Комисия за Защита на Личните Данни

ИНФОРМАЦИОНЕН БЮЛЕТИН

Брой 4 (85), юли 2020 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода май и юни 2020 г.)

44-ТО НАРОДНО СЪБРАНИЕ ПРИЕ ГОДИШНИЯ ОТЧЕТ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ЗА 2019 Г.

На 11.07.2020 г. Народното събрание прие Годишния отчет за дейността на Комисията за защита на личните данни за 2019 година. Отчетът е депозиран в Народното събрание на 31.03.2020 г. съгласно чл. 7, ал. 6 от Закона за защита на личните данни. На 03.06.2020 г. е приет с пълно единодушие на редовно заседание на Комисията по вътрешна сигурност и обществен ред, която в своето становище пред Народното събрание представи накратко основните моменти от годишния отчет.

В становището е подчертано, че 2019-та година се характеризира с три значими предизвикателства пред Комисията за защита на личните данни, с които тя успешно се е справила - първо, актуализиране на законовата и подзаконовата правна рамка в областта на защита на личните данни в Република България, на второ място, промяна във фокуса на контролната дейност и на трето място, продължаването на практическото прилагане на новата правна рамка в областта на защита на личните данни, по-специално, Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. (Регламентът) и отмяна на Директива 95/46/ЕО (Регламент (ЕС) 2016(689). В становището на Комисията по вътрешна сигурност и обществен ред е изтъкната засилената информационна дейност на КЗЛД по ключови въпроси от обществен интерес, както и във връзка с прилагането на регламент (ЕС) 2016/679. Подчертано е институционалното взаимодействие на КЗЛД.

Народните представители бяха запознати с контролната дейност на КЗЛД, част от която е извършването на проверки на националните звена на Европол, Евродак и Интерпол, както и на Шенгенската информационна система в Националното бюро СЕРЕНЕ към дирекция „Международно оперативно сътрудничество“ на МВР и консулски служби в посолства на Република България. Представена бе информация за резултати от проведени разследвания, разглеждане на жалби от физически лица, наложени имуществени санкции и глоби.

Предложението на Комисията по вътрешна сигурност и обществен ред бе Народното събрание да вземе решение за приемане на Годишния отчет на КЗЛД за 2019 г. С готовност да отговарят на въпроси на народни представители, в залата присъстваха председателят на КЗЛД – Венцислав Караджов и главният секретар – Десислава Тошкова.

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

КЗЛД ПРЕДОСТАВИ НА НАРОДНОТО СЪБРАНИЕ И НА ЕВРОПЕЙСКАТА КОМИСИЯ ЕЖЕГОДНАТА ИНФОРМАЦИЯ В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА НА ЗЕС

В изпълнение на разпоредбата на чл. 261а, ал. 5 от Закона за електронните съобщения (ЗЕС) ежегодно, до 31 май, Комисията за защита на личните данни предоставя на Народното събрание и на Европейската комисия обобщена статистическа информация за предходната календарна година относно случаите на предоставяне на трафични данни на компетентните органи за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления, както и за осъществяване на операции по издирване и спасяване на лица. Информацията се изготвя въз основа на постъпилите данни от предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, относно:

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

По данни от Публичния регистър на предприятията, уведомили Комисията за регулиране на съобщенията за намеренията си да осъществяват обществени електронни съобщения (чл.33, ал.1, т.1 от ЗЕС), броят на предприятията към 21.04.2020 г. е **1125.**

През 2019 г. **99** предприятия са подали в КЗЛД ежегодна статистическа информация, като 26 предприятия информират за приблизително 48 000 случая на поискана от тях информация за трафични данни. Както и през предходните години, броят на предприятията, предоставили на КЗЛД ежегодна статистическа информация, не съответства на общия брой задължени субекти. Тази трайна тенденция би могла да се обясни с разбирането на задължените предприятия, че законовото им задължение възниква единствено при наличие на конкретни искания за достъп до информация през отчетната година.

През 2019 г. се запазват следните тенденции:

- Случаите на поискана и непредоставена информация са под 1 %. Може да се приеме, че системата за предоставяне на достъп до трафични данни за целите на националната сигурност и борбата с престъпността работи ефективно.
- Случаите на поисканата и предоставена информация за услугата „Данни относно мобилни мрежи или услуги“ са доминиращи в сравнение с другите видове услуги.
- Повечето от исканията (64 %) са за време на задържане „0-3 месеца“. Време на задържане е периодът, изминал от датата на запазване на данните до датата на поисканото предаване на тези данни.

През предходната 2019 г., в рамките на румънското и финландското председателство на Съвета на ЕС, продължи обсъждането на темата, свързана със съхранението на трафичните данни и предложението за ePrivacy Regulation - Регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО. Коментирана е възможността основанията за законосъобразното обработване на трафични данни да бъдат максимално в съответствие с изискванията на Общия

регламент, дори да ги надградят. Прието е, че не бива да се допуска по-ниско ниво на защита на правата на физическите лица, с оглед на конкретната хипотеза на обработване.

Съветът на ЕС акцентира върху важността на следното:

• Съхранението на трафичните данни е основен инструмент за правоприлагащите, съдебните и други компетентни органи, чиято цел е ефективното разследване на тежки престъпления, като например тероризъм и киберпрестъпления.

• Използването на такъв тип данни и други подобни мерки трябва да почиват преди всичко на защитата на основните права на физическите лица.

• Законодателните реформи на европейско ниво, в това число и бъдещият Регламент за неприкосновеността на личния живот и електронните съобщения, трябва да предвиждат правната възможност за въвеждането на схеми за съхранение на данни, които да отчитат бъдещото развитие на технологиите и да са в съответствие с Хартата на основните права на ЕС.

Отчита се изключителната им важност на съхранението на трафични данни за успешното разследване на престъпления (като тероризъм и киберпрестъпления) от страна на компетентните правоприлагащи органи. Във връзка с това, както и с необходимостта от осигуряване на сигурността на данните на физическите лица, е важно да се въведат задължения за телекомуникационните оператори и доставчици на услуги относно съхранението на трафични данни. Те трябва да са пропорционални, доказано необходими и прозрачни, както и да защитават основните права на физическите лица – право на лична неприкосновеност, на защита на личните данни, недопускане на дискриминация и презумпция за невинност.

ДВЕ ГОДИНИ ОТ НАЧАЛОТО НА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ

На 25 май 2020 г. се отбеляза втората годишнина от прилагането на Общия регламент относно защитата на данните, широко известен като GDPR. Регламентът е единен набор от правила на законодателството на ЕС, пряко приложим в държавите-членки на Съюза. В рамките на изминалите две години той се превърна в качествено нов еталон, по който се работи с лични данни в ЕС, и се утвърди като „златен стандарт" на глобално ниво в областта на поверителността.

