Комисия за Защита на Личните Данни

ИНФОРМАЦИОНЕН БЮЛЕТИН

Брой 6 (93), ноември 2021 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода септември и октомври 2021 г.)

КЗЛД ПУБЛИКУВА СВОИ ВЪТРЕШНИ ПРАВИЛА ОТНОСНО ИЗВЪРШВАНЕ НА НАДЗОРНАТА Ѝ ДЕЙНОСТ

Поради засилен обществен интерес, през септември 2021 г. Комисията за защита на личните данни публикува на институционалния си сайт свои вътрешни правила относно извършване на надзорната ѝ дейност – „**Инструкцията за практическото осъществяване на надзорната дейност на КЗЛД**“ и две приложения към нея – „**Методика за определяне на нивото на риска при нарушения на сигурността на личните данни**“ и „**Въпросник за извършване на проверки при осъществяване на надзорната дейност на КЗЛД**“. Комисията информира администраторите на лични данни и обработващите данни, че трите документа са публикувани на сайта на КЗЛД в раздел „Полезна информация“, подраздел „Надзорна дейност на КЗЛД“ - **ТУК**.

Инструкцията е вътрешен документ, приет на основание чл. 12, ал. 10 от Закона за защита на личните данни с решение на КЗЛД от 29.05.2020 г.(Протокол № 23/2020 г.), изм. и доп. с решение от 24.06.2021 г. (Протокол № 27/2021 г.). Като установява методологията за извършване на различни видове проверки (секторни, съвместни проверки с други надзорни органи, предварителна консултация и др.), инструкцията има за цел да създаде унифицирани правила и единен подход при осъществяване на надзорната дейност от страна на КЗЛД и нейната администрация.

Методиката е важен инструмент в дейността на надзорния орган при разглеждане на уведомления за нарушения на сигурността на личните данни, подадени на основание чл. 33 от Регламент (ЕС) 2016/679, респ. чл. 67 от Закона за защита на личните данни. В зависимост от преценката на нивото на риска, Комисията взема решения за последващи действия и комуникация с администратора, засегнат от нарушението (вж. Глава Четвърта, Раздел VII от Правилника за дейността на КЗЛД и на нейната администрация).

Целта на **Въпросника** за извършване на проверки при осъществяване на надзорната дейност на КЗЛД е събирането на предварителна информация, която да изясни контекста на обработването на лични данни и да улесни установяването на факти и обстоятелства, относими към предмета на конкретната проверка. Въпросникът се изпраща предварително на вниманието на всеки администратор – обект на проверка.

С публикуването на Инструкцията и приложенията към нея Комисията цели да повиши информираността по въпросите, свързани с осъществяването на нейните надзорни правомощия, като допринася за последователното прилагане на Регламент (ЕС) 2016/679 и Закона за защита на личните данни. Комисията обаче обръща внимание, че тези документи са изцяло с вътрешен характер и не създават права или задължения за администраторите на лични данни, обработващите данни и субектите на данни. (Не)познаването на съдържанието на публикуваните документи и/или (не)прилагането им в дейността на даден администратор/обработващ лични данни е ирелевантно за констатациите на надзорния орган относно наличието или липсата на съответствие с изискванията в областта на защитата на личните данни и не може да се счита за смекчаващо или отегчаващо вината обстоятелство в конкретен случай.

При разработването на документите Комисията е отчела натрупания национален и чуждестранен опит в областта на контролната дейност, насоките на Европейския комитет по защита на данните, правната уредба в областта на защитата на личните данни и минималните изисквания за мрежова и информационна сигурност. Инструкцията за практическото осъществяване на надзорната дейност на Комисията за защита на личните данни и приложенията към нея подлежат на периодична актуализация с цел отчитане на натрупаните добри практики в национален и европейски мащаб и съобразяване с динамиката на обществените отношения-предмет на надзор.

КЗЛД ПРОВЕДЕ ОБУЧЕНИЕ НА ТЕМА "КАКВО ДА ПРАВИМ ПРИ ИЗТИЧАНЕ НА ИНФОРМАЦИЯ?"

На 14-ти октомври 2021 г. се проведе онлайн обучение на тема „Какво да правим при изтичане на информация?", организирано от Асоциация на индустриалния капитал в България и CTeam Group. Чрез дистанционна платформа присъстваха предварително регистрирани участници, по-голямата част от които представители на частния бизнес.

Лектори на обучението бяха представители на Комисията за защита на личните данни – председателят Венцислав Караджов, членът на Комисията Цанко Цолов и служители от дирекция „Правно-аналитична, информационна и контролна дейност". Целта на обучението бе да бъдат разгледани действията на всички участници в системата за защита на личните данни при настъпване на нарушение на сигурността на данните – администратори, обработващи, надзорен орган (КЗЛД), физически лица.

Организирането, координирането и провеждането на обучения в областта на защитата на личните данни е едно от основните правомощия и задължения на КЗЛД. Такива се осъществяват както на териториален, така и на секторен принцип и се съобразяват с конкретни интереси и проблеми на аудиторията.

Председателят на КЗЛД, Венцислав Караджов откри семинара, като представи приоритетите на КЗЛД във връзка със защитата на личните данни и по-специално – тези, свързани с нарушенията на сигурността.

На участниците бе разяснено какво се разбира под „сигурност на обработването на личните данни", **кога има нарушение на сигурността и какви са видовете нарушения**. Обобщена бе последователността на действия, които следва да се предприемат от АЛД при настъпване на нарушение на сигурността на личните данни. Обяснено бе защо уведомяването по чл.33 от Регламент (ЕС) 2016/679 трябва да разглежда като важен инструмент за засилване на спазването на заложените в Регламента изисквания за защита на личните данни. Разгледани бяха **условията, изискващи уведомяване на надзорния орган** при констатиране на нарушение на сигурността на личните данни, както и задълженията на администраторите, обработващите и съвместните администратори. В отделна презентация бяха разгледани **условията, изискващи уведомяване на засегнатите субекти на данни**, в съответствие с чл. 34 от Регламент (ЕС) 2016/679, който регламентира условията, при които се налага или допуска уведомяване на субектите на личните данни при нарушаване на сигурността. Посочени бяха формата и минималното съдържание на уведомлението за субектите на лични данни, засегнати от нарушението. Обърнато внимание на обстоятелството, че правилното поведение на АЛД е отваряне на информацията към засегнатите субекти, тъй като информираното физическо лице може също да предприеме мерки, които да допълнят вече взетите от АЛД такива.

Разгледани бяха **технически и организационни мерки** за минимизиране вероятността от настъпване на нарушение, както и мерки, които следва да се предприемат при настъпване на нарушение на сигурността на данните.

На семинара **бе представен приетият от КЗЛД формуляр на Уведомление за нарушаване на сигурността на данните** на основание чл. 33 от Регламент (ЕС) 2016/679 или на основание чл. 67 от ЗЗЛД. Попълването му не е задължително, но е препоръчително, с оглед избягване на последващи искания за допълнителна информация, както и унифициране на уведомленията, пристигащи в КЗЛД. Формулярът е публикуван на институционалния сайт.

Оценката на риска, който възниква в резултат от настъпило нарушение на сигурността, е важен фактор по отношение на последващите действия както на администратора, така и на КЗЛД. В две отделни презентации бяха разгледани темите за **оценка на риска, извършвана от администратора**, и **оценка на риска, извършвана от КЗЛД** при получаване на уведомление за настъпило нарушение.

Участниците в обучението бяха запознати с **методиката на КЗЛД за оценка на риска**, която е вътрешен документ, подпомагащ обработването на постъпващите в КЗЛД уведомления за нарушения на сигурността. Посочено бе, че правилната оценка на риска е от съществено значение за по-нататъшните действия на КЗЛД във връзка с обработването на едно уведомление.

Разгледан бе въпросът за **документиране на всяко нарушение на сигурността на личните данни**, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него. Всеки администратор трябва да разполага с планове и процедури за реакция при евентуални нарушения на сигурността на данните, докладване и отговорни лица в процеса на възстановяване.

Участниците в обучението бяха запознати с **административния** процес в КЗЛД, протичащ при получаване на уведомление за нарушение на сигурността - процедурата по неговото обработване, инструментите, които се ползват, как се взима решение, какви са последствията. Посочени бяха основните стъпки на процесът по обработване на уведомление – регистрация, служебно събиране на допълнителна информация (напр. проверка за наличие на жалби и сигнали, свързани с конкретното нарушение), изискване на допълнителна информация от АЛД при необходимост, преценка за допустимост, оценка на риска и в зависимост от нея предприемане на по-нататъшни действия, решение на КЗЛД за налагане на корективни мерки.

След като в рамките на 10 презентации бяха изяснени основните понятия, действащите лица и техните задължения при констатирано нарушение на сигурността на данните, в отделен панел **бяха разгледани казуси** за различен тип нарушения, действия на администратора, изпращане на уведомление за настъпило нарушение и действия на надзорния орган след оценка на риска върху субектите на данни. На участниците в семинара бе дадена думата за задаване на въпроси, при което съответно бяха предоставени компетентни разяснения.

УЧАСТИЕ НА КЗЛД В КРЪГЛА МАСА НА ТЕМА "ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ДИГИТАЛИЗАЦИЯТА - ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ"

В началото на октомври 2021 г. чрез видеоконферентна връзка се проведе кръгла маса на тема „Защитата на личните данни и дигитализацията – предизвикателства и перспективи". Събитието бе организирано съвместно от Научноизследователски институт и катедра „Правни науки" на Икономически университет – Варна. Във форума се включиха представители на Комисията за защита на личните данни, на Института за държавата и правото на Българска академия на науките, на академичната общност на Икономически университет – Варна и други университети (ВУТП, УНСС, ТУ-Варна, Шуменски университет „Епископ Константин Преславски"), както и представители на юридическата практика (Административен съд – Варна).

Председателят на КЗЛД Венцислав Караджов изнесе доклад на тема „Защита на данните по подразбиране и на етапа на проектиране в епохата на дигитализацията". В своя доклад той посочи, че с въвеждането на изцяло новата правна рамка за защита на данните на ниво Европейски съюз, бяха приети Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) и Директива (ЕС) 2016/680, които въвеждат изискването за защита на личните данни на етапа на проектирането и по подразбиране.

В своя доклад г-н Караджов подчерта, че защитата на данните на етапа на проектирането вменява задължението за включване на елемента за поверителност на данните през целия инженерен процес по разработване на

дигитален продукт, т.е. защитата на данните следва да е концептуално заложен елемент в момента на разработване, а не нещо добавяно като допълнителна стойност при вече разработен и/или приключил дизайн на продукт. Г-н Караджов посочи седемте „фундаментални принципа“ за защита на данните на етапа на проектирането в рамките на Регламент (ЕС) 2016/679:

- Проактивен, а не реактивен подход (превенция, а не последващо саниране);
- Настройката за поверителност да е зададена като „default“;
- Вграждане на поверителността в самия дизайн;
- Пълна функционалност – positive-sum, not zero-sum;
- Сигурност от край до край – пълен цикъл на защита;
- Видимост и прозрачност;
- Фокус към потребителя с уважение към поверителността му.

Относно защитата на данните по подразбиране г-н Караджов посочи, че това представлява принцип, според който администратор на лични данни обработва само данни, които са изрично необходими за всяка отделна цел, за която се обработват без намесата на ползвателя на съответната технология. Едновременно с това администраторът следва да отговаря за въвеждането на такива настройки и опции по подразбиране, които да позволяват само обработване, което е строго необходимо за постигане на определената законосъобразна цел. Особено съществен елемент при защитата по подразбиране е достъпността на данните и в частност – контролът на достъпа до тези данни през цялото време на обработване.

Венцислав Караджов, който е и заместник председател на Европейския комитет по защита на данните, насочи аудиторията към един изключително полезен за администраторите на лични данни инструмент относно спазването на изискванията на защита на данните на етапа на проектирането и по подразбиране - Насоки № 4/2019 относно член 25 – “Защита на данните на етапа на проектирането и по подразбиране” на Европейския комитет по защита на данните, приети на 20 октомври 2020 г.

Друг докладчик на форума и представител на администрацията на КЗЛД бе Христо Аламинов – началник на отдел „Международно сътрудничество и управление на проекти“ в дирекция „Правно-нормативна и международна дейност“. Неговият доклад, озаглавен **„Нарушения на сигурността на данните и дигитализацията“** представи общ преглед на значението и ползите от изследване на нарушенията на сигурността на личните данни в контекста на дигитализацията. Посочено бе, че независимо от крайно отрицателните последици, които нарушенията на сигурността имат, както за физическите лица, чиито данни са засегнати, така и за администраторите/ обработващите лични данни, те са ценен източник на информация. Докладчикът подчерта, че независимо от това кой от елементите на дигитализацията се изследва, може да се открият условия за нарушения на сигурността на данните. Тези предпоставки трябва да се анализират и да се въведат подходящи технически и организационни мерки за защита. Г-н Аламинов разгледа значението на уведомлението за нарушение на сигурността на данните, което намира място в Регламент (ЕС) 2016/679. С времето данните от уведомленията започват да се обобщават, а Европейският комитет по защита на данните, подпомаган от експерти от националните надзорни органи, издава насоки, препоръки и най-добри практики по отношение на обстоятелствата, при които нарушение на сигурността на личните данни има вероятност да доведе до висок риск за правата и свободите на физическите лица. Този процес демонстрира значението, което уведомяването за нарушенията на сигурността на данните има, като спомага за предотвратяване на бъдещи нарушения на разпоредбите на Общия регламент, благодарение на използването на нарушенията на сигурността на данните като източник на информация. Докладчикът насочи аудиторията към един практически пример в тази посока - Насоки 01/2021 на ЕКЗД относно примери, свързани с уведомлението за нарушение на сигурността на данните.

Кръглата маса постави на полето на полемиката практическите предизвикателства на най-актуалните аспекти на ефективната защита на личните данни в дигитална среда. Представените доклади провокираха интересни и ползотворни дискусии относно предизвикателствата, свързани със защитата на личните данни в дигиталното общество.

АНАЛИЗИРАНИ СА РЕЗУЛТАТИТЕ ОТ ПРОВЕДЕНО ПРОУЧВАНЕ НА КЗЛД

В началото на 2021 г,, по повод Деня за защита на личните данни – 28 януари, КЗЛД стартира анкета, насочена към администраторите на лични данни от частния сектор. Целта на анкетата беше да се събере информация относно готовността на администраторите и обработващите лични данни да привлекат в своите екипи (да се доверят на) лица със специфични трудови умения, които да участват при управлението на процесите по обработване на лични данни. Събраната информация ще бъде 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 се проведе в периода между 28 януари 2021 г. и 10 май 2021 г. Целевата група бе администратори и обработващи лични данни в частния сектор, тъй като съществуват редица нормативните изисквания пред публичния сектор за наемане на лица със специфични потребности.

След анализиране на резултатите от анкетата, като основен се наложи 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 бе 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 бе 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.

Резултатите от проведеното проучване са обобщени в доклад, приет на заседание на КЗЛД на 13 октомври 2021 г. В съответствие с решение на КЗЛД докладът е публикуван в настоящия бюлетин, в раздел „**Доклади**“.

СЪСТОЯХА СЕ ДВЕ СЪБИТИЯ ЗА РАЗПРОСТРАНЕНИЕ НА РЕЗУЛТАТИ ОТ ИЗПЪЛНЕНИЕ НА ПРОЕКТ ПО ПРОГРАМА “ЕРАЗЪМ +”

На 25 и 27 октомври 2021 г. се състояха две събития за разпространение на резултати от изпълнението на **проект „AI-Trans: Increasing AI Transparency Through Digital Alternative Learning of Privacy Training”**. Домакин бе Софийският университет „Св. Климент Охридски“, който е партньор на Комисията за защита на личните данни при изпълнението на проекта.

Проектът AI Trans има за цел да започне дискусия върху темата за личната информация в общества и икономики, в които изкуственият интелект намира все по-широко приложение. Екипът предлага систематизиран преглед на уязвими сектори и типични рискове, както и на европейски инициативи за въвеждане на регулация като необходима защита на основни човешки права и свободи.

Двете събития протекоха под заглавие „**Обществени предизвикателства при защита на личните данни в използването на технологии, базирани на изкуствения интелект**“. В съвременното ежедневие хората използват **десетки видове електронни устройства** (телефони, таблети, „умни гривни“, часовници, играчки, домакински уреди и много други), които са снабдени със сензори и програми и **обменят данни през интернет**. Често това е огромен масив чувствителна информация, която става достъпна на „трети страни“, чийто основен бизнес се гради върху търговската експлоатация на този невидим масив. Това е един дълбоко потопен айсберг с неясни измерения, който носи големи рискове и поставя сериозни етични въпроси. Системите, които съхраняват данни могат да бъдат обект на злоумишлен взлом. Изтичане на информация е възможно също така в резултат от грешки. Това прави възможна злоупотребата от страна на недобросъвестни търговци, правителства, корпорации или други „агенти“ с достъп. Освен това, информационните масиви правят възможна работата на мощни изчислителни машини, изградени от множество изкуствени невронни слоеве. На такива машини днес все повече са поверени важни решения, засягащи различни аспекти от живота на човека. Това е сериозна дилема между **ползите и вредите от овластяването на „мислещата машина“.**

Фокусът на състоялите се две събития бе използването на технологии, базирани на изкуствения интелект, като проблем за защитата на личните данни. Теми на презентациите бяха „Проектът AI Trans и европейската регулация за защита на личните данни. За проекта AI Trans“, „Изкуственият интелект и личната информация: сектори на въздействие и типове рискове“, „Медицински и фитнес устройства за носене: възможности и заплахи“, „Социални мрежи и търсачки – изкуствен интелект и рискове, свързани с употребата на личните данни“, „Изкуствен интелект или защо „умните“ машини не могат да заменят човека в образованието“. Лектори на двете събития бяха представители на Комисията за защита на личните данни, фондация „Либре“ и Софийски университет „Св. Климент Охридски“.

