила сътрудничеството си с Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи“, която отговаря за *GovCERT Bulgaria* (Национален център за действия при инциденти по отношение на информационната сигурност).

5. Обществени поръчки.

За обезпечаване на дейността на КЗЛД през 2021 г. са възложени обществени поръчки, както следва:

5.1. Чрез публично състезание:

– „Доставка и инсталация на мрежово оборудване за обезпечаване на информационната инфраструктура на КЗЛД“.

5.2**.** Чрез събиране на оферти с обява:

– Извършване на денонощна физическа охрана на сградата, в която се помещават администрациите на Комисията за защита на личните данни и Института по отбрана „Проф. Цветан Лазаров“, и на паркинга пред нея;

– „Доставка на горива и аксесоари за автомобилите, собственост на Комисията за защита на личните данни, чрез зареждане с карти за безналично плащане“.

6. Финансови ресурси – обща информация относно разходването на бюджета на КЗЛД през 2021 г.

Със Закона за държавния бюджет на Република България (ЗДБРБ) за 2021 г. е утвърден бюджетът за дейността на КЗЛД в размер на **3 220 500 лв.** През годината по него са извършени корекции, както следва:

– намаление на разходите за издръжка общо с 49 800 лв. в изпълнение на разпоредбите на ПМС №113/29.03.2021 г. и ПМС №177/29.04.2021 г. за одобряване на допълнителни разходи и трансфери по бюджета на Министерството на здравеопазването за 2021 г. за сметка на разходи и/или трансфери по бюджетите на първостепенните разпоредители с бюджет за 2021 г.;

– намаление на разходите за персонал с 45 000 лв. в изпълнение на разпоредбите на ПМС №474/30.12.2021 г. за осигуряване на допълнителен трансфер по бюджета на Държавното обществено осигуряване за 2021 г. за сметка на икономии на утвърдените разходи и/или трансфери по бюджетите на други първостепенни разпоредители с бюджет по държавния бюджет за 2021 г.;

– увеличение на разходите за издръжка с 1286 лв. в изпълнение на разпоредбите на ПМС №154/15.04.2021 г. за одобряване на допълнителни разходи/трансфери за 2021 г. по бюджета на КЗЛД на база фактически извършени разходи за графически експертизи на подписи, възлагани по чл. 49 от АПК.

След извършените промени утвърденият бюджет на КЗЛД за 2021 г. е в размер на **3 126 986 лв.**

За обезпечаване на дейността на Комисията за защита на личните данни и нейната администрация са извършени разходи общо в размер на **3 100 781 лв.**, или **99,16%** от утвърдените разчети за годината. Видовете разходи, отразени по параграфи от ЕБК, са представени в таблицата, както следва:

Параграф	**Наименование на разходите**	**Сума (лева)**
01-00	Заплати и възнаграждения за персонала, нает по трудови и служебни правоотношения	1 764 780
02-00	Други възнаграждения и плащания за персонала	71 616
05-00	Задължителни осигурителни вноски от работодатели	435 296
10-00	Издръжка	643 682
19-00	Платени данъци, такси и административни санкции	12 489
52-00	Придобиване на дълготрайни материални активи	165 394
53-00	Придобиване на нематериални дълготрайни активи	7524
	Общо разходи по бюджета	**3 100 781**

XII. ЦЕЛИ И ПРИОРИТЕТИ НА КЗЛД ЗА 2022 г.

1. Отбелязване на 20-ата годишнина от създаването на Комисията за защита на личните данни.

2022 г. е юбилейна за Комисията за защита на личните данни. През януари се навършват 20 години от влизането в сила на Закона за защита на личните данни (01.01.2002 г.), а през май – 20 години от създаването на КЗЛД (23.05.2002 г.). По повод тази двойна годишнина Комисията планира серия от мероприятия, чието провеждане да бъде разпределено равномерно и поетапно през цялата година. Като отчита, че провеждането на публичните събития е в зависимост от епидемичната обстановка през годината и действащите противоепидемични мерки, Комисията има амбицията да сподели 20 години добри практики с основните групи участници в националната система за защита на личните данни:

– към физическите лица (субекти на данни);

– към администраторите и обработващите лични данни;

– към длъжностните лица по защита на данните.