Европейският съюз се стреми да запази челна позиция в сферата на защитата на личните данни в условията на цифровата трансформация на обществото и световната икономика. Данните са ценен елемент на цифровата икономика и играят все по-важна роля за разработването на иновативни системи. От съществено значение е да се създаде среда за реализиране на технологичната революция при пълно зачитане на правата на хората. Регламентът създава среда за разработване на заслужаващи доверие иновации, като гарантира, че гражданите имат по-голям контрол върху личните си данни и са все по-добре осведомени за своите права. На предприятията Регламентът предоставя възможности да извлекат максимална полза от цифровите трансформации, като същевременно гарантира доверието на гражданите. Извън Европа той създава възможности за насърчаване на потоци от данни въз основа на високи стандарти между държави, споделящи ценностите на ЕС. Все повече държави по цял свят приемат правила за защита на данните, като използват стандарта на ЕС в тази област като отправна точка. Това сближаване открива нови възможности за безопасни потоци от данни между ЕС и трети държави.

На 24 юни 2020 г., малко повече от две години от влизането в сила на Общия регламент относно защитата на данните (ОРЗД), **Европейската комисия публикува доклад за преглед и оценка на резултатите от изпълнението му.** В Регламента се предвижда първият такъв доклад да се извърши 2 години след началото на прилагането му, както и на всеки четири години след това. В доклада се отчита, че Регламентът е постигнал повечето от своите цели, най-вече като е осигурил силен набор от приложими права за гражданите и е създал нова европейска система за управление и правоприлагане. Прави се заключението, че хармонизацията между държавите членки се увеличава. Констатира се, че предприятията развиват култура на спазване на изискванията и все повече използват силната защита на данните като конкурентно предимство. Докладът съдържа списък с действия за улесняване на прилагането на Регламента за всички заинтересовани страни, особено за малките и средните предприятия, за насърчаване и по-нататъшно развитие на истинска европейска култура за защита на данните и за стриктно прилагане на правилата.

Вера Йоурова, заместник-председател на Европейската комисия, отговарящ за ценностите и прозрачността, заявява: „*Европейският режим за защита на данните се превърна в ориентир, който ни води в насочените към човека цифрови трансформации и е важен стълб, върху който изграждаме други политики, като стратегията за данните или подхода си към изкуствения интелект. Общият регламент относно защитата на данните е отличен пример за това как чрез подход, базиран на основните права, Европейският съюз предоставя възможности на своите граждани и позволява на предприятията да се възползват максимално от цифровата революция. Всички ние обаче трябва да продължим работата си, за да направим така, че ОРЗД да достигне пълния си потенциал.*“

Комисарят по въпросите на правосъдието **Дидие Рейндерс** заяви: „*Общият регламент относно защитата на данните успешно изпълни целите си и се превърна в световен модел за държавите, които искат да предоставят на своите граждани високо равнище на защита. Можем обаче да постигнем още по-добри резултати, както го показва днешният доклад. Например, нуждаем се от повече единство в прилагането на правилата в Съюза: това е важно за гражданите и за предприятията, особено за МСП. Необходимо е също така да гарантираме, че гражданите се възползват в пълна степен от правата си. Комисията ще проследява напредъка в тясно сътрудничество с Европейския комитет по защита на данните и при редовния си обмен на информация с държавите членки, така че ОРЗД да може да разгърне пълния си потенциал.*“

В публикуваното от Европейската комисия прессъобщение са резюмирани **основните констатации от прегледа на Регламента**:

• **Гражданите разполагат с повече възможности и са по-осведомени за правата си:** Общият регламент относно защитата на данните повишава прозрачността и предоставя на физическите лица упражняеми права, като правото на достъп, коригиране, заличаване, правото на възражение и правото на преносимост на данните. Според резултатите, публикувани миналата седмица в проучване на Агенцията на ЕС за основните права, понастоящем 69 % от населението в ЕС на възраст над 16 години са чували за ОРЗД, а 71 % от хората са чували за националния си орган за защита на данните. Може обаче да се направи повече, за да се помогне на гражданите да упражняват правата си, особено правото на преносимост на данните.

• **Правилата за защита на данните са адаптирани за цифровата ера:** ОРЗД предоставя правомощия на хората да играят по-активна роля по отношение на това, което се случва с данните им в цифровия преход. Той допринася и за насърчаване на надеждни иновации, по-конкретно чрез основан на риска подход и принципи като защита на данните на етапа на проектирането и по подразбиране.

• **Органите за защита на данните използват своите по-големи корективни правомощия:** От предупреждения и порицания до административни глоби − ОРЗД предоставя на националните органи за защита на данните подходящи инструменти за прилагане на правилата. Те обаче трябва да получат адекватна подкрепа с необходимите човешки, технически и финансови ресурси. Много държави членки правят това, като значително увеличават бюджетните кредити и броя на персонала. Като цяло между 2016 г. и 2019 г. беше увеличен персоналът с 42 %, а бюджетът с 49 % за всички национални органи за защита на данните в ЕС взети заедно. Въпреки това все още съществуват значителни различия между държавите членки.

• **Органите за защита на данните работят заедно в рамките на Европейския комитет по защита на данните (ЕКЗД), но има възможност за подобрение:** С ОРЗД беше създадена иновативна система за управление, имаща за цел да гарантира последователно и ефективно прилагане на ОРЗД чрез т.нар. „обслужване на едно гише“, което предвижда, че дружество, извършващо трансгранична обработка на данни, контактува само с един орган за защита на данните, а именно органа на държавата членка, в която се намира основното му място на установяване. Между 25 май 2018 г. и 31 декември 2019 г. бяха подадени 141 проекта за решения чрез „обслужването на едно гише“, 79 от които доведоха до окончателни решения. Може обаче да се направи повече, за да се развие истинска обща култура в областта на защитата на данните. По-конкретно, обработването на трансгранични случаи изисква по-ефективен и хармонизиран подход и ефективно използване на всички инструменти, предвидени в ОРЗД, за да могат да си сътрудничат органите за защита на данните.

• **Съвети и насоки от страна на органите за защита на данните:** ЕКЗД издава насоки, обхващащи ключови аспекти на Регламента, както и по нововъзникващи въпроси. Няколко органи за защита на данните създадоха нови инструменти, включително горещи телефонни линии за оказване на помощ на физически лица и предприятия, както и инструменти за малките предприятия и микропредприятията. От съществено значение е да се гарантира, че насоките, предоставени на национално ниво, съответстват напълно на насоките, приети от ЕКЗД.