ПРОДЪЛЖАВА НАДГРАЖДАНЕТО НА МОБИЛНОТО ПРИЛОЖЕНИЕ “GDPR В ТВОЯ ДЖОБ”

Продължава надграждането, както на съдържанието, така и на функционалностите на мобилното приложение „GDPR в твоя джоб“. Съдържанието му е обогатено с националното законодателство за защита на личните данни на Франция и Германия (на федерално ниво), като същевременно приложението „говори“ на пет езика със своите потребители.

От началото на месец октомври 2021 г. ползвателите на приложението могат да избират между български, английски, немски, френски и италиански език, за да достъпят „Правната библиотека“, „GDPR речник“, „Ръководството за граждани“, както и „Ръководството за МСП“.

Приложението „GDPR в твоя джоб” има за цел да представи GDPR на гражданите и малките и средните предприятия по лесен за използване и разбиране начин и да им даде практически знания и съвети относно техните права и задължения в областта на защитата на личните данни. Последната версия на софтуера може да бъде свободно изтеглена от магазините за приложения **Google Play** и **App Store**. От пускането на бета версията на приложението през септември 2019 г. досега, се наблюдава значителен интерес – изтеглено е от над 5 900 пъти.

Приложението е разработено в рамките на проект SMEDATA. Надграждането му продължава в изпълнение на проект SMEDATA II. Проектът SMEDATA II е съфинансиран от Европейската комисия по Програма „Права, равенство и гражданство 2014 – 2020“ на Европейския съюз и се координира от КЗЛД и се осъществява в партньорство с АПИС Европа, Съюзът на юристите в България, адвокатско дружество „Ърнст и Янг България“, българския клон на Европейската асоциация на жените юристи и Римския университет „Рома Тре“.

Проект „SMEDATA II: 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” е финансиран по програма „Права, равенство и гражданство” на Европейския съюз с номер на договор 101005747 – SMEDATA II – REC-AG-2020 / REC-RDAT-TRAI-AG-2020.

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

ЗА ПОРЕДНА ГОДИНА БЕ ОТБЕЛЯЗАН ЕВРОПЕЙСКИЯТ МЕСЕЦ НА КИБЕРСИГУРНОСТТА

И тази година, за девети пореден път, месец октомври бе отбелязан като Европейски месец на киберсигурността (*European Cyber Security Month – ECSM*). Ежегодната информационна кампания стартира за първи път през 2012 г. и е част от усилията за повишаване на осведомеността сред гражданите, бизнеса и организациите относно киберсигурността. Координира се от Агенцията на Европейския съюз за киберсигурност (ENISA) и се подпомага от Европейската комисия, държавите-членки на ЕС, Европол, Европейската централна банка, държавите от Европейската асоциация за свободна търговия (ЕАСТ) и над 300 партньори от публичния и частния сектор.

На национално ниво в България отбелязването на Европейския месец на киберсигурността се координира от Държавна агенция „Електронно управление“ (ДАЕУ), а традиционни партньори са Столична община и Главна дирекция „Борба с организираната престъпност“. За първа година, с цел посланията да достигнат до по-широк кръг граждани, ДАЕУ привлече популярни личности, които да подпомогнат каузата за изграждане на здравословни навици в областта на киберсигурността и на достъпен език да допринесат за повишаване на осведомеността относно рисковете за киберсигурността, както и да споделят актуални начини за смекчаването на тези рискове.

На 1-ви октомври бе даден официален старт на инициативите от календара на предвидените за 2021 г. събития. По този повод, председателят на ДАЕУ, който е и национален координатор по киберсигурност, Красимир Симонски заяви: „В ежедневието си сме все по-зависими от цифровите технологии, а пандемията от COVID-19 ускори цифровизацията и подчерта значението на киберсигурността. .... Сега повече от всякога осведомеността в областта на цифровата сигурност е от ключово значение, за да могат гражданите да идентифицират рисковете и да реагират ефективно на киберзаплахите.“

Две теми бяха фокус на кампанията за 2021 г. - **„Киберсигурност у дома“** и **„Първа помощ“**

„Киберсигурност у дома“ включва съвети за сигурност в кибер пространството при извършването на онлайн трансакции, комуникиране, работа или обучение онлайн. Предоставени бяха съвети за добра киберхигиена при ежедневните онлайн дейности.

„Първа помощ“ дава съвети за това какво да се прави ако вече сме станали жертва на киберинцидент - за това как да се реагира в случай на измама при пазаруване онлайн, компрометиране на кредитна карта и/или банкова сметка и хакерска атака на профил в социалните медии. Предвидено бе под формата на интервюта и видеоматериали да бъдат разказани истинските истории на хора, станали жертва на киберинциденти.

Теми на онлайн срещите, проведени на национално ниво бяха „Образование и кариерно развитие в Киберсигурността“„„IT общност за граждански контрол и независимо участие на експерти“„„Що е то етичен хакер и има ли почва у нас? - демонстрации на хакерски техники на живо“„„Киберсигурност в малките и средни предприятия (МСП) - анализ от емпирично изследване на киберсигурността в МСП в България“, „Киберсигурност в общините – мерки, политики и добри практики”.

Европейският месец на киберсигурността е една от инициативите, в които ENISA подпомага държавите-членки в техните усилия за повишаване на осведомеността относно киберсигурността и насърчаване на образованието за киберсигурност в ЕС. Всяка година през целия месец октомври в Европа се провеждат стотици дейности, включително конференции, семинари, обучения, уебинари, презентации, онлайн тестове и други, за да се предоставят ресурси на гражданите да научат повече за защитата си онлайн.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ

През месеците септември и октомври 2021 г. се състояха три дистанционни заседания на Европейския комитет по защита на данните. На състоялото се на **14-ти септември 2021 г.** заседание бе предоставена информация и се състоя дискусия относно подготовката на Проект за Насоки относно взаимодействието между член 3 и глава V от ОРЗД. Възложено бе изготвяне на изявление от името на ЕКЗД относно пакета от законодателните предложения за цифрови пазари и услуги (Digital Services Act и Digital Markets Act) и стратегията на ЕС за данните (Data Governance Act), както да се организира текущо изследване на актуалното развитие по темата, свързана с употребата на мобилни приложения, инсталирани на smart устройства, което да доведе до обобщаване на модел за одит на мобилни приложения.

Във връзка с представените от Facebook умни очила Ray-Ban Stories бяха изразени притеснения относно значително увеличените възможности и функции за заснемане на обществени места на физически лица без тяхно знание. Представен бе напредъкът по започналите две разследвания на китайската платформа за кратки видеа TikTok. Представени бяха резултатите от проведената кръгла маса за защита на личните данни, част от срещата на Групата на седемте (Г-7), както и обмена на информация между надзорните органи в състава на ЕКЗД.

Бяха обсъдени и множество жалби от страна на австрийската правозащитна организация NYOB.

На следващото заседание, състояло се на **24-ти септември 2021 г.** бе обсъден мандат за сътрудничеството между органите по защита на данните за разглеждане на жалбите, подадени от NOYB в различни държави-членки на ЕС.

Фокус на състоялото се на 24-ти септември заседание бе обсъждането и приемането на **Становище на ЕКЗД относно проекта на решение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватното ниво на защита на личните данни от страна на Южна Корея.** Във връзка с приетото Становище, на 27 септември ЕКЗД публикува и прессъобщение, в което заявява:

„ЕКЗД прие становището си по проекта на решение на Европейската комисия относно адекватното ниво на защита на данните за Република Корея. Комитетът се съсредоточи върху общите аспекти на ОРЗД и достъпа на публичните органи до лични данни, предавани от Европейското икономическо пространство (ЕИП) на Република Корея за целите на правоприлагането и националната сигурност, включително правните средства за защита, с които разполагат физическите лица в ЕИП. ЕКЗД оцени също така ефективността на предпазните мерки предвидени в корейското законодателство.

Председателят на ЕКЗД Андреа Йелинек заяви: „Това решение относно адекватното ниво на защита е от първостепенно значение, тъй като ще обхваща предаването на данни както в публичния, така и в частния сектор. Високото равнище на защита на данните е от съществено значение за поддържане на нашите дългогодишни връзки с Южна Корея и за защита на правата, и свободите на физическите лица. Въпреки че подчертаваме, че основните аспекти на корейската рамка за защита на данните по същество са еквивалентни на тези на Европейския съюз, призоваваме Комисията допълнително да изясни някои въпроси и да следи отблизо положението.“

Относно общата рамка за защита на данните ЕКЗД отбелязва, че съществуват ключови области от уредбата на Южна Корея за защита на данните, които следва да бъдат приведени в съответствие с разпоредбите на ЕС като, например:

- понятия за защита на данните (напр. лична информация; обработване, субект на данни);
- основания за законосъобразно обработване за легитимни цели;
- ограничение на целите;
- запазване на данни, сигурност и поверителност; и
- прозрачност.

ЕКЗД приветства усилията, положени от Европейската комисия и от корейските органи, за да се гарантира, че Република Корея осигурява ниво на защита на данните, което по същество е равностойно на предвиденото в ОРЗД. Например приемането от органа за защита на данните в Южна Корея на уведомления, които имат за цел да запълнят пропуските между ОРЗД и националната рамка за защита на данните, например за осигуряване на допълнителната защита, предоставена с уведомление № 2021-1.

ЕКЗД приканва Европейската комисия да предостави допълнителна информация относно обвързващия характер, изпълнимостта и валидността на уведомление № 2021-1 и препоръчва внимателно наблюдение на практическото приложение.

По отношение на **достъпа на публичните органи до данните, предавани на Република Корея**, ЕКЗД отбелязва, че разпоредбите на Закона за защита на личната информация (ЗЗЛИ) се прилагат без ограничения в областта на правоприлагането. ЕКЗД отбелязва също, че обработването на данни в областта на националната сигурност е предмет на по-ограничен набор от разпоредби, залегнали в ЗЗЛИ, въпреки че заложените основните принципи, както и основните гаранции за правата на субектите на данни, и разпоредбите относно надзора, правоприлагането и средствата за правна защита, се прилагат по отношение на достъпа, и използването на лични данни от органите за национална сигурност. В конституцията на Южна Корея също така са залегнали основни принципи за защита на данните, които са приложими по отношение на достъпа до лични данни от страна на публичните органи в областта на правоприлагането и националната сигурност. Освен това, ЕКЗД е съгласен със заключението на Комисията, че може да се счита, че Южна Корея разполага с независима и ефективна система за надзор.

Накрая, що се отнася до ефективните мерки и правото на правна защита, ЕКЗД отправя искане към Комисията да изясни съществените и/или процедурните изисквания, например тежестта на

доказване, на които подлежи жалбата до Комисията за защита на личната информация или всеки иск пред съд, както и дали физическите лица на ЕС биха били в състояние да изпълнят това предварително условие.

За своята оценка ЕКЗД използва Референтен документ относно адекватно ниво на защита съгласно ОРЗД и Препоръки 2/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, както и съществуващата съдебна практика на Съда на ЕС и на Европейския съд по правата на човека относно достъпа на публичните органи."

На своето заседание през **октомври 2021 г.** ЕКЗД прие окончателния вариант, след проведена обществена консултация, на Насоките за ограничаване на правата на субектите на данни съгласно чл. 23 от Регламент 2016/679. Те имат за цел да напомнят за условията, при които следва да се използват тези ограничения от държавите-членки или законодателя на ЕС, като се вземат предвид Хартата на основните права и ОРЗД. Насоките предоставят задълбочен анализ на критериите за прилагане на ограничения, оценките, с които трябва да се съобразяват, начините, по които субектите на данни могат да упражнят правата си след премахването на ограниченията и последиците от нарушенията на чл. 23 от Регламента. Освен това в приетия документ се анализира, как законодателните мерки, с които се въвеждат ограниченията, трябва да отговарят на изискването за предвидимост и се разглеждат основанията за ограниченията, изброени в чл. 23(1) от Регламента, както и задълженията и правата, които могат да бъдат ограничени.

СЪВЕТЪТ НА ЕС ПОСТИГНА СЪГЛАСИЕ ПО ПОЗИЦИЯТА СИ ОТНОСНО АКТА ЗА УПРАВЛЕНИЕ НА ДАННИТЕ

Европейският съюз работи усилено за укрепване на различни механизми за обмен на данни, като целта е да се насърчи наличността на данни, които могат да се използват за реализиране на приложения и новаторски решения в областта на изкуствения интелект, персонализираната медицина, зелената мобилност, умното производство и много други области.

На 01.10.2021 г. държавите членки постигнаха съгласие по мандат за водене на преговори по **предложение за регламент относно европейска рамка за управление на данните (Акт за управление на данните).** Стремежът е да се създадат стабилни механизми за улесняване на повторното използване на определени категории защитени данни от обществения сектор, да се повиши доверието в посредническите услуги за данни и да се насърчи алтруизма по отношение на данните в ЕС.

В публикуваното същия ден прессъобщение се заявява:

„Актът за управление на данните е част от по-широка политика, която дава на ЕС конкурентно предимство във все повече основаната на данни икономика.

Насърчаване на повторната употреба на данни от обществения сектор

С Акта за управление на данните ще се създаде механизъм, който ще позволи безопасното повторно използване на определени категории данни от обществения сектор, които са предмет на **права на други лица**. Това включва например данни, защитени от права върху интелектуална собственост, търговски тайни и лични данни. Органите от обществения сектор, позволяващи този вид повторно използване, ще трябва да бъдат технически оборудвани, за да гарантират, че неприкосновеността на личния живот и поверителността са напълно запазени.

В това отношение Актът за управление на данните ще допълни Директивата за отворените данни от 2019 г., която не обхваща тези видове данни.

За да се избегне създаването на скъпо струващи задължения за публичния сектор, позицията

на Съвета въвежда по-голяма гъвкавост в текста и отчита националните особености, които вече съществуват в някои държави членки.

Създаване на нов бизнес модел за посредничество в областта на данните

С предложението се създава рамка за насърчаване на нов бизнес модел – посреднически услуги за данни – с цел гарантиране на сигурна среда в помощ на дружествата или физическите лица при обмена на данни.

За **дружествата** тези услуги могат да бъдат под формата на цифрови платформи, които да подкрепят доброволното споделяне на данни между дружествата или да улесняват законно установените задължения за обмен на данни. Чрез използването на тези услуги дружествата ще могат да споделят своите данни без страх от злоупотреба или загуба на конкурентно предимство.

По отношение на **личните данни** тези доставчици ще помогнат на физическите лица да упражняват правата си съгласно Общия регламент за защита на данните (ОРЗД). Това ще даде възможност на хората да упражняват пълен контрол върху данните си и ще им позволи да ги споделят с дружества, на които имат доверие. Това може да се постигне например чрез нови инструменти за управление на личната информация, като пространства за лични данни или портфейли от данни, които са приложения за посредничество с други лица въз основа на съгласие.

Доставчиците на посреднически услуги за данни ще трябва да бъдат вписани в регистър, така че клиентите им да знаят, че могат да разчитат на тях.

Доставчиците на услуги няма да имат право да използват споделени данни за други цели. Те няма да могат да се възползват от данните, например като ги продават. Доставчиците обаче могат да начисляват такси за транзакциите.

В позицията на Съвета е изяснен обхватът на тези разпоредби, по-специално за да се посочи по-ясно кои видове дружества могат да бъдат посредници на данни.

Насърчаване на алтруизма по отношение на данните

Предложението също така улеснява физическите лица и дружествата да **предоставят доброволно данни за общото благо**, като например конкретен научноизследователски проект. Субектите, които желаят да събират данни за цели от общ интерес въз основа на алтруизъм по отношение на данните, могат да поискат да бъдат регистрирани в национален регистър на признатите организации за алтруистично споделяне на данни. Регистрираните организации ще бъдат признати в целия ЕС. Това ще създаде необходимото доверие в алтруизма по отношение на данните, насърчавайки физическите лица и дружествата да „дарят“ данни на такива организации, така че те да могат да се използват за по-широки обществени ползи.

В текста на Съвета се добавя изискването за спазване на кодекс за поведение като условие за регистрация като призната организация за алтруистично споделяне на данни. Такива кодекси за поведение следва да се разработят в сътрудничество с организациите за алтруистично споделяне на данни и съответните заинтересовани страни и да се приемат от Комисията чрез актове за изпълнение.

Европейски комитет за иновации в областта на данните

Ще бъде създадена нова структура – Европейски комитет за иновации в областта на данните, който наред с други задачи ще консултира и подпомага Комисията за подобряване на оперативната съвместимост на посредническите услуги за данни и за осигуряване на последователна практика при обработването на искания за данни от публичния сектор. Съветът въведе някои подобрения в задачите и структурата на комитета.

Международен достъп и прехвърляне на нелични данни

С предложението се създават гаранции за данните от обществения сектор, посредническите услуги за данни и организациите за алтруистично споделяне на данни срещу незаконно международно прехвърляне или правителствен достъп до нелични данни. По отношение на личните данни ЕС вече разполага с подобни гаранции съгласно ОРЗД.

Основната промяна, въведена от Съвета, е, че Комисията – чрез акт за изпълнение – може да приема образци на договорни клаузи в подкрепа на органите от публичния сектор и повторните ползватели в случай на прехвърляне на данни от публичния сектор на трети държави.“

Мандатът бе одобрен от Комитета на постоянните представители на Съвета. Това ще даде възможност на председателството на Съвета на ЕС да започне преговори с Европейския парламент. Съветът и Европейският парламент трябва постигнат съгласие по окончателния текст на Акта за управление на данните. Съгласно текста на Съвета новите правила ще започнат да се прилагат 18 месеца след влизането в сила на регламента (вместо 12 месеца, както беше предложено от Комисията).