2. Приемане на нова Стратегия на КЗЛД за развитие в областта на защитата на личните данни.

През 2022 г. е необходимо да бъдат извършени преглед и анализ на изпълнението на стратегическите цели за периода 2017 – 2022 г., залегнали в „**Стратегията на КЗЛД – Хоризонт 2022**“, с оглед изготвяне на нова стратегия за следващия 5-годишен период – **2023 – 2028 г.** Целесъобразно е новите стратегически цели да отчетат натрупания вече 20-годишен опит в прилагането на изискванията за защита на личните данни, 4-годишната практика по Регламент (ЕС) 2016/679, съвременните тенденции и предизвикателства пред защитата на личните данни и непрекъснато променящата се нормативна среда.

3. Финализиране на подзаконовата правна уредба в областта на защитата на личните данни и изпълнение на правомощия, произтичащи от националното законодателство.

Натрупаният почти 4-годишен опит в прилагането на новите завишени изисквания в областта на защитата на личните данни вече позволява да бъде финализиран качествено процесът по изграждане на националната подзаконова правна уредба в тази област. През отчетната 2021 г. надзорният орган е приел проект на изисквания за акредитация на органите за наблюдение на кодексите за поведение и проект на критерии за акредитиране

на сертифициращи органи. В съответствие с посочения в чл. 63 от ОРЗД механизъм за съгласуваност проектоизискванията следва да бъдат представени през 2022 г. на ЕКЗД за становище. След отразяване на получените становища КЗЛД ще пристъпи към изготвяне на проектите на наредби по чл. 14, ал. 5 и чл. 14а, ал. 3 от ЗЗЛД, които следва да уредят процедурите по акредитиране в национален план. По този начин ще бъде даден старт на ефективното прилагане на доброволните инструменти за отчетност, каквито са кодексите за поведение и сертифицирането, интерес към които проявяват множество администратори на лични данни още от началото на прилагането на Регламент (ЕС) 2016/679 през 2018 г.

В допълнение Комисията е амбицирана да намери подходяща реализация на своето правомощие да провежда сертифицирани обучения в областта на защитата на личните данни в изпълнение на чл. 16 от Закона за защита на личните данни. Интересът на администраторите и обработващите към такава обучителна дейност, особено за нуждите на длъжностните лица по защита на данните, респ. лицата, определени за изпълнение на тези функции, е много голям и е заявен още от началото на прилагането на Регламент (ЕС) 2016/679. КЗЛД, считано от 2019 г., когато влизат в сила измененията и допълненията в ЗЗЛД, регулярно е поставяла пред Министерството на финансите въпроса за необходимостта от допълнително финансиране за целите на обучение в областта на защитата на личните данни (или с цел реконструкция и вътрешно преустройство на сградата, предвидена за обучителен център, или с цел разработване и въвеждане на електронна платформа за дистанционни обучения), но до този момент не е получила нужната подкрепа. Комисията счита, че вече близо четири години след започване прилагането на новата правна рамка за защита на данните е крайно наложително отпускането на необходимото финансиране за стартиране на постоянна обучителна дейност. Прибягването до алтернативни методи за повишаване на знанията в сферата на защитата на личните данни (основно под формата на семинари, превод и публикуване на информационни материали на интернет страницата на КЗЛД, изготвяне и разпространение на тематични брошури) е важна превантивна дейност, но тя не може да компенсира липсата на пълноценно организирано обучение за администраторите, обработващите и техните длъжностни лица по защита на данните.

4. Изводи от анализите на съвременните заплахи и предизвикателства.

Комисията ще продължи активно да следи тенденциите за развитие на предизвикателствата, свързани с развитието на изкуствения интелект и новите технологии за лицево разпознаване, големите бази данни и свързаната с тях възможност за профилиране, както и защитата на децата и младите хора в дигиталното пространство.