• **Използване на пълния потенциал на международното предаване на данни:** През последните две години международната ангажираност на Комисията в областта на свободното и безопасно предаване на данни доведе до важни резултати. Това включва Япония, с която ЕС вече споделя най-голямата в света зона на свободно и безопасно движение на данни. Комисията ще продължи работата си относно адекватното ниво на защита на данните с партньорите си по света. Освен това Комисията в сътрудничество с ЕКЗД се стреми към модернизиране на други механизми за предаване на данни, включително стандартните договорни клаузи, най-широко използваното средство за трансфер на данни. ЕКЗД работи по конкретни насоки относно използването на сертифицирането и кодексите за поведение за предаването на данни извън ЕС, като насоките трябва да бъдат финализирани възможно най-скоро. Като се има предвид, че Съдът на Европейския съюз може да предостави разяснения в решение, което ще бъде постановено на 16 юли и което може да е от значение за някои елементи на стандарта за адекватност на защитата на данните, Комисията ще докладва отделно относно съществуващите решения за адекватното ниво на защита, след като Съдът постанови решението си.

• **Насърчаване на международното сътрудничество:** През последните две години Комисията засили двустранния, регионалния и многостранния диалог, като насърчи глобална култура на зачитане на неприкосновеността на личния живот и сближаването между различните системи за неприкосновеност на личния живот в полза както на гражданите, така и на предприятията. Комисията се ангажира да продължи тази работа като част от по-широкообхватните си външни действия, например в контекста на партньорството между Африка и ЕС и в подкрепата си за международни инициативи, като „свободното движение на данни, основано на доверие“. В момент, когато нарушенията на правилата за защита на неприкосновеността на личния живот могат да засегнат много хора едновременно в различни части на света, е време да се засили международното сътрудничество между правоприлагащите органи в

областта на защитата на данните. Ето защо Комисията ще поиска разрешение от Съвета да започне преговори за сключване на споразумения за сътрудничество и взаимопомощ със съответните трети държави.

Пълният текст на доклада за преглед и оценка на Общия регламент относно защитата на данните е публикуван **ТУК**.

РЕЗУЛТАТИ ОТ ПРОВЕДЕНА АНКЕТА СРЕД ДЛЪЖНОСТНИТЕ ЛИЦА ПО ЗАЩИТА НА ДАННИТЕ В ПУБЛИЧНИЯ СЕКТОР

На 28 януари 2020 г., в Деня за защита на личните данни, КЗЛД стартира проучване под формата на онлайн анкета, насочена към длъжностните лица по защита на данните (ДЛЗД) в публичния сектор. Анкетирането приключи на 18.05.2020 г., а анализът на резултатите бе изготвен в края на месец май 2020 г., по повод 2 години Общ регламент относно защитата на данните.

Анкетата бе напълно анонимна и целта ѝ бе да обобщи опита, позицията и изпълнението на функциите на ДЛЗД в публичния сектор. Механизмът на анонимното анкетиране е доказано ефективен за събиране на информация и получаване на обективна картина по конкретна тема, обект на изследване. Съдържанието на анкетата бе адаптирано за конкретните дейности и правоотношения, характерни за администратори от публично-правния спектър, като въпросите бяха ориентирани както към количествени параметри, така и към качествения аспект на работата на ДЛЗД.

Чрез своя институционален сайт КЗЛД предостави достъп до анкетата и призова ДЛЗД от публичния сектор да участват в проучването, като със съвестно, добронамерено и обективно предоставяне на информация и изразяване на мнение дадат своя принос в усилията да се дефинират евентуални проблеми и да се предприемат действия за справянето с тях.

В анкетата на КЗЛД участваха 166 длъжностни лица. Като се има предвид, че 1500 администратори от публичния сектор за подали уведомление в КЗЛД за определено ДЛЗД, а определянето на такова в публичните органи е задължително, може да се направи изводът, че около 10% от ДЛЗД в публичния сектор са участвали в анкетата. Въпреки че процентът на участие не може да формира представителна извадка, резултатите бяха внимателно анализирани и бяха направени съответните изводи:

Повечето участвали в анкетата са ДЛЗД в организации с над 100 служители, а самите те са част от персонала на организацията, като изпълняват и други функции, освен като ДЛЗД. При изследване на нагласата в по-малките администратори (до 50 човека) за определяне на външно за организацията ДЛЗД, се налага изводът, че **съвместяването е по-разпространено сред малките организации.**

За около 40% от изпълняващите и други функции ДЗЛД, реалното време, в което са ангажирани като длъжностни лица по защита на данните е не повече от 1 - 1,5 часа на ден от работното им време. Резултатите от проучването относно отделяното време за работа като ДЛЗД показват, **че съвместяването на длъжността в малките организации води до по-малко време за изпълнение на задачите на ДЛЗД**.

Почти всички ДЛЗД изпълняват основния обем от по-важни задачи, които стоят пред тях, но все още не са разпознаваеми от другите служители в организацията, като лице, към което следва да се обръщат по въпросите за защита на данните. Налага се изводът, че **колкото е по-голяма организацията, толкова по-малко е разпознаваемо ДЛЗД**.

ДЛЗД в организации до 50 човека информират и съветват ограничено своите колеги и ръководството на организацията. Прави впечатление високият процент на отговори относно изпълнението на задачи, които ДЛЗД би следвало само да консултират. Обичайна е практиката ДЛЗД да бъде ангажирано и със задължения, които не са изрично определени за неговата функция, но по принцип попадат в сферата на защита на данните. Приблизително 25% от анкетираните посочват, че са изправени пред натиск от ръководството, 40% не действат в условията на независимост, 25 % са попадали в конфликт на интереси. Над 75% са считани за „отговорници“ за осигуряването на съответствие със законодателството за защита на данните в организацията. Тези резултати налагат извода, че е необходимо **засилване на информираността относно задачите на ДЛЗД, с акцент върху основните задачи на ДЛЗД**.

По-голямата част от ДЛЗД се ползват с доверието и подкрепата на ръководството, имат лесен контакт със същото и на тях се разчита за съответствието с Регламент (ЕС) 2016/679 и ЗЗЛД.