ОРГАНИТЕ ЗА ЗАЩИТА НА ДАННИТЕ И ПОВЕРИТЕЛНОСТТА НА Г-7 ЗАЯВИХА СВОИТЕ АНГАЖИМЕНТИ ЗА СЪТРУДНИЧЕСТВО

През септември 2021 г. под председателството на Службата на британския комисар по информацията (ICO) на кръгла маса се събраха органите за защита на личните данни и неприкосновеността от страните от Г-7[1], както и гости от Организацията за икономическо сътрудничество и развитие (ОИСР) и Световния икономически форум (СЕФ). Срещата бе тясно свързана с „Пътна карта за сътрудничество за свободен поток на данни и доверие“, обявена от министрите на цифровите технологии и технологиите на Г-7 на 28 април 2021 г. Дискутирани бяха възникващи предизвикателства, които налагат по-тясно международно сътрудничество и бе постигнато съгласие относно ангажиментите за сътрудничество в определени области. Това бе дискусия в контекста на нарастващата глобална икономика, базирана на данни, и промените, наложени от продължаващата пандемия. Публикувано бе комюнике с договорените ангажименти, в което се посочва, че в основата на този бърз растеж е технологичното развитие, позволяващо богатство от иновации, базирани на данни. Това налага органите за защита на личните данни и неприкосновеността да стават все по-ефективни в предвиждането, тълкуването и влиянието на този напредък в начина на използване на данните. За да се изгради доверие, основано на високите стандарти за защита на данните, се налага международно регулаторно сътрудничество, тъй като потоците от данни преминават през границите и дигиталният бизнес достига до клиентите в световен мащаб.

В публикуваното комюнике се заявява, че като регулатори за защита на личните данни и поверителност на най-напредналите цифрови икономики в света, органите за защита на данните от страните на Г-7 приемат, че могат да играят водеща роля в дискусиите по тези въпроси и да помогнат за повлияване на приемането на високи стандарти за защита на данните в световен мащаб.

---

1 Office of the Privacy Commissioner (Canada)
Commission Nationale de l'Informatique et des Libertés (France)
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI (Germany)
Garante per la Protezione dei Dati Personali (Italy)
Personal Information Protection Commission, (Japan)
Information Commissioner's Office (UK)
Federal Trade Commission (United States of America)

Обсъдени бяха редица конкретни ключови въпроси, по които може да се споделят опит и експертиза и да се проучат възможностите за по-тясно сътрудничество между органите за защита на данните и неприкосновеността.

В последователността на дискутирането им, темите бяха:

1. Пресечна точка на поверителност и конкуренция – сътрудничество между регулаторите в подкрепа на стабилна глобална цифрова икономика. Посочена бе необходимостта от засилване на сътрудничеството между органите за защита на данните и поверителността на Г- 7 по отношение на регулирането на цифровите пазари, както и по-голямо сътрудничество между органите за защита на данните и регулаторите на конкуренцията в глобалните форуми и мрежи за поверителност и конкуренция.

2. Бъдеще на онлайн проследяването. Обсъдено бе започването на стратегически диалог между органите за защита на данните и поверителността на Г -7 и технологичните фирми, стандартизиращите органи, дизайнерите, уеб разработчиците, потребителите и гражданското общество, за да се проучи ролята, която технологичното развитие може да играе за създаването на по-ориентиран към поверителността интернет, поддържането и запазването на принципа на информирано и смислено предварително съгласие онлайн. Подчертана бе необходимостта от по-широки усилия за подобряване на стандартите за защита на данните от уебсайтовете, включително чрез споделяне на опит и добри практики.

3. Проектиране на изкуствен интелект в съответствие със защитата на данните. Споделено бе убеждението за централната роля, която органите за защита на данните и поверителността трябва да играят в бъдещото управление на изкуствения интелект, както и за създаването на диалог между органите относно принципите, които трябва да регулират отговорното развитие на изкуствения интелект. Подчертана бе необходимостта от обмен на експертни знания относно нови приложения на изкуствения интелект и произтичащите от тях последици за поверителността.

4. Редизайн на средствата за защита в цифровата ера. Споделяне на информация и опит за това кои регулаторни средства за защита работят най-добре в конкретни ситуации, както и застъпничество пред законодателите за гарантиране, че регулаторните средства за защита са в крак с технологичните промени и поддържат достатъчен паритет между различните юрисдикции.

5. Технологични иновации породени от пандемията - стрес тест за правата на защита на данните. Подчертано бе, че е необходимо проактивно да се демонстрира ангажираност и способност, когато е необходимо да се реагира бързо, като едновременно с това се гарантират високи стандарти за защита на личните данни. Органите трябва да се застъпват за иновации, които ефективно отговарят на обществените нужди и защитават личния живот на гражданите, в крак с развитието на нови технологии, продукти и бизнес модели. Разпространението на нови технологии, свързани с пандемията, следва да е в съответствие с правото за поверителност и защита на данните.

6. Достъп на държавните органи до лични данни и поток от данни на международно ниво: Каква е ролята на регулаторното сътрудничество за осигуряване на истинско доверие? Във връзка с тази тема бе призовано да бъдат ангажирани съответните държавни органи да подкрепят напредващите инициативи на международно ниво (включително на Глобалната асамблея за поверителност (GPA), Съвета на Европа, G20 и по-специално работата на ОИСР по достъпа на държавните органи до лични данни, притежавани от частния сектор), които предлагат ключова възможност за предоставяне на съгласувани принципи, които могат да управляват тази важна тема. Необходимо е да се споделят съответните развития в законодателството и практиката между органите за защита на данните и поверителността на G7 и да се координират вътрешните усилия за насърчаване на принципите, приложими относно достъпа на държавните органи до лични данни. Необходимо е развиване на конструктивни и подходящи отношения с други съответни вътрешни надзорни органи в страните, за да се осигури съгласуван подход към поверителността и защитата на данните в контекста на достъп на държавните органи до лични данни.

7. Разработване на рамка за трансграничен трансфер на лични данни и сътрудничество между органите за защита на данните на G7.

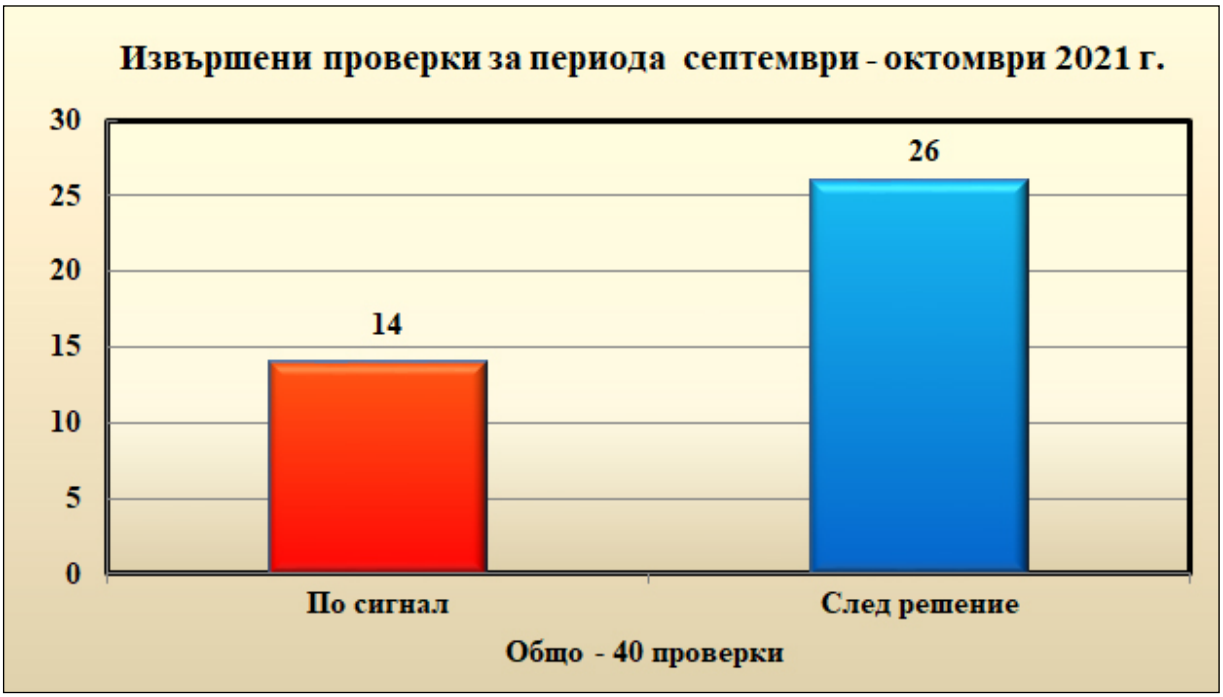
Подчертана бе необходимостта от насърчаване на по-открит и чест диалог между органите за защита на данните и поверителността на G7, изграден върху споделени мрежи, редовни срещи и текущи дискусии. Трябва да се осъществява обмен на опит и практики в управлението на нововъзникващи технологии и иновации, с цел насърчаване на оперативно съвместими регулаторни подходи между органите за защита на данните и поверителността на Г -7. Следва да се дефинират възможностите за по-голямо сътрудничество в областта на правоприлагането между органите за защита на данните и поверителността на G7, като се започне с развиването на споделено разбиране за правните рамки и практиките за правоприлагане в рамките на юрисдикциите, включително относно обхвата на тяхното национално прилагане.

Участниците в срещата поеха ангажимента да подкрепят договорените резултати и да помогнат за изграждането на тясна мрежа от експерти в различните органи на Г-7. Чрез този нов форум комисарите на Г-7 създадоха гъвкава среда, в която могат да обсъждат въпроси от взаимен интерес и да се стремят да създадат по-дългосрочни отношения, глас и влияние с международни организации и други ключови международни заинтересовани страни, за да популяризират своите споделени ценности и цели.

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА СЕПТЕМВРИ - ОКТОМВРИ 2021 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците септември и октомври 2021 г. са извършени общо 40 проверки – 14 след постъпили в КЗЛД сигнали и 26 след решение на КЗЛД.



Разгледани са 99 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

Във връзка с констатации, че с определени операции по обработване на лични данни са нарушени разпоредби на регламента, за отчетния период КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са издадени 9 Разпореждания и са отправени 1 Предупреждение и 1 Официално предупреждение.

РЕШЕНИЯ ПО ЖАЛБИ

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

РЕШЕНИЕ
№ ППН-01-871/2020
София, 27.09.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов, Мария Матева и Веселин Целков, на редовно заседание, проведено на 21.07.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 разгледа по основателност жалба № ППН-01-871/04.12.2020 г., подадена от Д.Л.Б. (Д.Б.)

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

Жалбоподателката информира, че многократно е призовавана от различни правоохранителни органи във връзка с ликвидирането на различни предприятия, като лицето Д.Л.Б., носещо нейните имена, неправомерно е използвало ЕГН-то ѝ.

Този психически тормоз започнал от 2016 година. Г-жа Д.Б. посочва, че е подала молба на 15.09.2016 г. до Община Варна, Дирекция МД, на която няма отговор. При многократното ѝ призоваване от полицейските органи, че е ликвидатор на дадени фирми, откъдето разбрала, че броят на същите е 74. Подала жалба до Окръжна прокуратура Монтана. С Постановление от 31.12.2018 г. окръжен прокурор О.Д. постановил, че отказва да образува досъдебно наказателно производство и прекратява преписката, тъй като обстоятелствата се дължат на съвпадение на имената – на жалбоподателката и на ликвидаторката и че са предприети действия по компетентност за коригиране на констатираната техническа грешка в информационните масиви. След това около година г-жа Д.Б. не била търсена за даване на обяснения по ликвидиране на търговски дружества, след което пак започнала да получава обаждания по телефона от НАП за поредна ликвидирана от нея фирма. Последното такова е на 01.12.2020 г. от НАП.

Жалбоподателката моли да бъде образувано производство и да бъдат наложени съответните наказания на виновното лице.

След получаване на жалбата е направена служебна проверка в публичния регистър на вписаните ликвидатори, публикуван на страницата на Агенция по вписванията. Направена е екранна разпечатка за вписания ликвидатор Д.Л.Б. Варна, професия „юрист“.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено заинтересованото лице – Национална агенция за приходите (НАП). Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения.

От НАП посочват, че извършена проверка по конкретния казус е установила, че данните за визираните дружества са постъпили в НАП чрез автоматична интеграция от Агенция по вписванията

за вписани обстоятелства в Търговския регистър и Регистъра на юридическите лица с нестопанска цел, като лицето Д.Л.Б. фигурира с трите си имена, но без идентификатор ЕГН. По данни от регистър ГРАО, вписани в регистъра на НАП с тези три имена се идентифицират три лица с различни ЕГН. Това е наложило служители в НАП да извършат допълнителна справка в правната информационна система „Сиела", от която са установили, че ЕГН на жалбоподателката като представляващ/ликвидатор е относимо към няколко дружества – Дружество 1, Дружество 2 (по повод на което е получила поканата от ТД на НАП Варна от 13.10.2017 г)., Дружество 3 и Дружество 4.

Предоставянето на отговор по какъв начин единният граждански номер на жалбоподателя г-жа Д.Б. е бил отразен в посочената правна информационна система е извън компетентността на НАП.

От НАП заявяват, че към настоящия момент некоректните записи с ЕГН за жалбоподателката като представляващ/ликвидатор във въпросните дружества са деактивирани в регистъра на агенцията.

Във връзка с посоченото в становището на НАП и приложените екранни разпечатки е направена служебна проверка чрез правно-информационната система „Сиела" по партидите на Дружество 1, Дружество 3 и Дружество 4. Като ликвидатор на трите дружества е вписано лицето Д.Л.Б. с ЕГН 79*****.

От Агенция по вписванията (накратко АВп), като трето лице, са изискани документите за назначаване на ликвидатор на горепосочените дружества, нотариално заверените съгласия по чл. 266, т. 3 от ТЗ, както и информация дали е налице документ по партидата на дружествата, с който ликвидаторът е индивидуализиран с ЕГН.

От АВп посочват, че за включване в списъка на ликвидаторите се подава заявление от лицето, към което се прилагат съответните документи. От извършената проверка в деловодството на Агенция по вписванията се установило, че на 09.12.2015 г. г-жа Д.Л.Б. с ЕГН 80***** е подала документи за включване в списъка на ликвидаторите към Агенция по вписванията и въз основа на тях е включена в същия.

Длъжностното лице по регистрацията към Агенция по вписванията назначава служебно ликвидатор в случаите, предвидени в закона. В хипотезата на принудителна ликвидация служебно назначеният ликвидатор може да приеме назначението, като представи нотариално заверено съгласие с образец на подписа по партидата на конкретния търговец съгласно чл. 266, ал. 3 от ТЗ или да откаже назначението, като представи отказ от встъпване в длъжност.

По отношение на посочените в писмото на КЗЛД търговски дружества е извършената справка и се установило, че търговската дейност на същите е прекратена на основание чл. 155, т. 3 от ТЗ и е открито производство по принудителна ликвидация.

За търговеца Дружество 4 – в ликвидация към настоящия момент като ликвидатор на дружеството е назначена г-жа Д.Л.Б. с Акт за назначаване на ликвидатор № ***/12.11.2019 г. В определения в акта срок ликвидаторът не е дал съгласие по чл. 266, ал. 3 от ТЗ и не е депозирал отказ от извършване на ликвидация.

Към момента за ликвидатор на Дружество 3 – в ликвидация с Акт за назначаване на ликвидатор № ***/17.04.2019 г. е определена г-жа М.С.С. В определения в акта срок ликвидаторът не е дал съгласие по чл. 266, ал. 3 от ТЗ и не е подал отказ от извършване на ликвидация.

По партидата на Дружество 1 – в ликвидация за ликвидатор е определена г-жа Д.Л.Б. с Акт за назначаване на ликвидатор № ***/22.06.2020 г. В определения в акта срок ликвидаторът не е дал съгласие по чл. 266, ал. 3 от ТЗ и не е подал заявление с искане да бъде освободен като ликвидатор.

От Агенция по вписанията са изискани и актовете за назначаване на ликвидатор с имена „Д.Л.Б." за трите дружества, които постъпиха по преписката. В същите не фигурира ЕГН на ликвидатора.

Във връзка с направена служебна проверка се установи, че Д.Л.Б. с ЕГН 79***** и същия адрес и телефонен номер като посочените в жалбата е регистрирана в регистър БУЛСТАТ като земеделски производител.

Предвид установеното и в условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено заинтересованото лице – „Сиела Норма“ АД. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения.

От дружеството посочват, че всички данни относно вписани и заличени обстоятелства, обявени и заличени актове в Търговския регистър и РЮЛНЦ, които се съдържат в продукта „Сиела Инфо“, „Сиела Норма“ АД получава във файлове от Агенция по вписванията по силата на договор. Получените от АВп данни се генерират автоматично в системата.

Посочените в писмото данни за лицето – имена Д.Л.Б. и ЕГН 79******, са получени от Агенцията по вписванията по описания по-горе начин.

След направена проверка от ръководителя на продукта Сиела Инфо не са открити файловете, в които се съдържат посочените данни, поради което от дружеството стигат до извода, че данните са от отдавна минал период. Дружеството не съхранява всички файлове, получени от АВп, тъй като информацията е в много голям обем и съхраняването на цялата информация, която се получава от АВп, ще натовари системите на дружеството прекомерно. По тази причина получените файлове от АВп периодично се изтриват.

В получаваните автоматично пакети по услугата по интеграция практиката на АВп да се идентифицират лицата в качеството им на служебни назначения по ЕГН е преустановена и справка за ликвидаторите може да се направи единствено в публикуваните списъци на ликвидатори в интернет страницата на АВп, където лицето Д.Л.Б. фигурира.

Справката в Сиела сочи, че действително в преобладаващата част от документите фигурират имената Д.Л.Б., но адресът и ЕГН-то съответстват и се отнасят за лицето, упражняващо адвокатска професия, като отсъстват документи, свързани и носещи личните данни на тъжителката.

Актовете за назначаване на ликвидатор, приложени към писмо до КЗЛД от Агенция по вписванията с изх. № 07-00-25/01.04.2021 г., са от периода, в който вече не се записва ЕГН в тези актове.