Провеждането на мултидисциплинарни обучения за нуждите на КЗЛД и на нейната администрация е важна предпоставка за качественото изпълнение на тази цел и в следващия отчетен период. Бурното развитие на технологиите налага да се постави акцент върху обученията в областта на киберсигурността. Провеждането на специализирани тематични семинари ще гарантира както навременно повишаване на осведомеността на надзорния орган и неговите служители, така и ще позволи вземането на правилни решения относно фокуса на контролната дейност. По-конкретно, по линия на съвременните предизвикателства през 2022 г. КЗЛД планира да:

- насочи своята превантивна дейност към участието в събития, които да насърчат обмяната на експертни знания и опит, свързани с тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване, както и наблюдение на процеса по правното регулиране на изкуствения интелект като едно от най-големите предизвикателства днес;
- подготви информационно-образователни материали и добри практики на база натрупания опит от своята надзорна дейност във връзка със случаи на неоторизиран достъп, неразрешено разкриване и разпространение на лични данни на ФЛ от големи информационни масиви. Предмет на такива разяснителни материали би могло да бъде съставянето на примерен списък с добри практики при избора и внедряването на подходящи технически и организационни мерки за защита на данните по начин, който гарантира едновременно сигурността на данните и спазването на принципа на отчетност по чл. 5, пар. 2 от Регламента;
- засили контролната си дейност под формата на секторни анализи и/или секторни проверки на администратори и обработващи, чието обработване е насочено към деца. Специфичен акцент ще бъде поставен върху обработването на лични данни на деца, структурирани в големи информационни масиви, както и при пряко предлагане на услуги на информационното общество към тази уязвима категория субекти на данни.

Изводите от извършените анализи на съвременните заплахи и предизвикателства ще бъдат отчетени при изготвянето на новата Стратегия на КЗЛД за развитие в областта на защитата на личните данни.

Следваща стъпка в този процес, естествено продължение на започналия през 2021 г. преглед на законодателството за съответствието му с правилата за защита на личните данни, е активното включване на КЗЛД в нормотворческия процес с цел навременно предвиждане и идентифициране на верните от гледна точка на защитата на личните данни законодателни решения. Проактивност по линия на законодателния процес е необходима не само за отчитане на съвременните предизвикателства в глобален аспект, но и във връзка с

установени празноти и пропуски в националната правна уредба, имащи отношение към обработването и защитата на личните данни, като напр. видеонаблюдението. КЗЛД счита за наложително да инициира дискусия с компетентните държавни институции с цел намиране на разумен подход за законодателно уреждане на обществените отношения, свързани с осъществяването на видеонаблюдение в преследване на легитимни цели като охрана на живота, здравето и собствеността, когато това видеонаблюдение засяга физически лица. Комисията може да способства този процес и чрез разработването на предвидените в чл. 25д от ЗЗЛД насоки към администраторите и обработващите при извършване на мащабно обработване на лични данни или систематично мащабно наблюдение на публичнодостъпни зони, включително чрез видеонаблюдение.

Водена от желанието си да даде насоки и примери за добри практики, в приоритетите на КЗЛД за следващия отчетен период е издаването на информационно-образователни брошури по темите – обект на нейния анализ през 2021 г. Повишаването на информираността на гражданите и администраторите по тези въпроси е включено като елемент от цялостната концепция за отбелязване на 20-ата годишнина на институцията.

5. Продължаване на усилията на КЗЛД за пълноправно членство в Шенген.

Тази задача продължава да бъде актуална и с постоянен характер в дейността на КЗЛД и за следващия отчетен период. Подготовката на надзорния орган за евентуална последваща проверка на готовността на страната ни за пълноправно членство в Шенген, що се отнася до изпълнение на изискванията в областта на защитата на личните данни, ще бъде от първостепенна важност за 2022 г.

КЗЛД ще продължи тенденцията си за участие на нейни представители в мисии за оценки на шенгенското законодателство в областта на защитата на личните данни в други държави членки, за да утвърди вече изградения авторитет на българските експерти в тази област.

Годишният отчет на Комисията за защита на личните данни за дейността ѝ през 2021 г. е приет с решение на Комисията на заседание, проведено на 09.03.2021 г. (Протокол № 10).

ПРЕДСЕДАТЕЛ: **ЧЛЕНОВЕ:**

Венцислав Караджов **Мария Матева**

Веселин Целков