По-голямата част от анкетираните определят своите знания и опит (правни познания за изпълнение на задачите на ДЛЗД и опит в областта на информационните и комуникационните технологии) като достатъчни. Същото важи и за другите условия на труд – наличие на необходими ресурси, достатъчно свободно време за изпълнение на задачите на ДЛЗД, участие във всички въпроси, свързани със защитата на данните. Едновременно с това анкетираните изявяват желанието за допълнително обучение от страна на КЗЛД. Това налага изводът, че **базисното обучение за ДЛЗД от страна на КЗЛД ще е целесъобразно да се замени със специализирано по определени теми**.

Като определени против волята им се самоопределят 24 анкетирани, а 19 не желаят да отговорят на този въпрос.

Като основни фактори за успешното изпълнение на функциите като ДЛЗД, анкетираните категорично са посочили на първо място доверието и подкрепата на ръководството, а едва след това – професионалната квалификация и времето за изпълнение на задълженията като ДЛЗД.

Сред предложенията и очакванията на участвалите в анкета са

1. Определяне на някакво възнаграждение за функцията им като ДЛЗД (в случаите, когато изпълняват и други функции).

2. Повече обучения с практическа насоченост, с което да повишават своята квалификация.

3. Предоставяне от страна на КЗЛД на ръководства, указания, насоки, бланки, с които да се улеснява работата им.

В обобщение, от отговорите се налага един основен извод: **ДЛЗД масово смесват задълженията на администратора със своите собствени.** Въпреки високата самооценка за познания и подготовка**, очакват организирани обучения**. Създава се впечатление, че не търсят активно информация, като поставят акцент върху ролята на надзорния орган в информирането им. Същевременно, явно се приема, че КЗЛД ще може да предложи „бланкетни“ обучения и решения с предварително изготвена документация и решени казуси за всички публични органи, от което следва, че **не се отчита секторната специфика**. **При разработване на обучителни материали ще е целесъобразно да се мисли за модели за окуражаването на тяхната самоинициативност и информираност, включително и чрез платформи за информационен обмен.**

Събраната и анализирана информация ще послужи за планиране на бъдещите превантивни и подпомагащи дейности на Комисията за защита на личните данни.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ

През юни 2020 г. Европейският комитет по защита на данните прие Изявление относно влиянието върху защитата на данните в резултат на оперативната съвместимост на приложенията за проследяване на контакти, Изявление относно обработването на лични данни в контекста на отварянето на границите в условията на COVID-19 и Изявление относно ограничаване на правата на субектите на данни в случаи на извънредното положение в държавите-членки.

Комитетът прие Изявление относно влиянието върху защитата на данните в резултата на оперативната съвместимост на приложенията за проследяване на контакти, основавайки се на своите Насоки 04/2020 относно използването на данни за местоположението и инструментите за проследяване на контакти в контекста на пандемията от COVID-19. Изявлението предлага по-задълбочен анализ на ключови аспекти, включително прозрачност, правни основания, контролиране, права на субектите на данни, запазване и минимизиране на данни, информационна сигурност и точност на данните в контекста на създаване на оперативно съвместима мрежа от приложения.

Комитетът подчертава, че споделянето с такива оперативно съвместими приложения на данни за хора, които са били диагностицирани или тествани с положителен резултат, трябва да се задейства само с доброволни действия на потребителя. Предоставянето на информация и контрол на субектите на данни ще увеличи доверието им в приложенията и потенциалното им използване. Целта на оперативната съвместимост не трябва да се използва като аргумент за разширяване на събирането на лични данни извън необходимото. Освен това приложенията за проследяване на контакти трябва да бъдат част от цялостна стратегия за обществено здраве за борба с пандемията.

В изявлението се посочва, че осигуряването на оперативна съвместимост е не само технически трудно и понякога невъзможно без непропорционални компромиси, но също така води до потенциален повишен риск за защитата на данните. Следователно администраторите трябва да гарантират, че мерките са ефективни и пропорционални и трябва да преценят дали същата цел не може да се постигне с по-малко натрапчива алтернатива.

Прието бе и **Изявление относно обработването на лични данни в контекста на отварянето на границите в условията на COVID-19**. Мерките, позволяващи безопасно отваряне на границите, предвидени или прилагани понастоящем от държавите-членки, включват тестване за COVID-19, изискване на сертификати, издадени от здравни специалисти, и използване на доброволно приложение за проследяване на контакти. Повечето мерки включват обработване на лични данни. Комитетът припомня, че законодателството за защита на данните остава приложимо и позволява ефективен отговор на пандемията, като същевременно защитава основните права и свободи. Обработването на лични данни трябва да бъде необходимо и пропорционално, а нивото на защита трябва да бъде еднакво навсякъде в Европейското икономическо пространство. В своето изявление Европейският комитет по защита на данните настоятелно призовава държавите-членки да предприемат общ европейски подход, когато решават кое обработване на лични данни е необходимо в този контекст.

Изявлението също така реферира към принципите на Регламент 2016/679 (GDPR), на които държавите-членки трябва да обърнат специално внимание при обработването на лични данни в контекста на отваряне на границите. Те включват законосъобразност, добросъвестност и прозрачност, ограничаване на целите, свеждане на данните до минимум, ограничаване на съхранението, сигурност на данните и защита на данните при проектиране и по подразбиране. Освен това решението за

разрешаване на влизането в дадена държава не трябва да се основава само на автоматизираните технологии за вземане на индивидуални решения. Във всеки случай подобни решения следва да бъдат обект на подходящи предпазни мерки, които трябва да включват специфична информация за субекта на данните и правото да се получи човешка намеса, субектът да изрази своята гледна точка, да получи обяснение на решението, прието след такава оценка и да оспори решението. Автоматизираните средства за вземане на индивидуални решения не трябва да се прилагат за деца.

Комитетът прие И**зявление относно ограничаване на правата на субектите на данни във връзка с извънредното положение в държавите-членки**, както и отговор на писмо на Съюза за граждански свободи за Европа. Комитетът припомня, че дори в тези изключителни времена защитата на личните данни трябва да се поддържа при всички спешни мерки, като по този начин допринася за спазването на всеобхватните ценности на демокрацията, върховенството на закона и основните права, на които е основан Съюзът. Както в изявлението, така и в писмото се подчертава, че GDPR остава приложим и позволява ефективен отговор на пандемията, като в същото време защитава основните права и свободи. Правилата за защита на данните дават възможност за операции по обработка на данни, необходими за принос в борбата срещу пандемията COVID-19.

Изявлението припомня основните принципи, свързани с ограниченията на правата на субектите на данни във връзка с извънредното положение в държавите-членки:

• Не могат да бъдат оправдани ограничения, които са общи, обширни или натрапчиви до степен, в която лишават основно право от неговото съдържание.