От изложеното в жалбата до КЗЛД е видно, че за период от една година на лицето не е било търсено за обяснения по ликвидиране на дружества. Очевидно несъответствието е било отстранено в информационните масиви на Агенция по вписванията, но при информационните системи на Сиела Инфо това е било неприложимо, защото практиката за вписване на актуални идентификатори – ЕГН от АВп вече е била преустановена. В противен случай корекцията би се реализирала автоматично.

По вписаните документи за отказ от поемане на назначението е видно, че лицето реално има друго ЕГН, но това обстоятелство не е интегрирано в тази част на информационните масиви на АВп, която от Сиела Норма получават, и не е подадено като ново в автоматизирания XML формат, който ползват за изграждане и актуализирана на информационните си системи. Тъй като лицето е единствено с тези три имена в списъка с ликвидатори, първото узнаване на ЕГН-то от системата на Сиела е било 79*****, а не 80*****, както сега в някои документи може да се наблюдава.

Корекции по служебен ред в АВп са невидими за информационните системи на Сиела. И тази колизия се е възпроизвеждала при всяко ново вписване на лице с имена Д.Л.Б. Проверката за промени е автоматична и очаква поява на нови лица или изтриване на стари в автоматично генерираните списъци.

От Сиела заявяват, че след получаване на писмото от КЗЛД, преглед на документацията и направена справка в ТРРЮЛНЦ, дружеството извършило корекция в системата и лицето Д.Л.Б. с ЕГН 79***** не фигурира в Сиела Инфо като ликвидатор на търговски дружества.

По редовността и допустимостта на жалбата КЗЛД намира следното:

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

Разглежданата жалба е съобразена с изискванията за редовност по чл. 29 от АПК, чл. 38а, ал. 2 от ЗЗЛД и по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА) – налице са данни за жалбоподателя; естество на искането; дата на узнаване на нарушението; лице, срещу което се подава жалбата; дата и подпис.

Жалбата е процесуално допустима – подадена в срока по чл. 38, ал. 1 от ЗЗЛД от субект на данни с твърдение за нарушени негови права по Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е" от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

На проведено на 19.05.2021 г. закрито заседание на Комисията жалбата е обявена за допустима и като страни в производството са конституирани: жалбоподател Д.Б. и ответна страна: Национална агенция за приходите, Агенция по вписванията и „Сиела Норма" АД. Страните са уведомени за насроченото за 21.07.2021 г. открито заседание за разглеждане на спора по същество.

На Агенция по вписванията е предоставена възможност за изразяване на становище и предоставяне на информация относно няколко въпроса. От АВп предоставят следната информация по поставените въпроси:

1. Вписва ли се в актовете за назначаване на ликвидатори ЕГН на ликвидатора? В случай че не се вписва, имало ли е такава практика в минал момент и кога е преустановена?

Съгласно разпоредбата на чл. 134, ал. 3 от Наредбата акта за назначаване следва да съдържа единствено информация относно името, образованието и специалността на ликвидатора, юридическото лице, в което се назначава за ликвидатор, възнаграждението на ликвидатора, както и срок за предоставяне на нотариално заверено съгласие от ликвидатора с образец от подписа му. В актовете за назначаване на ликвидатор не се вписва ЕГН на избрания ликвидатор. В Агенция по вписванията не е практика да се вписва ЕГН на избрания ликвидатор в акта за назначаване.

2. Предоставя ли Агенция по вписванията ЕГН на вписаните ликвидатори на дружествата, с които има сключени договори за получаване на информация от базата данни на агенцията?

Разпоредбата на чл. 12, ал. 1, т. 6 от ЗТРРЮЛНЦ предвижда възможността Агенция по вписванията да предоставя цялата база данни по чл. 2 от ЗТРРЮЛНЦ или структурирани части от нея чрез специализирани услуги за автоматизиран достъп до търговския регистър и до регисгъра на юридическите лица с нестопанска цел срещу заплащане на такса. Съгласно чл. 2. ал. 1 от ЗТРРЮЛНЦ Търговският регистър и регистъра на юридическите лица с нестопанска цел представлява обща електронна база данни, съдържаща обстоятелствата, вписани по силата на закон и актовете, обявени по силата на закон за търговците и клоновете на чуждестранните юридически с нестопанска цел. В базата данни се съхранява информация за делата на регистрираните търговци и юридическите лица с нестопанска цел за безсрочен период от време, като същите дела са разпределени в партиди. В изпълнение на задълженията, предвидени в ЗТРРЮЛНЦ, в регистъра се вписват обстоятелства, свързани с ликвидацията на търговците, в т.ч. и относно процедурата по назначаване на ликвидатори.

В тази връзка, Агенция по вписванията не предоставя ЕГН на вписани ликвидатори на дружествата. Единствените актове, които се представят във връзка с ликвидаторите са актовете за назначаване и както бе посочено по-горе същите не съдържат ЕГН на назначения ликвидатор, а единствено три имена, образование, адрес за кореспонденция, телефонен номер за връзка и електронна поща.

3. Каква информация и файлове са предоставени на „Сиела Норма" АД (въз основа на сключения с това дружество Договор № 93-00-123/25.06.2008 г.) относно вписване на ликвидатор с имена Д.Л.Б. на дружествата Дружество 1, Дружество 3 и Дружество 4?

Съгласно сключения договор Агенция по вписванията предоставя на „Сиела Норма“ АД еднократен достъп до цялата база данни, съдържаща информация за търговските субекти към датата на предоставянето, както и актуална информация за вписванията, заличаванията и обявяванията в базата данни по чл. 2 от ЗТРРЮЛНЦ.

В тази връзка и с оглед обстоятелството. че производството по ликвидация съгласно законовите изисквания подлежи на вписване в Търговския регистър и регистъра на юридическите лица с нестопанска цел, то информацията, която е предоставена във връзка със сключения договор по цитираните дружества е три имена на ликвидатора – Д.Л.Б., респективно файловете, които са предоставени са актове за назначаване с № ***/12.11.2019 г.; № ***/26.10.2018 г. и № ***/22.06.2020 г.

По преписката постъпи допълнително становище от Сиела.

От Сиела подчертават, че ако е имало разминаване между данните на лицето в Сиела Инфо и данните в ТРРЮЛНЦ, съответните държавни органи, които са потърсили жалбоподателката в качеството ѝ на ликвидатор, е следвало да се позовават на официалните данни, съдържащи се в ТРРЮЛНЦ като официален публичен регистър. Позоваването на данните в Сиела при работата на тези органи означава, че те са абонати на Сиела Инфо, за които важат Общи условия за ползване на компютърни правно-информационни системи „Сиела“ версии 5.1 и по-високи. В раздел X „ОТГОВОРНОСТ” на тези общи условия е записано, че информацията, предоставяна от „Сиела Норма“ АД чрез правно-информационните продукти „Сиела“, има справочно-информационен характер. Сиела Норма не носи никаква отговорност за каквито и да са загуби, преки, непреки или последващи вреди и пропуснати ползи, в резултат или във връзка с използването на ПИС Сиела, както и с неправилното използване или неумението и липсата на опит за ползване на ПИС.

При прецизна проверка на данните и умение за работа с информационния продукт може да се види, че в преобладаващата част от документите фигурират имената Д.Л.Б., като адресът и ЕГН-то съответстват и се отнасят за лицето, упражняващо адвокатска професия.

Очевидно е налице техническа грешка поради съвпадане на трите имена на две различни лица, чиито ЕГН-та са публични поради вписването на лицата в публични регистри: Търговски регистър и регистър БУЛСТАТ – едното като земеделски производител – Д.Л.Б. с ЕГН 79*** (жалбоподателката), другото като ликвидатор – Д.Л.Б. с ЕГН 80****, за която обаче дружеството не е уведомено нито през 2018 г., когато е констатирана грешката, нито по-късно – нито от държавните органи, нито от заинтересованото лице.

На проведеното открито заседание за разглеждане на жалбата по същество страните не се явяват, не се представляват.

При така установеното Комисията разгледа жалбата по същество, като я приема за частично основателна въз основа на следното:

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

Предмет на жалбата е твърдение за неправомерно обработване на личните данни на жалбоподателката чрез посочването ѝ като ликвидатор на няколко дружества и търсенето ѝ в това качество от органи на власт.

От фактическа страна се установи следното:

Видно от представените към жалбата писмени доказателства, до жалбоподателката са изпращани съобщения от Национална агенция за приходите, като същата е индивидуализирана чрез три имена (Д.Л.Б.), ЕГН (79*****) и адрес (гр. Монтана, ****) и се посочва, че е ликвидатор на няколко търговски дружества. Чрез посочените данни жалбоподателката може да бъде идентифицирана по несъмнен начин по смисъла на чл. 4, т. 1 от Регламент 2016/679.

Служебна проверка в публичния регистър на ликвидаторите, поддържан от Агенция по вписванията, свидетелства, че лице със същите имена – Д.Л.Б., е надлежно вписано като ликвидатор в регистъра. От представените от Агенция по вписванията документи за регистрация се установява, че вписаното в регистъра лице е с друго ЕГН – 80*** и с друг адрес – гр. Варна, ****. Адресът е посочен в публичния регистър, а ЕГН – не.

От НАП е изискана информация откъде разполага с ЕГН на жалбоподателката, което не е публично посочено в регистъра на ликвидаторите. От НАП посочват, че по данни от регистър ГРАО, с тези три имена има три лица с различни ЕГН-та. Това наложило проверка в правно-информационната система „Сиела“ по партидата на няколко дружества, където е отразено ЕГН на жалбоподателката като ликвидатор на дружествата. Представени са разпечатки в този смисъл.

Служебна проверка потвърди посоченото от НАП, че по партидата на три дружества (Дружество 1, Дружество 3 и Дружество 4)) като ликвидатор е посочено лице с имена „Д.Л.Б.“ и ЕГН 79***** – това на жалбоподателката.

В изисканите от Агенция по вписванията актовете за назначаване на ликвидатор с имена „Д.Л.Б.“ за трите дружества са вписани данните за контакт – адрес, електронна поща, телефон на лицето, вписано в публичния регистър на ликвидаторите. ЕГН не е вписан.

При така установено следва да се разгледа обработването на личните данни на жалбоподателката, извършено от всеки от администраторите на лични данни:

1. Агенция по вписванията:

Агенция по вписванията не обработва лични данни на жалбоподателката. Вписаното в регистъра на ликвидаторите лице е различно от жалбоподателката. В актовете за назначаване на ликвидатори на трите дружества са посочени данни за вписаното в регистъра лице.

Противно на твърденията на Сиела, не са представени никакви доказателства, че от Агенция по вписванията са предоставили ЕГН на жалбоподателката – в представените от АВп актове за назначаване на ликвидатор няма посочено ЕГН, а от Сиела посочват, че не съхраняват получената информация за дълъг период, тъй като е в огромен обем и натоварва сървърите, както и поради факта, че форматът на данните се сменя и старите стават неизползваеми. Тук следва да се посочи, че реквизите на акта за назначаване на ликвидатор при служебното му назначаване от длъжносно лице по регистрацията са нормативно определени в чл. 134, ал. 3 от Наредба № 1 от 14 февруари 2007 г. за водене, съхраняване и достъп до търговския регистър и до регистъра на юридическите лица с нестопанска цел и са: името, образованието и специалността на ликвидатора, юридическото лице, в което се назначава за ликвидатор, възнаграждението на ликвидатора, както и срок за представяне на нотариално заверено съгласие от ликвидатора с образец от подписа му. Тези реквизити са определени още от януари 2009 г., а назначаването на лице с имена „Д.Л.Б.“ за ликвидатор на Дружество 1, Дружество 3 и Дружество 4 е от периода 2019-2020 г.

Предвид горното, не се установи Агенция по вписванията да е предоставила ЕГН на жалбоподателката на Сиела, поради което жалбата спрямо нея е неоснователна.

2. Национална агенция за приходите:

НАП е обработила личните данни на жалбоподателката (ЕГН, адрес, телефон) за контакт с нея, считайки я за ликвидатор на няколко дружества – чрез изпращане на писма, позвъняване по телефон. Както беше посочено, жалбоподателката не е ликвидатор на тези дружества, а трето лице с идентични имена.

В случая служителите на НАП не са провели пълно и безспорно идентифициране на лицето – ликвидатор на дружествата. След получаване на информация от Агенция по вписванията са узнали трите имена на ликвидатора, след което поради липса на ЕГН са проверили в ГРАО, където с тези

имена са три различни лица. След справка в правно-информационната система Сиела Инфо по партидите на дружествата е узнато и ЕГН на жалбоподателката, където некоректно е посочено нейното ЕГН. Въпреки наличието на три лица с идентични имена, от НАП не са предприели допълнително действия за идентификация на ликвидатора и са се предоверили на информацията от Сиела Инфо. За това свидетелства и факта, че жалбоподателката е търсена на неин адрес и на неин телефонен номер, които данни при проверка в публичния регистър на вписаните ликвидатори в Агенция по вписванията би се установило, че са различни от тези на вписания ликвидатор. Тук следва да се посочи, че жалбоподателката е вписана в регистър БУЛСТАТ като земеделски производител и по партидата ѝ в регистъра са вписани адреса и телефонния ѝ номер, на които е търсена от НАП. Тези данни очевидно са налични в системата на НАП и се обработват за данъчни цели. В случая обаче са обработени и за други цели – за контакт с жалбоподателката в качеството на „ликвидатор“ на търговски дружества, каквото качество тя няма. Следователно, налице е нарушение на принципа за ограничение на целите по чл. 5, параграф 1, буква „б“ от Регламент 2016/679, съгласно който личните данни са събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

3. „Сиела Норма“ АД:

Сиела е обработила личните данни на жалбоподателката чрез посочване на единния ѝ граждански номер по партидите на няколко дружества, на които е назначен ликвидатор с идентични имена като нейните.

Както е посочено в т. 1, не се споделя становището на Сиела, че ЕГН на жалбоподателката е предоставено на дружеството от Агенция по вписванията чрез автоматично получените пакети по услугата по интеграция между Търговския регистър и правно-информационната система Сиела, извършено въз основа на сключен договор. Жалбоподателката и вписания ликвидатор са различни лица. Следователно, идентифицирането на жалбоподателката чрез ЕГН като ликвидатор на търговски дружества по партидата им е неточно.

Принципът за точност при обработването на лични данни по чл. 5, параграф 1, буква „г“ от Регламент 2016/679 предвижда, че личните данни следва да са точни и при необходимост да бъдат поддържани в актуален вид. Фактът, че правно-информационната система Сиела представлява информационна база данни означава, че има задължението да спазва този принцип. Чрез посочване на ЕГН на жалбоподателката като ликвидатор на няколко търговски дружества, каквото качество същата няма, е нарушен посоченият принцип за точност.

При така констатираните нарушения, извършени от НАП и Сиела Норма, жалбата следва да бъде частично уважена. КЗЛД разполага с оперативна самостоятелност, като в съответствие с предоставените ѝ функции преценява кое от корективни правомощия по чл. 58, пар. 2 от Регламент 2016/679 да упражни. Преценката се основава на съображенията за целесъобразност и ефективност на решението при отчитане на особеностите на всеки конкретен случай и степента на засягане на интересите на конкретното физическо лице – субект на данни, както и на обществения интерес. Правомощията по чл. 58, пар. 2, без тази по буква „и”, имат характера на принудителни административни мерки, чиято цел е да предотвратят или да преустановят извършването на нарушение, като по този начин се постигне дължимото поведение в областта на зашитата на личните данни. Административното наказание „глоба” или „имуществена санкция” по чл. 58 пар. 2, буква „и” има санкционен характер. При прилагането на подходящата корективна мярка по член 58, пар. 2 от Регламента се взема предвид естеството, тежестта и последиците от нарушението, както и всички смекчаващи и отегчаващи отговорността обстоятелства. Оценката за това какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай отразява и целта, преследвана с избраната корективна мярка – предотвратяване или преустановяване на нарушението, санкциониране на

неправомерното поведение или и двете, каквато възможност е предвидена в чл. 58, пар. 2, буква „и" от Регламент 2016/679.

Извършеното от НАП нарушение се характеризира с по-ниска степен на обществена опасност, тъй като в случая служителите са въведени в заблуждение от справката в правно-информационната система Сиела. Освен това няма данни жалбоподателката да се е обърнала с официално искане до НАП за заличаване или коригиране на данните ѝ като ликвидатор на дружества. В хода на производството от НАП посочиха, че са заличили жалбоподателката от системите си като ликвидатор на дружества.

Предвид множеството смекчаващи отговорността обстоятелства, КЗЛД намира, че следва да отправи официално предупреждение до НАП на основание чл. 58, параграф 2, буква „б" от Регламент 2016/679. Същото има за цел да обърне внимание на администратора да предприема по-внимателни действия при идентификация на лицата в сходни случаи предвид мотивите на настоящото решение и като предупреждение, че при следващо подобно нарушение би могло да се стигне и до налагане на имуществена санкция.

Относно нарушението, извършено от Сиела, КЗЛД приема, че ЕГН на жалбоподателката не е предоставено на Сиела от Агенция по вписванията. Тъй като жалбоподателката е вписана отделно в регистър БУЛСТАТ като земеделски производител, налице е обосновано предположение, че е налице автоматично индексиране и пренасяне на ЕГН при лица с идентични имена, когато за едно тях няма ЕГН. Предвид изложеното, КЗЛД намира, че следва на основание чл. 58, параграф 2, буква „г" от Регламент 2016/679 да разпореди на администратора да съобрази операциите по обработване с разпоредбите на регламента за точност на обработваните данни, като провери системата си за евентуална автоматична индексация и вписване на ЕГН на лица с идентични имена при липса на ЕГН от източника на информация.

КЗЛД намира, че в допълнение към посоченото разпореждане следва да наложи и административно наказание „имуществена санкция" за извършеното нарушение на основание чл. 83, параграф 5, буква „а" от Регламент 2016/679.

Отегчаващо отговорността обстоятелство, което обуславя налагането на имуществена санкция е, че Сиела предоставя информационната база данни на всички свои клиенти, т.е. неограничено към налични и потенциални потребители, като при неточна информация е възможно да бъдат въведени в заблуждение както частноправни субекти, така и държавни органи, какъвто е настоящият случай. Именно неточното посочване на ЕГН на жалбоподателката в Сиела Инфо е довело до неколкократното търсене на жалбоподателката от различни органи, които г-жа Д.Б. определя като „този психически тормоз".

Конкретните обстоятелства за определяне размера на имуществената санкция, в съответствие с чл. 83, параграф 2 от Регламент 2016/679, са следните:

Буква „а" – естество, тежест и продължителност на нарушението, брой засегнати субекти и причинена вреда: обработването се състои в безспорно идентифициране на физическо лице чрез посочване на ЕГН. До този момент лицето не е идентифицирано само чрез трите си имена и без допълнителни данни за идентификация. В случая е идентифицирано грешното лице пред всички трети лица, които ползват продукта Сиела Норма, което е довело и до търсене на лицето от различни органи във връзка с ликвидация на няколко търговски дружества. Това са отегчаващи отговорността обстоятелсва. Не е установено възникването на имуществени вреди, но в жалбата е изложено твърдение за неимущесвени такива – „този психически тормоз" във връзка с търсенето на жалбоподателката от различни органи. Това е в пряка и непосредствена връзка с нарушението – ако не беше посочено ЕГН на жалбопоподателката в Сиела Норма като ликвидатор на дружества, не би се стигнало до търсенето ѝ във връзка с тази дейност. Това също е отегчаващо отговорността обстоятелство. С нарушението е засегнато един субект на данни, което смекчава отговорността.

Буква „б" – дали нарушението е извършено умишлено или по небрежност: нарушението е извършено от юридическо лице, което не формира вина.

Буква „в" – действия за смекчаване на последиците от вредите: няма причинени имуществени вреди, неимуществените не могат да бъдат отстранени.

Буква „г" – степен на отговорност предвид въведените технически и организационни мерки: нарушението не отнася до непредприемане на технически и организационни мерки.

Буква „д" – свързани предишни нарушения: няма нарушение на сигурността на данните по смисъла на член 33 от Регламента или други свързани нарушения – смекчаващо отговорността обстоятелство.

Буква „е" – степен на сътрудничество с надзорния орган за отстраняване на нарушението и смекчаване на неблагоприятните последици: след узнаване за жалбата е извършена вътрешна проверка от администратора и са предприети действия за коригиране на все още наличното ЕГН на жалбоподателката като ликвидатор по партиди на дружества. Това е смекчаващо отговорността обстоятелство.

Буква „ж" – засегнати категории лични данни: ЕГН – уникален национален идентификатор. Не са обработени специални категории лични данни по смисъла на чл. 9 от Регламент 2016/679 – смекчаващо обстоятелство.

Буква „з" – узнаване на нарушението от надзорния орган: след сезиране на надзорния орган от субекта на данни.

Буква „и" – налагани предходни корективни мерки и дали са спазени: няма влезли в сила мерки по чл. 58, пар. 2 от Регламента към момента на постановяване на решението.

Буква „й" – придържане към одобрени кодекси на поведение или сертифициране: към момента на обработването няма одобрени кодекси за поведение.

Буква „к" – други обстоятелства: не са установени.

Съгласно чл. 10г от ЗЗЛД при упражняване на задачите и правомощията си по отношение на администратори или обработващи лични данни, които са микропредприятия, малки и средни предприятия, КЗЛД следва да вземе предвид техните специални потребности и налични ресурси. В този смисъл при налагане на административното наказание „имуществена санкция" размерът следва да бъде определен по начин, който да не създава изключителни затруднения на санкционирания администратор или обработващ. Анализ на финансови данни на дружеството показва, че администраторът попада в понятието средно предприятие по смисъла на чл. 3 от Закона за малките и средните предприятия.

След обсъждане на всички смекчаващите и отегчаващите отговорността обстоятелства в тяхната съвкупност, КЗЛД намира, че размерът на административното наказание „имуществена санкция" следва да бъде в размер на 5000 лв.

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

РЕШИ:

1. Обявява жалба № ППН-01-871/04.12.2020 г., подадена от Д.Л.Б., за неоснователна спрямо Агенция по вписванията.

2. Обявява жалба № ППН-01-871/04.12.2020 г., подадена от Д.Л.Б., за основателна спрямо Национална агенция за приходите за нарушение на чл. 5, параграф 1, буква „б" от Регламент 2016/679.

3. На основание чл. 58, параграф 2, буква „б" от Регламент 2016/679 отправя до Национална агенция за приходите официално предупреждение за операции по обработване на данни, нарушили разпоредбата по т. 2.

4. Обявява жалба № ППН-01-871/04.12.2020 г., подадена от Д.Л.Б., за основателна спрямо „Сиела Норма“ АД за нарушение на чл. 5, параграф 1, буква „г“ от Регламент 2016/679.

5. На основание чл. 58, параграф 2, буква „г“ от Регламент 2016/679 за нарушението по т. 4 разпорежда на „Сиела Норма“ АД да съобрази операциите по обработване с разпоредбите на регламента за точност на обработваните данни, като провери системата си за евентуална автоматична индексация и вписване на ЕГН на лица с идентични имена при липса на ЕГН от източника на информация. Срок за изпълнение на разпореждането 3 месеца от влизане в сила на решението, след което да бъде уведомена КЗЛД за изпълнението с представяне на съответните доказателства.

6. На основание чл. 58, параграф 2, буква „и” от Регламент 2016/679 във връзка с чл. 83, параграф 5, буква „а” налага на администратора на лични данни „Сиела Норма” АД с ЕИК 130199580, административно наказание „имуществена санкция” в размер на 5 000 (пет хиляди) лв. за нарушението по т. 4.

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

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

Банка БНБ – ЦУ

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Комисия за защита на личните данни, БУЛСТАТ 130961721

В случай че санкцията не бъде платена в 14-дневен срок от влизане в сила на решението, ще бъдат предприети действия за принудителното му събиране.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п

РЕШЕНИЕ
№ ППН-01-80/2021
София, 26.10.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов, Мария Матева и Веселин Целков, на редовно заседание, проведено на 29.09.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 разгледа по основателност жалба № ППН-01-80/27.01.2021 г., подадена от И.З.

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

Жалбата постъпи в КЗЛД по компетентност от Районна прокуратура Варна.

В жалбата до прокуратурата се посочва, че на 26.08.2020 г. на жалбоподателя е връчена за становище молба на Р.Д., депозирана по ИД 1 по описа на ЧСИ 1, по което същият има качеството на негов длъжник.

В молбата си Р.Д. е посочил, че жалбоподателят е длъжник по ИД 2, което според г-н И.З. не отговаря на истината. Жалбоподателят заявява, че не е бил длъжник на Р.Д. по посоченото изпълнително дело, тъй като задължението, заради което е образувано делото, е погасено още преди да бъде образувано. Въз основа на депозирани доказателства, изпълнителното дело е прекратено на основание чл. 433, ал. 1, т. 1 от ГПК още през 2018 г.

В молбата си Р.Д. е посочил, че на 24.04.2020 г. ЧСИ 2 е изготвила и му е предоставила справка от регистъра на банковите сметки и сейфове за сметките на жалбоподателя.

Жалбоподателят счита, че видно от тази справка, същата е направена на 24.04.2020 г. в 10:29:24 ч. на основание вече прекратено още през 2018 г. ИД 2.

Г-н И.З. посочва, че изготвената справка от регистъра на банковите сметки и сейфове е информация, която представлява лични данни, защитени от Регламент 2016/679, които не могат да бъдат предоставяни и използвани от Р.Д.

Счита, че е извършено престъпление (доколкото жалбата му е подадена до Районна прокуратура Варна).

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено заинтересованото лице – ЧСИ 2, вписана с рег. № *** в регистъра на Камарата на частните съдебни изпълнители (накратко по-нататък „ЧСИ 2“). Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения. В Комисията постъпи отговор за неоснователност на жалбата.

ЧСИ 2 счита, че не следва да се приема от КЗЛД, че банковата сметка представлява „лични данни“, когато се отнася за едни и същи страни по граждански и търговски дела. Идентификационните данни на страните се съдържат в тези дела (ЕГН). По тях може да се получат данни за наличието на техни банкови сметки във всяка банка, като банкова тайна представлява само размерът на авоара на титуляра на сметката.

В чл. 127, ал. 4 от ГПК изрично е прието, че по осъдителен иск за парично вземане ищецът посочва банкова сметка или друг начин на плащане като задължителен реквизит от съдържанието на исковата молба.

В чл. 489, ал. 1 от ГПК съдебният изпълнител посочва своята банкова сметка, по която за участие в публична продан наддавачите са длъжни да внасят задатък 10% върху началната цена. В Търговския закон чл. 13, при регистрация на дружествата, същите следва да посочват тяхната банкова сметка. Така е и в Германия, банковите сметки са обявени публично.

За да се направят правилни изводи от КЗЛД, ЧСИ 2 счита, че следва да се вземат предвид особеностите по движението на изпълнителното дело, а именно:

Взискателят адвокат Р.Д. е образувал на 06.06.2018 г. изп. дело № *** въз основа на изп. лист от 2018 г., издаден от ВРС – 13 състав по НЧХД **/2016 г., срещу адвокат И.Д., по силата на който И.З. е осъден да заплати на Р.Д. сумата 1000 лв., представляваща разноски за адвокатско възнаграждение. С Покана за доброволно изпълнение изх. № *****, получена от длъжника И.З. лично на 13.06.2018 г. от призовкаря на кантората, е посочено, че ако не плати доброволно задължението си в двуседмичен срок, ЧСИ ще пристъпи към принудително изпълнение по реда на ГПК, чрез удръжки от банкови сметки, трудово възнаграждение и пр.

На 20.06.2018 г. постъпила молба от длъжника И.З., чрез адвокат Д.П., с която моли да се прекрати изп.д. № *** на основание чл. 433, т. 1 и да му се присъдят разноски в размер на 300 лв. Приложено е банково бордеро от 08.02.2018 г. за платена сума в размер на 1 000 лв., с посочено основание за плащане – НЧХД № **/2016 г., с вносител – В.Б. Върху молбата е поставена резолюция: „да се вземе становище от взискателя”.

На 19.07.2018 г. постъпило становище от взискателя Р.Д., в което изразява становище, че след направена справка в „БАНКА ДСК“ установил, че по негова сметка, която на никого не е давал, дори на адвоката си, включително и на длъжника И.З., има постъпила на 08.02.2018 г. сума 1000 лв., платена от лицето В.Б., че няма взаимоотношения с такова лице и затова на 20.02.2018 г. е поискал и му бил издаден изп. лист, защото не е знаел и не е бил уведомен от И.З. за плащането и че тази сметка той ползува само за изплащане на застраховка „БУЛСТРАД-ЖИВОТ“. Приема, че тъй като длъжникът твърди, че тази сума е за погасяване на дълга, той е съгласен делото да се прекрати, като разноските направени от него останат за негова сметка. По отношение на разноските за пълномощника на И.З. взискателят изразява несъгласие.

Последвала жалба от И.З., с която се обжалват действията на ЧСИ за отказ от присъждане на разноски в размер на 300 лв. в негова полза. С определение на ВОС е потвърден отказът на ЧСИ да присъди 300 лв. в полза на И.З. по изп. д. № *** и прекратяването на изп. дело, влязло в законна сила на 21.01.2019 г.

На 24.04.2020 г. адвокат Р.Д. поискал **устно** от служителката в кантората справка за банкови сметки на дльжника И.З. по прекратеното изп. дело, като се позовал на плащане на такса от негова страна за такава справка по прекратеното изп. дело. Служителката счела, че няма нищо нередно и предоставила справката. Едва в края на 2020 г., след като били разпитани от дльжностно лице от икономическа полиция, разбрали, че е постъпила настоящата жалба от И.З. и че справката по прекратеното изпълнително дело е послужила на Р.Д. за доброволно плащане на негово задължение към И.З. за присъдена сума в размер на 383 лв.

Предвид гореизложеното, според ЧСИ 2, ако КЗЛД счете за осъществено нарушение, следва да се вземе предвид, че са спазени принципите, свързани с обработването на личните данни на жалбоподателя. Счита, че законосъобразно добросъвестно и прозрачно са обработени личните данни за легитимни цели, дори законен интерес, че няма риск за вреда на жалбоподателя, тъй като се касае за доброволно реализиране на негово вземане чрез плащане, макар и в незначителен размер. От друга страна, жалбоподателят е постъпил по същия начин с доброволно плащане на своето задължение към взискателя Р.Д. по прекратеното изп. дело, но не е заявил по какъв начин се е снабдил с неговата банкова сметка.

По редовността и допустимостта на жалбата КЗЛД намира следното:

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

Жалбата, подадена до Районна прокуратура Варна, е съобразена с изискванията за редовност по чл. 29 от АПК, чл. 38а, ал. 2 от ЗЗЛД и по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА) – налице са данни за жалбоподателя; естество на искането; дата на узнаване на нарушението; лице, срещу което се подава жалбата; дата и подпис.

Жалбата е процесуално допустима – подадена в срока по чл. 38, ал. 1 от ЗЗЛД от субект на данни с твърдение за нарушени негови права по Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

На проведено на 30.06.2021 г. закрито заседание на Комисията жалбата е обявена за допустима и като страни в производството са конституирани: жалбоподател И.З. и ответна страна ЧСИ 2, в качеството на администратор на лични данни. Страните са уведомени за насроченото за 29.09.2021 г. открито заседание за разглеждане на спора по същество.

На проведеното заседание жалбоподателят се представлява от адвокат. Процесуалният представител счита жалбата за основателна. Претендира разноски.

Ответната страна – не се явява, не изпраща представител.

При така установеното Комисията разгледа жалбата по същество, като я приема за основателна въз основа на следното:

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

Предмет на жалбата е твърдение за неправомерно обработване на лични данни на жалбоподателя, изразяващо се в направена от частен съдебен изпълнител справка в Българска народна банка за притежаваните от него банкови сметки, която справка е направена по прекратено изпълнително дело.

От представените по преписката доказателства се установява, че през 2018 г. при ЧСИ 2 образувано ИД 2 (или ***) с взискател Р.Д. и ответник И.З. – жалбоподател в настоящото производство. Посоченото изпълнително дело е **прекратено към дата 22.01.2019 г.,** видно от Определение № *** по в.гр.д. № *** на Варненски окръжен съд, ГО, V състав.

Видно от представената справка за банкови сметки и сейфове на физическо или юридическо лице от Регистър на банковите сметки и сейфове при БНБ, същата е извършена **на 24.04.2020 г.** във връзка с ИД 2. за лицето И.З.

От сведенията, дадени в настоящото производство, както и пред Районна прокуратура – Варна, се установява, че справката е направена от служител в кантората на ЧСИ 2 по устно искане на Р.Д. (взискател по ИД 2) и след заплащане на съответната такса.

Обработването на лични данни от администратори на лични данни е законосъобразно и допустимо, ако е налице някое от основанията, изчерпателно изброени в чл. 6, параграф 1 от Регламент (ЕС) 2016/679.

Съгласно чл. 2, ал. 1 от Закона за частните съдебни изпълнители (ЗЧСИ) частен съдебен изпълнител е лице, на което държавата възлага принудително изпълнение на частни притезания.

Съгласно чл. 16, ал. 1 от ЗЧСИ частният съдебен изпълнител **има право на достъп до лични данни на длъжника, когато това е нужно за целите на изпълнението**. Съгласно чл. 18, ал. 1 от ЧСИ по възлагане от взискателя ЧСИ може **във връзка с изпълнителното производство** да проучва имущественото състояние на длъжника, **да прави справки**, да набавя документи, книжа и други, да определя начина на изпълнението, както и да бъде пазач на описаното имущество.

Предвид горното, ЧСИ има право да обработва лични данни на длъжника, включително да прави справки, за упражняване на официалните правомощия, които са му предоставени със ЗЧСИ и Гражданския процесуален кодекс (ГПК) – основание за обработване по чл. 6, параграф 1, буква „д“, предл. второ от Регламент 2016/679.

Съгласно чл. 16, ал. 1 и чл. 18, ал. 1 от ЗЧСИ обаче, законодателят е предоставил официални правомощия на ЧСИ да прави справки за длъжника единствено за целите на изпълнението и във връзка с изпълнителното производство. Както беше посочено, справката в БНБ за банкови сметки на жалбоподателя е направена на 24.04.2020 г. по ИД 2 (или ***) по описа на ЧСИ 2, което е прекратено на 22.01.2019 г. От това следва, че справката е направена по вече прекратено изпълнително дело, т.е. обработването не е нужно за целите на изпълнението и изпълнителното производство.

Предвид горното, макар първоначално ЧСИ 2 да обработва лични данни на жалбоподателя на основание чл. 6, параграф 1, буква „д“, предл. второ от Регламент 2016/679 за целите на образуване и водене на изпълнителното дело, извършването на справка за банковите сметки на жалбоподателя след прекратяване на изпълнителното дело (след изпълнение на целта на обработването) представлява обработване по начин, който е несъвместим с тези цели. С това администраторът е извършил нарушение на принципа за ограничение на целите по чл. 5, параграф 1, буква „б“ от Регламент

2016/679, съгласно който личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

Неоснователно е възражението на ЧСИ 2, че банковата сметка не следва да се приема за лични данни, когато се отнася за едни и същи страни по граждански и търговски дела, тъй като техни идентификационни данни се съдържат в тези дела (ЕГН) и по тях може да се получат данни за наличието на банкови сметки във всяка банка.

Съгласно чл. 4, т. 1 от Регламент 2016/679 „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

В конкретния случай банковата сметка представлява лични данни от първата категория – всяка информация, свързана с идентифицирано физическо лице, тъй като справката в БНБ е извършена по имена и ЕГН на жалбоподателя, с които е идентифициран. Чрез справката е достъпена допълнителна информация за така идентифицираното лице – данни за всичките му банкови сметки, които са 3 на брой, а както посочва и самият жалбоподател – една от сметките не е предоставяна на никого, освен на застраховател за получаване на плащане. Именно поради тази причина лицето има право на защита на данните му да не стават достояние на трети лица, когато обработването не е необходимо за целите на изпълнителното производство и принудителното изпълнение.