• При специфични условия член 23 от Регламент 2016/679 позволява на националните законодатели да ограничат чрез законодателна мярка обхвата на задълженията на администраторите и обработващите лични данни и правата на субектите на данни, когато такова ограничение зачита същността на основните права и свободи и е необходима и пропорционална мярка в демократичното общество за защита на важни цели от общ обществен интерес на Съюза или на държава-членка, каквото е по-специално общественото здраве.

• Правата на субектите на данни са в основата на основното право на защита на данните и член 23 от Регламент 2016/679 трябва да се тълкува и чете, като се има предвид, че тяхното прилагане трябва да бъде общо правило. Тъй като ограниченията са изключения от общото правило, те трябва да се прилагат само при ограничени обстоятелства.

• Ограниченията трябва да бъдат предвидени „по закон“ и законът за установяване на ограничения трябва да бъде достатъчно ясен, за да позволи на гражданите да разберат условията, при които администраторите имат право да прибягват до тях. Освен това трябва да са предвидими ограничения за лицата, които са техен обект. Ограниченията, наложени за непрецизирана във времето продължителност, които е прилагат със задна дата или са предмет на неопределени условия, не отговарят на критерия за предвидимост.

• Самото съществуване на пандемия или всяка друга извънредна ситуация сама по себе си не е достатъчна причина да се налага какъвто и да е вид ограничение на правата на субектите на данни. По-скоро всяко ограничение трябва ясно да допринася за защитата на важна цел от общ обществен интерес на ЕС или на държава-членка.

• Извънредното положение, прието в пандемичен контекст, е правно условие, което може да узакони ограниченията на правата на субектите на данни, при условие че тези ограничения се прилагат само доколкото са строго необходими и пропорционални, за да се защити целта за обществено здраве. Следователно, ограниченията трябва да бъдат строго ограничени по обхват и във времето, тъй като правата на субекта на данните могат да бъдат ограничени, но не и отказани. Освен това гаранциите, предвидени в член 23, параграф 2 от Регламента, трябва да се прилагат изцяло.

• Без ясно изразено ограничение във времето, ограниченията, приети в условията на извънредно положение, спиращи или отлагащи прилагането на правата на субекта на данни, както и задълженията

на администраторите и обработващите лични данни, биха се равнявали на действително суспендиране на тези права и не са съвместими със същността на основните права и свободи.

Комитетът прие отговор на писмо от евродепутата Мориц Кьорнер относно **значимостта на забраните за криптиране в трети страни при извършване на оценка на нивото на защита на данните**, в случаи на прехвърляне на лични данни в страни, където тези забрани съществуват. Според Комитета всяка забрана за криптиране или разпоредби, отслабващи криптирането, сериозно биха довели до недостатъчно спазване на задълженията за сигурност на GDPR, приложими към администраторите и обработващите, независимо от това дали са в трета страна или в ЕИП. Мерките за сигурност са един от елементите, които Европейската комисия трябва да вземе предвид, когато оценява адекватността на нивото на защита в трета страна.

Комитетът прие отговор на членове на Европейския парламент във връзка с **използването на приложението за лицево разпознаване Clearview AI** от органите на реда. Комитетът споделя притесненията си относно някои разработки в технологиите за разпознаване на лица и припомня, че съгласно Директива за защита на личните данни в полицейската и наказателната дейност (Директива (ЕС) 2016/680) правоприлагащите органи могат да обработват биометрични данни с цел еднозначно идентифициране на физическо лице само в съответствие със строгите условия на членове 8 и 10 от Директивата. Комитетът изразява съмнение дали някое законодателство на Съюза или на държавите-членки предоставя правно основание за използване на услуга, като тази, предлагана от Clearview AI. Следователно, както съществува и без да се засяга някакво бъдещо или предстоящо разследване, не може да се установи със сигурност законността на такава употреба от правоприлагащите органи на ЕС. Без да се засяга по-нататъшен анализ въз основа на предоставени допълнителни елементи, Комитетът е на мнение, че използването на услуга като Clearview AI от органите на реда в Европейския съюз, вероятно няма да съответства на правилата за защита на данните в ЕС. Европейският комитет по защита на данните се позовава на своите насоки относно обработването на лични данни чрез видео устройства и обявява предстояща работа по използването на технологията за разпознаване на лица от органите на реда.

Комитетът прие отговор на отворено писмо от NOYB (Европейски център за цифрови права - организация с нестопанска цел) **относно сътрудничеството между надзорните органи и процедурите за съгласуване**. Комитетът посочва, че работи непрекъснато върху подобряването на сътрудничеството между надзорните органи и процедурите за съгласуваност, както и че е наясно за съществуването на проблеми, изискващи подобрение, като например различията в националните административно-процесуални закони и практики, както и времето и ресурсите, необходими за решаване на трансгранични дела. Комитетът заявява, че е ангажиран с намирането на решения, когато те са в неговата компетентност.

Европейският комитет по защита на данните **реши да създаде работна група**, която да координира потенциалните действия и да придобие по-изчерпателен преглед на обработката и практиките на социалната мрежа TikTok в ЕС. Стартирана през септември 2016 г., в момента платформата е водеща за споделяне на кратки клипове в Китай и става все по-популярна и в други страни, превръщайки се в едно от най-бързо развиващите се и изтегляни приложения. Главната ѝ аудитория са тийнейджъри. В отговор на искане на евродепутата Кьорнер относно TikTok, Комитетът посочва, че вече е издал насоки и препоръки, които трябва да се вземат предвид от всички администратори на данни, чиято обработка е предмет на GDPR, по-специално когато става въпрос за прехвърлянето на лични данни към трети страни, съществени и процедурни условия за достъп до лични данни от публичните органи или прилагането на териториалния обхват на GDPR, по-специално що се отнася до обработката на данни на непълнолетни лица. Комитетът припомня, че GDPR се прилага за обработването на лични данни от администратор, дори ако не е установен в Съюза, когато дейностите по обработка са свързани с предлагането на стоки или услуги на субекти на данни в Съюза.

Европейският комитет по защита на дните обяви, че ще публикува на своя уебсайт регистър, съдържащ решения, взети от националните надзорни органи в съответствие с процедурата за сътрудничество „едно гише“ (член 60 GDPR). Съгласно GDPR надзорните органи имат задължение да си сътрудничат по дела с трансграничен компонент, за да осигурят еднакво прилагане на Регламента - така наречения механизъм „едно гише“ („One-Stop-Shop“ - OSS). Съгласно този механизъм, водещият надзорен орган отговаря за изготвянето на проекторешенията и работи съвместно със засегнатите надзорни органи за постигане на консенсус. До края на април 2020 г. водещи надзорни органи приеха 103 окончателни решения по механизма „едно гише“. Комитетът възнамерява да публикува резюмета на английски език, подготвени от неговия секретариат. Информацията ще бъде публично достъпна след валидиране от съответния водещ орган и в съответствие с условията, предвидени в националното му законодателство.