При така констатираното нарушение жалбата следва да бъде уважена. Комисията разполага с оперативна самостоятелност, като в съответствие с предоставените ѝ функции преценява кое от корективни правомощия по чл. 58, пар. 2 от Регламент 2016/679 да упражни. Преценката се основава на съображенията за целесъобразност и ефективност на решението при отчитане на особеностите на всеки конкретен случай и степента на засягане на интересите на конкретното физическо лице – субект на данни, както и на обществения интерес. Правомощията по чл. 58, пар. 2, без тази по буква „и”, имат характера на принудителни административни мерки, чиято цел е да предотвратят или да преустановят извършването на нарушение, като по този начин се постигне дължимото поведение в областта на зашитата на личните данни. Административното наказание „глоба” или „имуществена санкция” по чл. 58 пар. 2, буква „и” има санкционен характер. При прилагането на подходящата корективна мярка по член 58, пар. 2 от Регламента се взема предвид естеството, тежестта и последиците от нарушението, както и всички смекчаващи и отегчаващи отговорността обстоятелства. Оценката за това какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай отразява и целта, преследвана с избраната корективна мярка – предотвратяване или преустановяване на нарушението, санкциониране на неправомерното поведение или и двете, каквато възможност е предвидена в чл. 58, пар. 2, буква „и” от Регламент 2016/679.

Администраторът на лични данни не попада в понятието „предприятие“ по смисъла на § 1, т. 1 от ДР на Закона за малките и средните предприятия, тъй като не извършва стопанска дейност, а осъществява властнически правомощия, поради което чл. 10г от ЗЗЛД е неприложим.

Предвид посочените правомощия на КЗЛД и тяхната цел, както и след преценка на конкретните смекчаващи и отегчаващи отговорността обстоятелства, обсъдени съгласно изискванията на чл. 83, параграф 2 от Регламент 2016/679, КЗЛД намира, че нарушението е с висока обществена опасност и следва да бъде наложено административно наказание „глоба“ на ЧСИ 2. Конкретните обстоятелства в съответствие с чл. 83, параграф 2 от Регламента са следните:

Буква „а” – естество, тежест и продължителност на нарушението: Администраторът на лични данни е лице, на което държавата е възложила да осъществява властнически правомощия, с оглед на което отговорността му е завишена. Нарушението е извършено чрез справка в регистър на

държавен орган, който не е публичен и общодостъпен. Достъпът на ЧСИ е предоставен единствено за изпълнение на властнически правомощия. Правомощията и задълженията на ЧСИ са подробно разписани в ЗЧСИ и ГПК, а в случая е допуснато нарушение именно на разпоредби от ЗЧСИ, което е довело и до неправомерното обработване. Тук следва да се посочи, че освен достъп до регистъра на БНБ, на частните съдебни изпълнители е предоставен достъп и до редица други регистри, които не са публични и общодостъпни (НБД „Население“ и др.), които следва да бъдат достъпвани единствено при служебна необходимост, а не във всички случаи. Именно поради тези отегчаващи отговорността обстоятелства на администратора следва да бъде наложено административно наказание „глоба“, което ще санкционира неправомерното поведение и ще въздейства предупредително занапред.

Като смекчаващи отговорността обстоятелства се приема, че нарушението е еднократно и с него са засегнати правата само на едно лице, като няма данни за настъпила вреда за лицето, вследствие на обработването.

Буква „б” – дали нарушението е извършено умишлено или по небрежност: нарушението е извършено умишлено – взискателят е заплатил такса, поискал е справката и служителят на частния съдебен изпълнител е направил справката и я е предоставил на взискателя.

Буква „в” – действия за смекчаване на последиците от вредите: не са констатирани вреди, които да подлежат на отстраняване, което е смекчаващо отговорността обстоятелство.

Буква „г” – степен на отговорност предвид въведените технически и организационни мерки: в случая задължението по какъв начин да се обработват данните произтича директно от закона (ЗЧСИ и ГПК), поради което нарушението не отнася до непредприемане на технически и организационни мерки. Именно това прави нецелесъобразно даването на разпореждане на администратора да изготви правила и да предприеме мерки, тъй като правата и задълженията във връзка с обработването са уредени в закона. Това е отечаващо отговорността обстоятелство.

Буква „д” – свързани предишни нарушения: не са установени свързани нарушения – смекчаващо отговорността обстоятелство.

Буква „е” – степен на сътрудничество с надзорния орган за отстраняване на нарушението и смекчаване на неблагоприятните последици: нарушението е довършено (справката е извършена и е предоставена на взискателя), поради което същото не може да бъде отстранено. Последиците от нарушението (узнаване на банковите сметки от трето лице) не могат да бъдат отстранени.

Буква „ж” – засегнати категории лични данни: неправомерно е достъпено до банкови сметки на жалбоподателя (останалите лични данни – имена и ЕГН на жалбоподателя са известни на ответната страна по делото). Целта на банковите сметки все пак е при необходимост да бъдат предоставяни на трети лица за извършване на съответните банкови операции. Не са обработени специални категории лични данни по смисъла на чл. 9 от Регламент 2016/679. Това са смекчаващи отговорността обстоятелства.

Буква „з” – узнаване на нарушението от надзорния орган: след сезиране на КЗЛД от субекта на данни чрез прокуратурата.

Буква „и” – налагани предходни корективни мерки и дали са спазени: нарушението е първо за администратора и не са му налагани мерки по чл. 58, пар. 2 от Регламент 2016/679, което смекчава отговорността.

Буква „й” – придържане към одобрени кодекси на поведение или сертифициране: към момента на извършване на нарушението няма одобрени кодекси за поведение.

Буква „к” – други обстоятелства: не са установени.

След обсъждане в съвкупност на посочените смекчаващите и отегчаващите отговорността обстоятелства, КЗЛД намира, че административното наказание „глоба“ следва да е в размер, близък до минимума.

Относно направеното от адвоката на жалбоподателя искане за разноски, следва да се има предвид, че съгласно чл. 12, ал. 3 от АПК в производствата по този кодекс не се заплащат разноски, освен ако това е предвидено в него или в друг закон, както и в случаите на обжалване на административни актове по съдебен ред и при предявяване на иск по този кодекс. В специалния закон (ЗЗЛД) не е уредена възможността за присъждане на разноски при разглеждане на жалби по чл. 38 от ЗЗЛД. В производството по издаване на индивидуални административни актове по Глава пета, раздел I от АПК, чиито разпоредби се прилагат за неуредените в ЗЗЛД и Регламент 2016/679 случаи, също не е предвидена възможността за присъждане на разноски, освен пътни и други разходи по чл. 47, ал. 2 от АПК, каквито в настоящия случай не се претендират.

Предвид горното, искането за разноски за адвокатско възнаграждение следва да бъде отхвърлено. В този смисъл е Решение № 9833/17.07.2020 г. по адм.д. № 13339/2019 г. по описа на Върховния административен съд на Република България, Пето отделение.

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

РЕШИ:

1. Обявява жалба № ППН-01-80/27.01.2021 г., подадена от И.З. срещу ЧСИ 2, да бъде обявена за основателна за нарушение на чл. 5, параграф 1, буква „б“ от Регламент 2016/679;

2. На основание чл. 58, параграф 2, буква „и” от Регламент 2016/679 във връзка с чл. 83, параграф 5, буква „а” налага на администратора на лични данни ЧСИ 2, БУЛСТАТ *, административно наказание „глоба” в размер на 750 (седемстотин и петдесет) лв.;**

3. Отхвърля искането на И.З. за присъждане на разноски в производството.

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

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

Банка БНБ – ЦУ

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Комисия за защита на личните данни, БУЛСТАТ 130961721

В случай че санкцията не бъде платена в 14-дневен срок от влизане в сила на решението, ще бъдат предприети действия за принудителното му събиране.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-93/2021 г.
гр. София, 06.10.2021 г.

ОТНОСНО: *Обработване на данни за ваксинационния статус*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 29.09.2021 г., разгледа редица писма от организации и граждани относно законосъобразното обработване на данни за ваксинационния статус.

Анализът на горепосочените писма показва, че както гражданите, така и бизнесът, имат нужда от разяснения и насоки във връзка с допустимостта на обработване на данни за ваксинационния статус.

Настоящото становище има за цел да отговори на исканията, като отчита насоките и принципните позиции на Европейския комитет по защита на данните (ЕКЗД) и Европейския надзорен орган по защита на данните (ЕНОЗД), изразени по същите въпроси.

Правен анализ:

На равнище ЕС европейските съзаконодатели приеха Регламента за Цифровия COVID сертификат на ЕС[1] , който се прилага пряко във всички държави членки считано от 1 юли 2021 г. (в него е заложено да се прилага до 30 юни 2022 г.). Целта му е да улесни и направи безопасно свободното движение на граждани в рамките на ЕС по време на пандемията от COVID-19.

Сертификатът разполага с оперативно съвместим и машинночетим QR код, достъпен на хартиен или цифров носител.

Чрез него се удостоверява, че дадено лице е:

- ваксинирано срещу COVID-19;
- получило отрицателен резултат от тест; или
- преболедувало инфекцията.

Разпоредбата на чл. 10, пар. 1 във вр. със съобр. 48 от Регламента за Цифровия COVID сертификат на ЕС дефинира ясно, че Регламент (ЕС) 2016/679 (ОРЗД) се прилага за обработването на лични данни, извършвано при неговото изпълнение.

Съгласно чл. 10, пар. 2 от Регламент (ЕС) 2021/953 (който е *lex specialis* по отношение на ОРЗД) 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 COVID-19** и само в рамките на определения от регламента срок, като след това не следва да се извършва по-нататъшно обработване.

Допълнителен правно обвързващ аргумент в полза на заложения в Регламент (ЕС) 2021/953 подход е и съображение (54) от Регламент (ЕС) 2016/679, което гласи:

---

1 Регламент (ЕС) 2021/953 на Европейския парламент и на Съвета от 14 юни 2021 година относно рамка за издаването, проверката и приемането на оперативно съвместими сертификати за ваксинация срещу, направено изследване за и преболедуване на COVID-19 (Цифров COVID сертификат на ЕС) с цел улесняване на свободното движение по време на пандемията от COVID-19

(54) Обработването на специални категории лични данни може да е необходимо по съображения от обществен интерес в областта на общественото здраве, без съгласието на субекта на данните. Такова обработване следва да бъде предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на физическите лица. В този контекст понятието „обществено здраве" следва да се тълкува по смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета и означава всички елементи, свързани със здравето, а именно здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху това здравословно състояние, потребности от здравно обслужване, средства, отделени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причини за смъртност. ***Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели от трети страни като работодатели или застрахователни дружества и банки.***

За всяка друга цел обаче, националното законодателство трябва изрично да предоставя правно основание за обработване на данните от сертификатите[2]. В този смисъл ОРЗД е напълно приложим и по отношение на обработването на личните данни за всяка друга цел, различна от целта на Регламента за Цифровия COVID сертификат на ЕС. В този дух е и *Съвместното становище 04/2021[3] на Европейския комитет по защита на данните (ЕКЗД) и Европейския надзорен орган по защита на данните (ЕНОЗД) относно предложението за Регламент на Европейския парламент и на Съвета спрямо рамката за издаване, проверка и приемане на оперативно съвместими удостоверения за ваксинация, направен тест и преболедуване с цел улесняване на свободното движение по време на пандемията от COVID-19 (Цифрово зелено удостоверение).*

Дали и как сертификатите попадат в обхвата на ОРЗД ще зависи от начина, по който администраторите възнамеряват да ги използват. В тази връзка могат да се очертаят следните хипотези:

1) Администраторът възнамерява да записва систематично сертификатите или информацията, която те съдържат, като част от регистър с лични данни;

2) Администраторът възнамерява да въведе цифрова проверка на сертификатите, включваща сканиране на техния QR код (със или без записване на данните, които съдържат);

3) Администраторът възнамерява да въведе ръчна проверка на сертификатите, включваща проверяване на отпечатани хартиени копия или ръчна проверка на цифровия сертификат (само чрез визуализиране на сертификата, без да се сканира QR кода и/или без да се записва/документира информацията, съдържаща се в него).

Хипотези (1) и (2) представляват дейности по обработване на лични данни, които попадат в материалния обхват на ОРЗД (чл. 2, пар. 1 ОРЗД) и в този смисъл трябва да отговарят на предвидените в него условия за законосъобразност.

Хипотеза (3) не попада в обхвата на ОРЗД, но въпреки това, изискването за споделяне на чувствителна медицинска информация представлява намеса в основното право на личен живот, което е защитено с чл. 7 от Хартата на основните права на ЕС (Хартата). Чрез подобна намеса могат да бъдат засегнати и други права на човека, освен неговата неприкосновеност, като напр. правото на недискриминация, правото на труд, правото на образование, права на детето[4] и т.н. Следователно такава мярка трябва да бъде обект на условията за законосъобразност, необходимост и пропорционалност, предвидени в чл. 52, пар. 1 от Хартата и администраторът трябва да извърши внимателна преценка дали подобна намеса може да бъде законово оправдана.

---

2 Съображение 48 от Регламент (ЕС) 2021/953

3 https://edpb.europa.eu/system/files/2021-07/edpb_edps_joint_opinion_dgc_bg.pdf

4 В случаите, когато се отказват социално гарантираните му права, като например да посещава детска градина или ясла, когато родителите му не докажат статут на ваксинирани, преболедували или тествани за COVID-19.

Безспорно е, че сертификатите съдържат чувствителна здравна информация, която представлява специална категория данни и нейното обработване трябва да отговаря на по-завишения праг за законосъобразност, заложен в чл. 9 от ОРЗД.

Като мярка, предназначена да защити здравето и безопасността на персонала (работници/служители) чл. 9, пар. 2, б. „б" от ОРЗД може да осигури подходящо основание за законосъобразно обработване на данните от цифровите сертификати. Приложими могат да бъдат и условията за законосъобразност по чл. 9, пар. 2, б. „ж" или чл. 9, пар. 2, б. „и" ОРЗД, ако националното законодателство налага по-широко използване на сертификатите.

Следва да се отбележи, че някои от практическите приложенията на сертификатите могат да се квалифицират като дейности по автоматизираното вземане на индивидуални решения и профилиране, които от своя страна се регламентират от чл. 22 на ОРЗД. Такъв например може да бъде случаят, когато се използва цифрова проверка на сертификатите (чрез сканиране на QR кода) за целите на автоматизиран достъп до помещения. Тази дейност би представлявала автоматизирано вземане на индивидуално решение, което поражда неблагоприятни последствия за субекта на данни, вкл. правни такива. Към момента нито правото на ЕС, нито националното ни право, разрешават (каквото е изискването на чл. 22, пар. 2, б. „б" от ОРЗД) проверка на сертификатите, основана единствено на автоматизирано обработване, за целите на даване или отказ на достъп до помещения въз основана на съображения за безопасност на здравето. На практика това означава, че използването на сертификатите за такива цели не може да се основава **единствено** на автоматизирано обработване, което не включва адекватно човешко участие в процеса на тяхната проверка.

Когато обработването на данни от сертификатите отговаря на изискванията за законосъобразност, необходимост и пропорционалност, трябва да бъдат приложени подходящи технически и организационни мерки за тяхната сигурност. Администраторът следва да прецени необходимостта от извършване на оценка на въздействието върху защитата на данните по чл. 35 от ОРЗД с цел установяване на рисковете и тяхното смекчаване на всички етапи от обработването. Когато сертификатите се използват като условие и средство за получаване на достъп до помещения, такава оценка ще е почти винаги необходима, тъй като касае мащабно обработване на специални категории лични данни.

Способите за защита на данните на етапите на „проектиране" и по „подразбиране" също трябва да бъдат отчетени от администратора, гарантирайки, че се обработват само минимален обем от данни и се използват технологии, щадящи поверителността. В тази връзка следва да се предвидят процедури за проверка, чрез които да се избягва записването и запазването на лични данни в съответствие с принципа за свеждане на данните до минимум и в изпълнение на Регламента за Цифровия COVID сертификат на ЕС, който има за цел децентрализирано проверяване на сертификатите без обработване на допълнителни данни за това.

В съответствие с принципа за прозрачност, субектите на данни (служители, посетители и др.) трябва да бъдат предварително информирани за наложените от администратора мерки при проверка на сертификатите, като напр. как ще се извършва тя, какви данни ще се обработват, кой ще има достъп до тях и към кой могат да се отправят искания или възражения свързани с обработването на тези данни.

Защитата на личните данни е само един от аспектите при въвеждането и прилагането на мерки за ограничаване на разпространението на епидемията.

Към настоящия момент в редица държави от ЕС (Германия[5], Франция[6], Италия[7], Нидерландия,

5 На 22 април 2021 г. е обнародван закон, с който се дават привилегии на ваксинираните лица.

6 На 26 юли 2021 г. френският парламент приема закон, който разширява ползването на сертификатите, впоследствие преминал и през конституционен контрол.

7 Нормативният акт, с който се разширява ползването на сертификатите е обнародван на 6 август 2021 г. в Официалния вестник на Италия: https://www.gazzettaufficiale.it/eli/id/2021/08/06/21G00125/sg

Австрия[8], Гърция, Дания[9], Кипър[10] и др.) са извършени или са в процес на извършване законодателни промени, които да отговорят както на наложените безпрецедентни обществени отношения, така и на действащия правопорядък, гарантиращ основните права и свободи на гражданите. Швейцария, макар и да не е държава-членка на ЕС, прие в началото на месец септември т.г. законодателство, с което въвежда задължително ползване на сертификатите за целите на посещение на ресторанти и други обществени обекти. Тъй като темата надскача пределите на компетентност на един надзорен орган по защита на личните данни, считаме, че в стратегически план тя следва да бъде дискутирана във възможно най-широк кръг от други публични органи, граждани и организации. Подобен подход би спомогнал за приемането на необходимите правно обвързващи актове на национално равнище.