РОЛЯТА НА ОБЩЕСТВЕНИТЕ СЪВЕТИ КЪМ УЧИЛИЩАТА И ДЕТСКИТЕ ГРАДИНИ

По повод постъпили въпроси относно фигурата на обществените съвети към училищата и детските градини от гледна точка на защитата на личните данни, чрез своя институционален сайт, както и в настоящия брой на бюлетина, КЗЛД предоставя подробни разяснения по тази тема.

Обществените съвети се създават на основание разпоредбите на Закона за предучилищно и училищно образование (ЗПУО). В чл. 265 от ЗПУО се посочва целта на функционирането на тези съвети: създаване на условия за активни и демократично функциониращи общности към всяка детска градина и всяко училище. Обществеият съвет е орган за подпомагане на развитието на детската градина и училището и за граждански контрол на управлението им, като условията и редът за създаването, устройството и дейността на обществения съвет се уреждат с Правилник, приет от министъра на образованието и науката (Правилник за създаването, устройството и дейността на обществените съвети към детските градини и училищата, Обн. ДВ, бр 75/2016 г.).

При анализ на нормативно регламентираните функции на Обществените съвети се установява, че по правило те изпълняват задачите си, без да се налага обработване на лични данни. Разбира се, по изключение, съобразно спецификата на конкретен случай, е възможно на членовете на Обществените съвети да станат известни лични данни във връзка с постъпили предложения, искания от родители, учители, ученици или съответното училищно ръководство.

Независимо от това обаче Обществеият съвет **няма** качеството на отделен администратор на лични данни по смисъла на дефиницията на понятието, разписана в чл. 4, т. 7 от Регламент (ЕС) 2016/679, доколкото обработването на такива данни не е предпоставка за изпълнение на неговите функции по закон. Обществеият съвет не събира и не съхранява лични данни, структурирани в регистър с лични данни за целите на своята дейност, а наличието на такъв регистър е абсолютно задължителна предпоставка за определяне на една или друга структура като администратор на лични данни.

В този смисъл Обществените съвети нямат и качеството на съвместни администратори на лични данни с училището/детската градина, към които са създадени.

Обществените съвети не са и обработващ лични данни, тъй като не обработват такива данни от името на администратора, а упражняват функциите си по закон напълно самостоятелно с възможност за упражняване на контрол върху дейността на образователната институция (вж. чл. 269 от ЗПУО). В отношенията администратор-обработващ контролът се осъществява от администратора.

При евентуална необходимост от достъп до лични данни за изпълнение на своите задължения, Обществените съвети се явяват трета страна – получател на данните. Необходимостта от обработването на данните, категориите лични данни и техния обем, както и целите, за които данните биха се

предоставили в конкретен случай на Обществените съвети, се определят от администратора на лични данни – училището или детската градина, към които са създадени. Този извод се подкрепя от чл. 16, ал. 2 от Правилника за създаването, устройството и дейността на обществените съвети към детските градини и училищата, който допуска Обществеият съвет да дава становища и по други въпроси по искане на директора, на педагогическия съвет, на регионалното управление на образованието или на съответния министър – първостепенен разпоредител с бюджет. Когато даването на становище предполага запознаване с лични данни, преценката за това до какви данни е необходимо да се осъществи достъпът и с какви изисквания за гарантиране на тяхната сигурност, остава отговорност на съответния администратор, който ги предоставя. В тази връзка е необходимо членовете на Обществените съвети да поемат задължение за неразгласяване на лични данни, станали им известни при изпълнение на функциите им на орган за подпомагане развитието на образователната институция и за граждански контрол на управлението й. Това може да стане с подписването на декларация в посочения смисъл, която да се съхранява от съответната образователна институция, към която са създадени. Освен това следва да се има предвид, че по силата на чл. 26 от Правилника за създаването, устройството и дейността на обществените съвети към детските градини и училищата „кореспонденцията и документите за дейността на обществения съвет се съхраняват в детската градина или училището на място, определено от директора“. Това изключва възможността обществените съвети да определят средствата за обработване и съхранение на личните данни, до които евентуално биха могли да имат достъп. Задължение е на администратора на лични данни (съответната образователна институция) да уреди във вътрешната си политика за защита на личните данни правилата, на които се подчинява достъпът на членове на Обществените съвети до лични данни и свързаните с това технически и организационни мерки за сигурност. В регистъра на дейностите по обработване, поддържан от съответното учебно заведение на основание чл. 30, пар. 1 от Регламент (ЕС) 2016/679, Обществените съвети следва да бъдат посочени като получател на данните, а субектите на данни (ученици, родители, педагогически и непедагогически състав) следва да бъдат информирани за това обстоятелство, с представяне в цялост и на информацията за параметрите на обработване по чл. 13 и чл. 14 от Регламента.

Важно е да се отбележи също така, че членовете на Обществените съвети се явяват субекти на данни, чиито данни образователните институции обработват. Те също имат право на информацията по чл. 13 и чл. 14 от Регламента по отношение обработването на тяхната лична информация.

Предвид горното, следва да се има предвид, че за евентуалното обработване на лични данни от страна на Обществените съвети не е необходимо уреждането на отношенията между тях и училищата да става с писмен договор или друг съвместен акт. Това не отменя изискването при предоставянето на конкретен достъп до лични данни, да се държи сметка за необходимостта и пропорционалността на предоставените данни, съобразно конкретните нормативно определени функции на Обществените съвети. Спазването на принципите за защита на личните данни е отговорност на съответната образователна институция.

КЗЛД многократно се е произнасяла по въпроси, свързани с разясняването на фигурите на администратор на лични данни, обработващ лични данни, както и съвместни администратори. На сайта на Комисията **www.cpdp.bg** може да се намери допълнително информация и становища по поставени подобни въпроси.

ПУБЛИКУВАН Е ТРЕТИ БРОЙ НА ИНФОРМАЦИОННИЯ БЮЛЕТИН ПО ПРОЕКТ SMEDATA

В края на месец юни 2020 г. беше публикуван третият брой на Информационен бюлетин по проект „SMEDATA: Осигуряване на най-висока степен на защита на неприкосновеността на личния живот и личните данни чрез иновативни инструменти за малки и средни предприятия и граждани“.

В бюлетина е предоставена информация за финалната версия на мобилното приложение „GDPR в твоя джоб“ – интегрирано дигитално решение за достъп до база данни с практика на националните надзорни органи на България и Италия и на съда на национално и европейско ниво, както и получената от КЗЛД награда в категорията „Публична администрация“ от конкурса „Наградите на БАИТ” за 2019 г. за същото приложение. Представени са следващите етапи от осъществяването на проекта, включително международната конференция по прилагането на Общия регламент относно защитата на данните от малките и средни предприятия.

Проектът цели предоставянето на практически инструментариум на малките и средните предприятия, за постигане на съответствие с Общия регламент относно защитата на данните, като стремежът е да се осигури най-висока степен на защита на неприкосновеността на личния живот и защита на личните данни чрез иновативни инструменти за СП и гражданите.

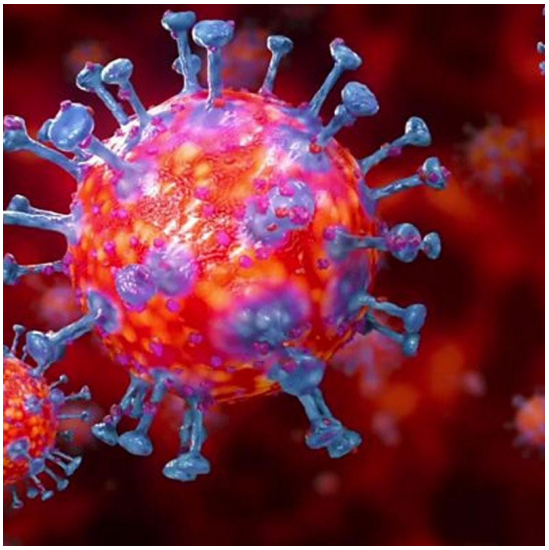
Комисията за защита на личните данни е координатор на проект „SMEDATA”, съфинансиран от Европейската комисия по Програма „Права, равенство и гражданство 2014 – 2020” на Европейския съюз. Партньори по проекта са Съюза на юристите в България, „Апис Европа”, EY България, Италианският орган по защита на данните, университетът „Roma Tre” и Европейската асоциация на жените юристи – клон България. Общият бюджет на проекта е 1 089 961,92 лева (557 288,68 евро), като е предвидено изпълнението му да приключи в края на ноември 2020 г.

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

КЗЛД ПРЕДПРИЕМА НЕОБХОДИМИТЕ МЕРКИ СРЕЩУ РАЗПРОСТРАНЕНИЕТО НА COVID-19

КЗЛД предприе редица технически и организационни мерки за защита на своите служители и на посетителите в сградата на институцията, съответстващи на мерките в национален мащаб за противодействие и превенция на коронавирус COVID-19.

Във връзка със Закона за изменение и допълнение на закона за здравето (обн. ДВ. бр.44 от 13 май 2020 г.) и решение № 325 на Министерския съвет от 14.05.2020 г. за обявяване на извънредна епидемична обстановка, считано от 14.05.2020 г. **в КЗЛД е създадена организация, гарантираща непрекъсваемост на работата на институцията в условията на пандемията от COVID-19**. Във връзка с Решение № 378 на Министерския съвет от 12 юни 2020 г. за удължаване на срока на обявената на 14 май 2020 г. извънредна епидемична обстановка, считано от 15.06.2020 г. същите мерки останаха в сила.



По отношение на пропускателния контрол са предприети следните мерки: охраната замерва телесната температура на всеки служител на КЗЛД и всеки посетител на сградата на КЗЛД (като напр. доставчици, куриери, участници в административни производства и други граждани-искатели на административни услуги на КЗЛД) и пропуска само лица, които нямат повишена телесна температура и нямат проява на остри респираторни болести (кашлица, хрема и др.). Осигурени са дезинфектанти, ръкавици и калцуни за всички посетители. В сградата на КЗЛД не се допускат външни посетители, които не носят маски. Допускането в сградата става само след като маската е поставена на лицето на външния посетител, извършена е дезинфекция на ръцете и са поставени ръкавици и калцуни. При влизането в сградата следва се спазват изискванията за недопускане на струпване на хора и спазването на дистанция от най-малко 1,5 м. Асансьорът може да се използва едновременно от не повече от две лица, носещи лични предпазни средства – маски.

При непосредствен контакт между служителите, както и между тях и външни посетители (обективна невъзможност за спазване на дистанция от поне 1,5 м., напр. при използване на стълбището в сградата, при ползване на асансьора), използването на маска за лице или предпазен шлем е задължително.

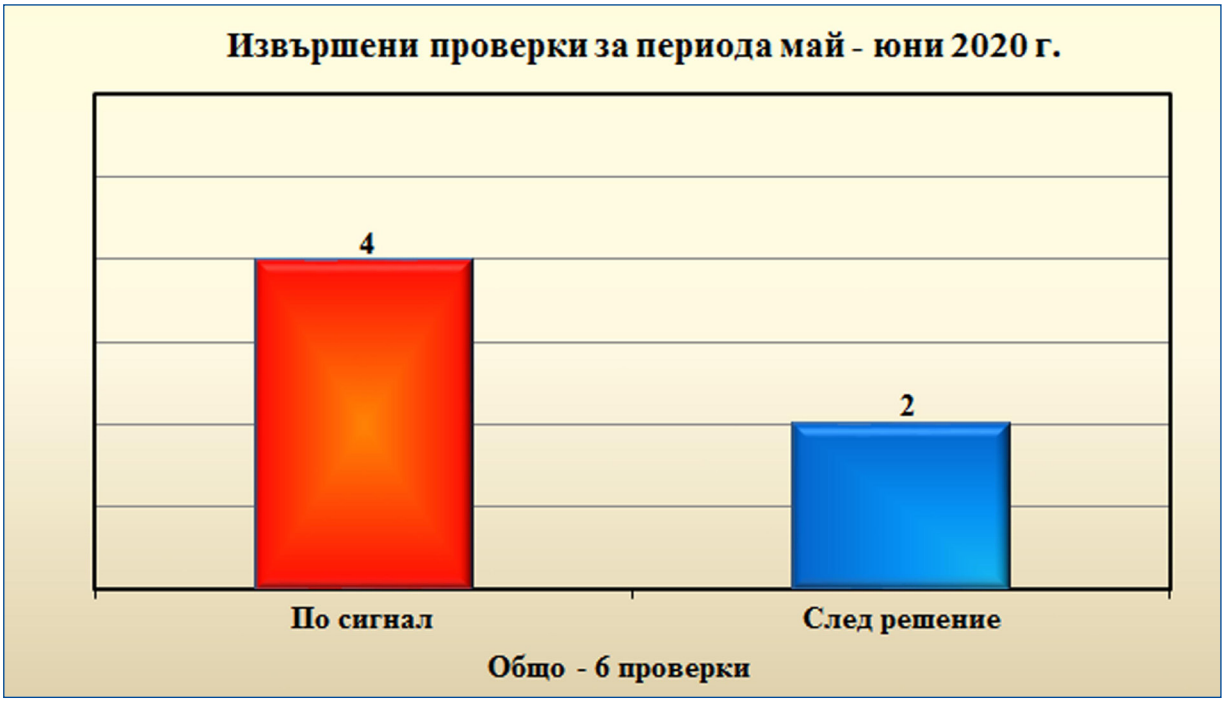
Избягва се предаването на документи от ръка на ръка. Документите се поставят на съответните за това места (напр. заседателна маса, на бюро, стол и др.), на максимално възможно разстояние от съответния друг (стоящ близо) човек при спазване на изискванията за дистанция от най-малко 1,5 м.