В Държавен вестник бр. 44 от 13.05.2020 г. беше обнародван Закон за изменение и допълнение на **Закона за здравето**, който урежда правните инструменти за ограничаване на разпространението на епидемията и преодоляване на последиците от нея, които се прилагат на територията на страната след отмяната на извънредното положение, т.е. след 13 май 2020 г. Регламентирани са както изцяло нови, различни по своя характер мерки, така и промени във вече въведените такива.

Законът дава право на Министерски съвет, по предложение на министъра на здравеопазването, да обявява извънредна епидемична обстановка на територията на страната при непосредствена опасност за живота и здравето на гражданите от разпространението на заразна болест, каквато е COVID-19. Уреждат се и условията, които следва да са изпълнени, за да бъде въведена такава обстановка. Във връзка с това, със свое Решение № 325 от 14.05.2020 г. Министерският съвет обяви извънредна епидемична обстановка на територията на страната, която продължава и към настоящия момент. Противоепидемичните мерки се въвеждат със **заповед** на министъра на здравеопазването или на друг компетентен орган (напр. директор на съответната РЗИ).

Наред с това, **Законът за мерките и действията по време на извънредното положение, обявено с решение на народното събрание от 13 март 2020 г. и за преодоляване на последиците (загл. доп. – ДВ, бр. 44 от 2020 г., в сила от 14.05.2020 г.)** предвижда, че министърът на здравеопазването освен по Закона за здравето може да въвежда и други временни мерки и ограничения, определени в **закон**.

Преди въвеждането на интрузивни мерки като тестове (антигенен/PCR) или обработване на данни за ваксинационния статус на лицата, администраторите могат да обмислят използването на агрегирани (обобщени) данни за здравето. Агрегираните данни, които не позволяват свързването на информация за здравето с отделни лица, могат да се считат за анонимни[11], т.е. не попадат в обхвата на ОРЗД.

Примерите за такива обобщени здравни данни включват:

- Процент на служителите, които са ваксинирани срещу COVID-19 в рамките на определен период от време;
- Процент на служителите без ваксинация срещу COVID-19 или на тези с неизвестен ваксинационен статус.

Службите по трудова медицина, разполагащи с ваксинационния статус на лицата, могат да бъдат натоварени с изготвянето на такива обобщени данни. За да се гарантира обаче, че обобщените

---

8 На 26 май 2021 г. австрийският парламент одобрява законопроект, въвеждащ така наречения „зелен пропуск", който предоставя на притежателите му достъп до ресторанти, хотели и културни заведения, ако могат да докажат, че са ваксинирани, преболедували от COVID-19 или са дали отрицателен тест за вируса.

9 Дания е една от първите държави въвели законодателство в тази област още през месец април 2021 г.

10 В Кипър такова законодателство действа от 9 юли 2021 г.

11 Вж. Становище 05/2014 на Работната група по чл. 29 относно техническите способи за анонимизиране, прието на 10 април 2014 г. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_bg.pdf

данни са анонимни, те винаги трябва да се отнасят до групи от индивиди, които са достатъчно големи, за да се изключи възможността за идентифициране на конкретно лице.

Поначало службата по трудова медицина може да не разполага с тази информация (или тя да е неточна или неактуална). В тези случаи, за да получат агрегирани данни, администраторите могат да насърчават персонала си да информира службата по трудова медицина за техния ваксинационен статус, при условие че това е доброволно и се извършва само от медицинско лице.

Администраторите могат да обмислят също така използването на анкети, от които да получат представа за процента на ваксинирани и неваксинирани служители. Тези анкети следва да бъдат доброволни и анонимни. В случай че се използва електронен инструмент за провеждането им, трябва да се гарантира, че той осигурява анонимност на участващите лица (дори ако такъв инструмент не събира имена или имейл адреси, той може да събира IP адреси). Поставянето на отворени въпроси в тези анкети трябва да се избягва, тъй като чрез отговорите им може да се идентифицира конкретно лице.

На равнище ЕС изискванията на Регламента за Цифровия COVID сертификат на ЕС изключват изначално приложимостта на съгласието по отношение на обработването на данните, съдържащи се в сертификатите. Както беше посочено по-горе, обработването на данните за други цели може да се извършва единствено, ако правното основание за това е установено в националното законодателство, т.е. то трябва да има характера на законово задължение. Съгласието, като основание, предвидено в правото на ЕС (ОРЗД), не може да бъде приложимо за обработване на лични данни от Цифровия COVID сертификат на ЕС. В съображение (48) от Регламент (ЕС) 2021/953 е предвидено изрично, че държавите членки могат да въведат в националното си законодателство възможност за обработване на данните за други цели, при условие че е предвидено ясно разписано правно основание за това, което съответства на правото на ЕС за защита на данните и с принципите на ефективност, необходимост и пропорционалност, и трябва да включва разпоредби, в които ясно се посочват обхватът и степента на обработването, конкретната цел, категориите субекти, които могат да проверяват сертификата, както и съответните гаранции за предотвратяване на дискриминация и злоупотреби, като се отчитат рисковете за правата и свободите на субектите на данни. Регламент (ЕС) 2021/953 забранява изрично съхраняването на данни от сертификата, когато обработването е за немедицински цели.

Доколкото в отвореното писмо, предоставено на КЗЛД, се повдигат въпроси, свързани с ваксинационния статус на родителите на деца от детските градини, изложените по-горе аргументи запазват в пълна степен своята приложимост. Следва обаче да се има предвид, че недопускането в детска градина на деца на неваксинирани родители, може да доведе до нарушаване и на конкретни права и интереси и на децата. Водени от принципа за осигуряване на най-добрия интерес на детето (чл. 3, т. 3 от Закона за закрила на детето), то не би следвало да търпи неблагоприятни правни последици и ограничения на неговите права или привилегии вследствие на действия или бездействия на неговите родители (арг. от чл. 10, ал. 3 от Закона за закрила на детето).

За пълнота на информацията следва да се има предвид, че Министерство на здравеопазването е разработило и пуснало за употреба приложение за проверка на Цифровия COVID сертификат на ЕС – т.нар. „Covid Check BG".

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

СТАНОВИЩЕ:

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 COVID-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 параграф втори, 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.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-77/2021 г.
гр. София, 06.10.2021 г.

ОТНОСНО: *Допустимост на обработване на лични данни при продажба на акцизни стоки – цигари и алкохол, от оператор чрез отдалечен достъп (посредством автомати с видеоконтрол и дистанционен достъп от оператор)*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 29.09.2021 г., разгледа писмо с вх. № ПНМД-01-77/12.08.2021 г. на главния секретар на Министерство на икономиката (МИ) по повод на постъпило писмо от управителя на търговско дружество със запитване относно допустимостта на продажбата на алкохол и цигари чрез автомати с видеоконтрол и дистанционен достъп от оператор съгласно българското законодателство. Във връзка с нормативно регламентираните функции на министъра на икономиката се обръща внимание на следното:

Законът за тютюна, тютюневите и свързаните с тях изделия (ЗТТСТИ) въвежда забрана за предлагането и продажбата на тютюневи и свързаните с тях изделия от автомати (чл. 30, ал. 2, т. 10), забрана на трансграничните продажби от разстояние, както и предлагането и продажбата на потребителите на тези изделия чрез услугите на информационното общество (чл. 31а). За неспазване на посочените правни норми в чл. 46 от ЗТТСТИ са предвидени административнонаказателни разпоредби. Предвид това, продажбата на тютюневи изделия от вендинг автомат би било нарушение на ЗТТСТИ.

В писмото на МИ се посочва, че Законът за виното и спиртните напитки (ЗВСН) урежда условията и реда за производството, получаването, преработката, етикетирането, търговията и

контрола на етиловия алкохол и дестилатите от земеделски произход, и на спиртните напитки. Член 131 от ЗВСН забранява продажбата на наливни спиртни напитки и бутилиране и продажба на спиртни напитки в пластмасови бутилки с вместимост над 0,5 литра.

Спиртните напитки и цигарите са акцизни стоки, които подлежат на специфични разпоредби, свързани с акцизното законодателство, което попада в компетентността на Министерството на финансите (МФ) и в частност на Агенция „Митници". Доколкото алкохолните напитки (пиво, вино и високоалкохолни напитки) попадат в обхвата на Закона за храните (ЗХр), а употребата на тютюневи изделия и алкохолни напитки, като рискови за здравето фактори се регулира от Закона за здравето (ЗЗдр), от значение е становището на Министерството на земеделието, храните и горите (МЗХГ) и Министерството на здравеопазването (МЗ).

От МИ считат, че по въпроса за приложимостта на предлаганата идентификация на лицата, които ще купуват тютюневи и алкохолни изделия от вендинг автоматите - сканиране на лична карта и лицево разпознаване, следва да се поиска становище от КЗЛД, поради което се обръщат към комисията с молба за произнасяне по компетентност по препратеното писмо на търговското дружество.

Към писмото на МИ е приложено копие от искането на дружеството, според което то е компания-лидер в сектора на бързооборотните стоки и представител на водещи марки от ЕС и трети страни като Johnnie Walker, J&B, Bushmills, Smirnoff, Hennessy, Gordons, Baileys и много други.

В качеството си на дистрибутор за България на световно известни и реномирани марки продукти, дружеството иска да получи становище по следните въпроси, свързани с въвеждането на територията на Република България на автомати за продажба на акцизни стоки - цигари и алкохол от оператор с отдалечен достъп чрез видеоконтрол.

Покупко-продажбата ще преминава през няколко етапа:

1. Когато купувачът натисне върху номера на желания от него артикул, автоматично съобщение ще излезе на екрана, което ще гласи, че за да се закупи съответната стока (цигари или алкохол), е нужна идентификация на лицето, която е съобразена със Закона за защита на личните данни.

2. След като лицето даде своето съгласие, операторът (продавачът) получава сигнал и се свързва в реално време с купувача. Операторът дава указание на лицето да приближи своята лична карта с лицевата ѝ част към обозначеното за това място на автомата. След като последния изпълни указанието, операторът идентифицира самоличността на купувача, като проверява дали лицето е навършило пълнолетие и дали е същото като това на снимката от личната карта.

3. Ако операторът установи, че всичко е наред и лицето има навършена 18- годишна възраст, му позволява да довърши своята покупка. В противен случай – процесът ще бъде прекратен.

С оглед на горното от дружеството молят за становище по следния въпрос:

„Описаният вид продажба на акцизни стоки, чрез продавач с дистанционен достъп до вендинг автомат, приложим ли е съгласно действащото българско законодателство?"

Правен анализ:

Законосъобразният характер на обработването на лични данни предполага наличието на поне едно от основанията, посочени в чл. 6, пар. 1 и/или чл. 9, пар. 2 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД), както и спазването на основните принципи, прогласени с чл. 5 от същия регламент.

Както се посочва в писмото на МИ, ЗТТСТИ въвежда забрани, както за продажба на тютюневи и свързани с тях изделия от автомати за продажба на тютюневи или свързани с тях изделия и от щандове за самообслужване, с изключение на обектите за безмитна търговия (чл. 30, ал. 2, т. 10), така и за трансграничните продажби от разстояние, както и предлагането и продажбата на потребители на

тютюневи и свързани с тях изделия чрез услугите на информационното общество (чл. 31а). С оглед на това може да се направи обоснован извод, че обработването на лични данни, което произтича от дейностите, забранени със ЗТТСТИ, би било незаконосъобразно поради липса на правно основание, респективно противоречие с принципа, посочен в чл. 5, пар. 1, б. „а" от ОРЗД.

В случай че законодателството допуска продажбата на алкохол да се извършва чрез вендинг машини или автомати, следва да се направят някои принципни уточнения, произтичащи **от въведената с чл. 54, т. 1 от ЗЗдр забрана за продажба на алкохолни напитки на лица под 18 години.**

Посочената забрана не налага, при нейното осъществяване, да се извършва идентификация на лицата, а само проверка на годината на раждане (т.е. дали лицето е навършило пълнолетие или не), както и дали отговаря на лицето по снимката на документа за самоличност. Приложение намира разпоредбата на чл. 11, пар. 1 от Регламент (ЕС) 2016/679, според която ако целите, за които администратор обработва лични данни, не изискват идентифициране на субекта на данните от администратора, същият не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данни с единствената цел да бъде спазен ОРЗД. Това кореспондира с принципа за обработване на минимален обем от данни, съгласно чл. 5, пар. 1, б. „в" от ОРЗД.

За целите на настоящия правен анализ е от съществено значение да се направи ясно разграничение между традиционния начин за продажба на алкохол и този, извършван чрез вендинг машини и автомати.

Проверката на възрастта на купувача при традиционния начин на продажба на алкохол може да се извърши при съмнение чрез изискване показването на документ за самоличност. Принципно положение е, че това не представлява обработване на лични данни, доколкото не се водят записи, представляващи регистри с лични данни.

По различен начин обаче, стои извършването на проверка за възрастта на купувача, когато това се осъществява изцяло или частично чрез автоматични средства, както се посочва в искането. В тази хипотеза проверката представлява обработване на лични данни, попадащо в материалния обхват на ОРЗД (чл. 2, пар. 1). С оглед на това, администраторът е длъжен да спази всички изисквания, произтичащи от ОРЗД.

За да е в състояние да съблюдава предвидената в ЗЗдр забрана за продажба на алкохол на лица под 18 години, за продавача (администратор на лични данни) възниква законово задължение да извърши съответната проверка, което от своя страна представлява основание за обработване на конкретни лични данни по смисъла на чл. 6, пар. 1, б. „в" от ОРЗД. Наличието на това основание изключва приложимостта на съгласието по чл. 6, пар. 1, б. „а" от ОРЗД, като основание за обработването на лични данни.

С оглед законосъобразния характер на обработването на личните данни в случая следва да се отчита и разпоредбата на чл. 25г от Закона за защита на личните данни (ЗЗЛД), според която администратор или обработващ лични данни може да копира документ за самоличност само ако това е предвидено със закон. Тъй като в конкретния случай липсва такова изискване по закон, копирането на документа за самоличност и в по широк смисъл неговото заснемане и запазване, са недопустими. Следователно планираният за използване механизъм за проверка чрез отдалечен достъп посредством видеоконтрол следва да отговаря на същите условия.

Тъй като използването на механизма за проверка на данни от документа за самоличност, извършвана чрез отдалечен достъп посредством видеоконтрол, би могло да породи висок риск за правата и свободите на субектите на данни, като в това число се включват и лицата до 18 годишна възраст, които са обект на специалната защита, администраторът следва да извърши оценка на риска и съответната оценка на въздействието върху защитата на данните. При извършване на оценките на риска и въздействието администраторът трябва да отчита потенциалните заплахи, които могат да

имат отношение при конкретното обработване, като например неоторизиран достъп до системата за видеоконтрол, наличие на скимиращи устройства и други.

В случай че такова обработване се предприеме от администратора, същият трябва да предприеме мерки за гарантиране прозрачността и информираността на субектите на данни по смисъла на чл. 13 и/или чл. 14 от ОРЗД. Съществен елемент на това задължение на администратора е в информацията да се посочи ясно кой е администраторът, какви са правата на субектите на данни и как те могат да бъдат упражнявани, като се отчита, че е възможно да се обработят и лични данни на деца (до 18 години). В този смисъл информацията трябва да бъде ясна, разбираема и лесно достъпна.

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

СТАНОВИЩЕ:

1. Обработването на лични данни, което би могло да произтече от дейностите, забранени с чл. 30, ал. 2, т. 10 от Закона за тютюна, тютюневите и свързаните с тях изделия (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.

2. Ако законодателството допуска продажбата на алкохол 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 на личните данни, съдържащи се в него, тъй като това би представлявало нарушение на законодателството за защита на личните данни.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п

ДОКЛАДИ

ДОКЛАД

за резултатите от проведено проучване
за необходимостта от експерти със специфични умения в областта на защитата на личните данни в малките и средни предприятия
октомври 2021 г.

СЪДЪРЖАНИЕ

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

АЛД - Администратор на лични данни

МСП - Малко и средно предприятие

ОРЗД - Общ регламент относно защитата на данните

ООН - Организация на обединените нации

КЗЛД -Комисия за защита на личните данни

ВЪВЕДЕНИЕ

Глобализиращият се свят създава едновременно възможности и заплахи. Най-скорошният пример за тези процеси е пандемичното разпространение на COVID-19, създавайки не само здравни, но и редица социални и икономически предизвикателства. В свой доклад, Организацията на обединените нации насърчава международната общност да се възползва от всяка възможност, с оглед прилагане на конкретни мерки, за да включи хората с увреждания в дневния си ред на глобалното развитие, тъй като темата засяга всички аспекти на съвремието. Освен това хората с увреждания са признати сред групите в неравностойно положение, за които напредъкът трябва да бъде наблюдаван с приоритет.

През 2015 г. се прие Програмата за устойчиво развитие на ООН до 2030 г. и нейните цели за устойчиво развитие, които изрично разглеждат въпросите, свързани с хората с увреждания в рамките на целите за устойчиво развитие, които да бъдат постигнати чрез образование, заетост и преодоляване на неравенствата. (United Nations, 2019).

През месец март 2021 г. Европейската комисия прие Стратегия за правата на хората с увреждания за периода 2021—2030 г. В нея Комисията оценява, че 50,8% от хората с увреждания са трудово заети в сравнение със 75% от хората без увреждания. ЕК също така отчита, че притежаването на подходящи умения и квалификации е предпоставка за достъп до пазара на труда и успех на него (Европейска комисия, 2021).

Със закон, приет от 41-ото Народно събрание на 26 януари 2012 г. Република България ратифицира Конвенция за правата на хората с увреждания. Съгласно член 27 от Конвенцията, държавата следва да гарантира и насърчава реализацията на правото на труд чрез създаване на възможности за трудова заетост и професионално израстване на хора с увреждания на пазара на труда, както и оказване на съдействие при намиране, придобиване, поддържане на и завръщане към трудова заетост.

В този период започна подготовката на най-сериозната реформа в областта на защита на личните данни след приемането на Конвенция 108 за защита на лицата при автоматизираната обработка на лични данни на Съвета на Европа от 28 януари 1981 г. На 6 април 2016 г. ЕС постигна съгласие за осъществяването на голяма реформа в областта на защитата на данните, като прие пакета за реформа на защитата на данните, включващ Общия регламент за защитата на данните, който заменя двадесет годишната Директива 95/46/ЕО („Директива за защита на данните") и Директивата за полицейското сътрудничество. От 25 май 2018 г. в Европейския съюз започва прилагането на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните, ОРЗД).

Същевременно, малките и средните предприятия продължават да изпитват трудности в прилагането на разпоредбите на ОРЗД. В първия си доклад, изготвен съгласно член 97 от ОРЗД, относно оценката и прегледа на Общия регламент относно защитата на данните, ЕК обръща специално внимание на възможностите и предизвикателствата за организациите, и по-специално за МСП.

Настоящото изследване има за цел да събере информация относно готовността на администраторите и обработващите лични данни да привлекат в своите екипи (да се доверят на) хора с увреждания при управлението на процесите им по обработване на лични данни.

На 28 януари 2021 г. на институционалната интернет страница на КЗЛД беше публикувана анкета, насочена към администраторите на лични данни от частния сектор. Целта на анкетата бе да се събере информация относно готовността на администраторите и обработващите лични данни да привлекат в своите екипи (да се доверят на) хора с увреждания. Събраните данни ще бъдат използвани за обосноваване нуждата от специфични 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.

ЦЕЛ НА ИЗСЛЕДВАНЕТО

Целта на анкетата е да се събере информация относно готовността на администраторите и обработващите лични данни да привлекат в своите екипи (да се доверят на) хора с увреждания при управлението на процесите им по обработване на лични данни.

Изследователската хипотеза, чието потвърждение се търси чрез проведеното проучване е: „прилагането на хоризонталната политика по защита на личните данни може да доведе до създаване на възможности за интегриране на хора със специфични умения на пазара на труда." В допълнение, ако хипотезата се потвърди, анкетата измерва до каква степен неформално обучение в областта на защитата на личните данни би могло да съдейства за изграждането на доверие към хората с увреждания от страна на работодателите, категоризирани като малки и средни предприятия.

Резултатите могат да послужат като основа за разработването на проектно предложение за подготовка на специфично обучителни съдържание в областта на защитата на личните данни. Сред специфичните цели на подобно проектно предложение биха били изграждане на капацитет за хора в неравностойно положение за справяне с предизвикателствата на единния европейски пазар, чрез разработване на програма за обучение за демонстриране на съответствие с Регламент (ЕС) 2016/679 и последващото насърчаване на тяхното социалното включване и мобилност на труда им на територията на Европейския съюз.

Анкетата има целева група – администратори и обработващи лични данни в частния сектор, тъй като съществуват редица нормативните изисквания пред публичния сектор за наемане на лица със специфични потребности.

Съгласно приетата с Решение № 957 на Министерския съвет от 23.12.2020 г. Национална стратегия за хората с увреждания 2021 - 2030 г. най-голямото предизвикателство в областта на политиката за правата на хора с увреждания е гарантиране на възможностите за работа и заетост на хората с увреждания, както и предоставяне на адекватна подкрепа за работещите и работодателите, предвид спецификата на тази част от работната сила.

През 2018 г. делът на изложените на риск от бедност или социално изключване хора с увреждания е 49,5 % – с 19,5 процентни пункта по-голям, отколкото при хората без увреждания, и с 20,7 процентни пункта над средното за ЕС.

Резултатите от реализирането на целенасочени усилия от страна на КЗЛД попадат изцяло в Приоритет 4: „Осигуряване на възможности за работа и заетост и подходящи условия на труд“ на Националната стратегия за хората с увреждания 2021 – 2030 г.

Съгласно член 3 на Закона за малките и средните предприятия категорията малки и средни предприятия включва предприятията, които имат: средносписъчен брой на персонала, по-малък от 250 души и годишен оборот, който не превишава 97 500 000 лв., и/или стойност на активите, която не превишава 84 000 000 лв. Малки предприятия са тези, които имат персонал, по-малък от 50 души и годишният им оборот не превишава 19 500 000 лв., и/или стойност на активите, която не превишава 19 500 000 лв. Най-многобройни от всички предприятия са тези, които могат да се категоризират като микропредприятия. Те имат средносписъчен брой на персонала, по-малък от 10 души и годишен оборот, който не превишава 3 900 000 лв., и/или стойност на активите, която не превишава 3 900 000 лв.

МЕТОД НА СЪБИРАНЕ НА ИНФОРМАЦИЯ

Видовете изследователски методи биват качествени и количествени. Конкретната изследователска хипотеза предполага количествено измерване на готовността на МСП за наемането на хора с увреждания. Поради липса на планирани финансови средства за осъществяване на проучвания в сферата на защита на личните данни, както и с оглед оптимизация на времето на участниците в проучването, същото се осъществява изцяло чрез количествено изследователски метод с предварително формулирани затворени въпроси с един отговор. Въпросникът съдържа контролни въпроси с оглед доказване искреността на предоставената информация.

Целта е да се постигне максимална яснота и еднозначност на предоставените отговори. Допълнителен елемент, на който се основава достоверността на данните е анонимността при предоставяне на отговорите.

Структура на анкетата: Анкетата съдържа 7 въпроса. Броят на въпросите с предварително формулирани отговори е 6. Анкетата съдържа и отворен въпрос, чиято цел е описване на уменията, квалификацията и качествата на служителя, чието занятие в структурата на МСП е подпомагане на процесите по защитата на лични данни.

Въпросите събират информация относно:

- Текущата организация на персонала, отговорен за спазването на правилата за защита на личните данни;
- Възможните подобрения на съществуващата организация;
- Необходимите умения на служителят/лицето, изпълняващ/о дейностите, свързани с обработването на лични данни и демонстриране на съответствието на тези дейности с разпоредбите на ОРЗД.

Период на събиране на информацията – 28 януари 2021 г. – 10 май 2021г.

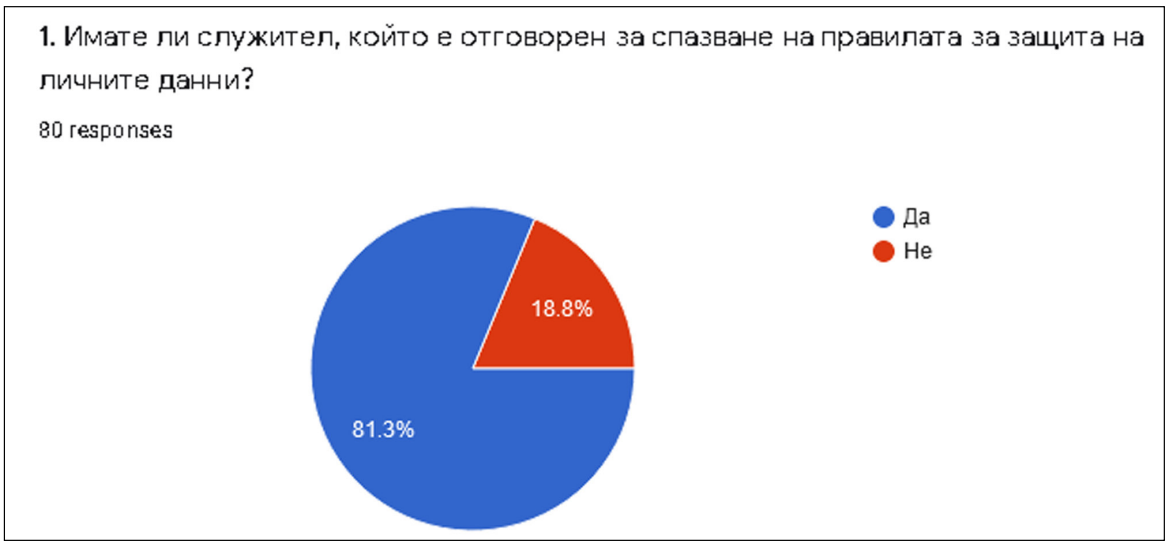
Целева група на проучването са малките и средните предприятия.

Брой попълнени анкети – 80

АНАЛИЗ НА СЪБРАНАТА ИНФОРМАЦИЯ

Анализът на събраната информация съдържа количествено описване и качествена проверка на изследователската хипотеза с опит за надграждане събраната информация 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.

81.3 % от анкетираните са заявили, че имат определен/ назначен служител, който е отговорен за спазването на правилата за защита на личните данни в техните предприятия. Под 1/5 от отговорилите не са вменили отговорностите по демонстрирането на съответствие с разпоредбите на ОРЗД на конкретен служител.



2/3 от определилите служител, който е отговорен за спазването на правилата за защита на личните данни в техните предприятия са уредили взаимоотношенията помежду си чрез трудов договор. 18,5% са сключили граждански договор с тези служители. Сред останалите възможности за регулиране на взаимоотношенията са договор за услуга, подписани декларации, допълнителни средства към основната заплата и вменени задължения в длъжностната характеристика, както и договор за изпълнение на длъжността „длъжностно лице по защита на данните“.

Съществен за проучването е отговорът на въпроса относно необходимостта от определяне на служител, отговорен за спазването на правилата за защита на личните данни, в случаите когато администраторът не е определил такъв към настоящия момент. 1/3 от участвалите малки и средни предприятия са заявили готовност да определят конкретен служител, натоварен с тези задачи.

С оглед потвърждаване или отхвърляне на формулираната хипотеза в изследването, към респондентите са отправени три конкретни въпроса относно физическото присъствие на служителите, техните специфични възможности, както и предпочитаната форма на заетост.

Близо 2/3 от анкетираните смятат, че не е необходимо физическо присъствие в помещенията, офисите и/или сградите на администратора. Над 2/3 (76,3%) от отговорилите биха се доверили на служител със специфични трудови умения, докато под 2/3 биха ангажирали външно лице със специфични потребности за изпълнение на дейности свързани с обработването на лични данни и демонстриране на съответствието на тези дейности с разпоредбите на Регламент (ЕС) 2016/679.

Участниците в изследването са поканени да споделят мнението относно уменията, които следва да притежава служителят/лицето, изпълняващо дейностите, свързани с обработването на лични данни, в съответствие с принципите и правилата на ОРЗД. В общия случай те оценят отговорността като висока, тъй като лицето трябва да има познания в сферата на нормативните актове, уреждащи дейността на администратора – Закона за защита на личните данни и Регламент (ЕС) 2016/679. Лицето трябва да е запознато с насоките на Европейския комитет за защита на данните и в същото време да познава много добре документооборота на дружеството. То следва да притежава познания относно класифицирането на данните като чувствителни и категориите, които трябва да бъдат защитени. Лицето, определено да подпомага администратора за защита на личните данни трябва да има експертиза и в областта на компютърните технологии, и в киберсигурността.

Откроява се желанието лицето да е с юридическо или техническо образование, със задълбочени познания в регулаторните практики и изисквания. Част от анкетираните споделят, че почти не работят с физически лица. Служителите се занимават със защитата на лични данни паралелно с обичайната си дейност. Дори в тези случаи, респондентите правилно се ориентират, тъй като признават, че лични данни се обработват за целите на управлението на човешките ресурси. Администраторите очакват от служителите по защита на личните данни добро разбиране на бизнес модела на предприятието, както

и детайлно познаване на регулациите в сектора. Служителят трябва да е с изграден авторитет сред колегите си, за да бъде включван от самото начало в нови процеси, в които се предвижда обработване на лични данни.

Качествата могат да бъдат обобщени в три групи:

• **Лични качества** – креативност, подреденост, отговорност, прецизност към детайлите, работоспособност при динамични условия, комуникативност, лоялност и конфиденциалност при изпълнение на служебните задължения, самостоятелност, независимост, прецизност, способност за работа под напрежение, убедителност, отзивчивост и нагласа за работа в екип, професионализъм, критичност и лоялност;

• **Компетенции**, най-вече свързани с доброто познаване и тълкуване на нормативната уредба в областта на защита на личните данни – Регламент (ЕС) 2016/679, както и българските закони; много добро познаване бизнес процесите на администратора и спецификата на дейността му;

• **Умения** – добри компютърни умения, компютърна грамотност, определено ниво на образование и ръководен опит, аналитични познания, както и познания за приложими бизнес модели, вкл. за структурата и организацията на администратора, организационни умения, умения за работа с хора и класифицирана информация, способност да разбира правни текстове.

Част от анкетираните споделят мнение, че лицето не следва да изпълнява и повече от разписаните задачи на длъжностното лице по защита на данните в Общия регламент относно защитата на данните, което налага необходимостта от добро познаване на Регламент (ЕС) 2016/679, Закона за защита на личните данни, препоръките на бившата Работна група по чл. 29 и насоките на Европейския комитет по защита на данните, процесите в организацията, добри познания в ИТ и административните дейности в компанията, познания за оценка на риска и въздействието, най-общо познаване на нормативната уредба и вътрешните регулации в сектора на администратора. Продължаваща тенденция е очакването за юридическо и/или техническо образование.

Открояват се секторни очаквания като уменията за работа с документи, договори, както и специфични умения за администриране на проектна документация. Изисква се също и професионална теоретична подготовка и практически опит в областта на защитата на личните данни. Познаването на дейността на администратора е един от често срещаните отговори, което показва важността на развитие именно на това познание в служителя или външния експерт. Като минимум се посочват изискванията на чл. 37 от ОРЗД, за да може служителят да изпълнява задачите на ДЛЗД, посочени в чл. 39. Познаването на нормативната база и непрекъснато осведомяване за промени, както в дейностите на фирмата, така и с работата на служителите в нея, както и бързото адаптиране в нова организация са сред желаните умения за служителите и външните експерти по защита на данните в МСП.

ИЗВОДИ

Независимо от ограничения брой участници в анкетата, могат да се приложат изследователски методи, които да спомогнат за извеждането на съотносими към групата на МСП заключения. Съществуват множество изследователски методи. Сред тях е и екстраполацията. Този метод би спомогнал за разглеждане на тенденции и модели. В общия случай, взаимоотношенията в минал или настоящ момент служат за описване на състоянието на обекта на изследване в бъдещ момент. Като принадлежащ към формализираната група, за екстраполацията съществуват и някои ограничения. Например, изследваният обект трябва да се развива по същия начин. С други думи, за да се приложи към настоящото изследване е необходимо допускане – администраторите няма да променят във времето очакванията си към служителите или външните лица, подпомагащи ги в управление на процесите по обработване на лични данни. За целите на изследването ще се приложи ретроспективна екстраполация.

Към 25 май 2018 г. в електронната система за регистрация на АЛД (еРАЛД) са вписани 297 751 администратора на лични данни (Комисия за защита на личните данни, 2018).

Според официални данни на Националния статистически институт през 2019 г. в Република България има 419 681 нефинансови предприятия, като само 759 от тях могат да се категоризират в групата на големите предприятия по брой на персонала. (Национален статистически институт, 2020).

Ако 18.8% от всички МСП нямат служител или външно лице, отговарящо за процесите по обработване на личните данни, то абсолютната стойност на броя им към настоящия момент би била между 55 977 и 79 800 малки и средни предприятия.

Ако 33.3% от неопределилите служител, биха желали да определят служител или външно лице, отговарящ за процесите по обработване на личните данни, то абсолютната стойност на броя им към настоящия момент би била между 18 640 и 26 273 малки и средни предприятия.

Ако 76.3% от МСП, които биха желали да определят служител или външно лице, отговарящ за процесите по обработване на личните данни, имат готовност да наемат лице с увреждания, то абсолютната стойност на броя им към настоящия момент би била между 14 222 и 20 046 предприятия.

Ако 60% от МСП, които биха желали да определят служител или външно лице, отговарящ за процесите по обработване на личните данни, имат готовност да ангажират външно лице със специфични умения, то броят на тези предприятия би бил между 11 184 и 15 763.

Общо разбиране на анкетираните е, че в Република България трудно се намират кадри, а още по-трудно се привличат служители с експертни познания по защита на данните. От създадения профил на желания служител/ външен експерт въз основа на описаните лични качества, компетенции и умения е видно, че всяко лице със специфични потребности, желаещо да повиши своята квалификация и познания в сферата на защита на неприкосновеността на личния живот и лични данни, би могло да се реализира успешно на трудовия пазар.

В заключение, броят на администраторите на лични данни, категоризирани като малки и средни предприятия, които биха наели служител и/или външен експерт със специфични потребности (например намалена трудоспособност) варира между 11 184 и 20 046 предприятия.

Следователно, интеграцията на хора със специфични потребности би могла да бъде опосредствана от специално обучение в сферата на защита неприкосновеността на личния живот и на личните данни. Обучителни модули следва да бъдат разработени от Комисията за защита на личните данни в сътрудничество с работодателски организации и асоциации на МСП и хора със специфични потребности.

ЦИТИРАНИ ИЗТОЧНИЦИ

United Nations. (2019). *Disability and Development Report*. New York: United Nations Publications.

Европейска комисия. (2021). *Съюз на равенство: Стратегия за правата на хората с увреждания за периода 2021 - 2030 г.* Брюксел: Европейска комисия.

Комисия за защита на личните данни. (2018). *Годишен отчет на Комисията за защита на личните данни за 2018 г.* София: Комисия за защита на личните данни.

Национален статистически институт. (30 11 2020 г.). *https://www.nsi.bg/*. Изтеглено на 10 06 2021 г. от https://www.nsi.bg/: https://www.nsi.bg/bg/content/8212/%D0%B1%D1%80%D0%BE%D0%B9-%D0%BD%D0%B0-%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D1%80%D0%B8%D1%8F%D1%82%D0%B8%D1%8F%D1%82%D0%B0

Комисия за защита на личните данни
Председател: Венцислав Караджов
Членове: Цанко Цолов
Мария Матева
Веселин Целков

Информационен бюлетин № 6 (93) 2021 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Уеб сайт на КЗЛД: www.cpdp.bg
Разпространява се в електронен вид

ISSN 2367-7759