По принцип присъствието на страните по административните производства в откритите заседания на КЗЛД не е задължително. Граждани и организации, страни по административни производства, **които искат да присъстват на откритите заседания на КЗЛД**, изчакват пред сградата. Влизането в сградата и допускането в заседателната зала става след повикване от служител на КЗЛД, съобразно дневния ред на заседанието на Комисията за съответния ден. Когато метеорологичните условия не позволяват изчакване на открито, гражданите могат да бъдат допускани във фоайето на сградата, при спазване на всички мерки, въведени в КЗЛД, където изчакват да бъдат повикани в заседателната зала от служител на КЗЛД.

Извън описаните мерки, всички служители на КЗЛД и граждани, които са на територията на КЗЛД, следва да спазват стриктно и всички заповеди на министъра на здравеопазването, свързани с въведената на територията на страната извънредна епидемична обстановка, чиито предмет е относим към организацията на работа на КЗЛД и предоставяните от нея административни услуги.

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАЙ - ЮНИ 2020 г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците май и юни 2020 г. са извършени общо 6 проверки – 4 след постъпили в КЗЛД сигнали и 2 след решение на КЗЛД.



Разгледани са 142 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 съответния администратор на лични данни е издадено 1 Наказателно постановление.

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-01-272/2019 г.
София, 07.05.2020 г.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав, председател – Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на редовно заседание, проведено на 25.03.2020 г. и обективирано в протокол № 11/25.03.2020 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни (ЗЗЛД) във вр. с чл. 57, § 1, б. „е“ от Регламент (ЕС) 2016/679, разгледа по същество жалба с рег. № ППН-01-272/14.03.2019 г., подадена от П.Б._

Комисията за защита на личните данни е сезирана с жалба рег. № ППН-01-272/14.03.2019 г., подадена П.Б.

В жалбата е посочено, че нТ.О.4.03.2019 г. г-жа П.Б. е получила обаждане на личния си телефонен номер от г-н Г., който се представил за служител на ***телекомуникационен оператор (Т.О.)*** с искане, г-жа П.Б. да заплати задължения към Т.О.

Жалбоподателката твърди, че тормозът по телефона продължил с часове, като служителят разполагал с трите ѝ имена и телефонния номер.

П.Б. излага твърдения, че е прекратила договорните отношение с Т.О. през януари 2019 г.

В условията на залегналото в административния процес служебно начало и задължението на административния орган за служебно събиране на доказателства и изясняване на действителните факти от значение за случая, от ответните дружества е изискано да представят писмени становища и относими към случая доказателства.

С писмо изх. № ППН-01-272#3/08.11.2019 г. Т.О. е уведомено на основание чл. 26 от АПК за образуваното административно производство и е предоставена възможност за изразяване на становище и предоставяне на относими към случая доказателства.

В отговор от Т.О. е депозирано становище, заведено с рег. № ППН-01-272#4/21.11.2019 г., в което е посочено, че между г-жа П.Б. и Т.О. са били налице договорни отношение с договор № *** от 04.02.2017 г. за домашен интернет, телевизия и домашен телефон, а с приложение № 1 към същия договор от 14.08.2018 г. е сключен абонамент за услуга мобилен интернет. Посочено е, че услугите са ползвани и заплащани редовно до месец ноември 2018 г. от абоната, като след този момент абоната изпада в забава и за двете услуги, задълженията, за които се изчисляват в една фактура. Сочат, че следващото плащане на дължими суми е едва през април 2019 г., когато е върнато оборудването, предоставено на абоната за ползване на пакетната услуга. Като доказателство е предоставен системен екран, от който се виждат промените в платежното поведение.

От Т.О. сочат, че с цел събиране на задълженията, Т.О. ангажира услугите на ***финансова институция (Ф.И.),*** с което дружество имат сключен договор от 30.04.2013 г., като същото действа в

качеството на обработващ лични данни за администратора Т.О. От Т.О. информират, че дружеството Ф.И. обработва данните на г-жа П.Б. на същото основание, на което ги обработва администраторът Т.О., сключен договор за предоставяне на електронни съобщителни услуги.

От Т.О. сочат, че в компанията не са открити документи, които да потвърждават твърденията на жалбоподателката, че тя е заявила надлежно желание за прекратяване на договора за пакет - домашен интернет, телефон и телевизия. Твърдят, че и към настоящия момент потвърждение за такова прекратяване не е получено.

Информират, че с оглед клиентски ориентираната политика, при проведен през март 2019 г. разговор с жалбоподателката чрез линията за жалби и оплаквания, договорът за пакетната услуга е прекратен и на г-жа П.Б. са издадени кредитни известия за част от дължимите суми за услугата, след датата, на която г-жа П.Б. твърди, че е договорът е следвало да бъде прекратен.

От Т.О. молят Комисията да приеме, че данните на жалбоподателката са обработени за целите на налични договорни отношение между г-жа П.Б. и Т.О. и за събиране на дължими суми от жалбоподателката към Т.О. по сключен договор.

От Ф.И. е изискано становище и доказателства, като до момента такива не са депозирани в Комисията.

Жалбата на П.Б. е съобразена в цялост с изискванията за редовност, съгласно чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА), а именно: налице са данни за жалбоподателя, естеството на искането, дата и подпис.

Нормата на чл. 38, ал. 1, действаща към датата на подаване на жалбата от ЗЗЛД предвижда преклузивен срок за сезиране на Комисията Предвидените в чл. 38, ал. 1 от ЗЗЛД срокове са спазени.

В чл. 27, ал. 2 от АПК законодателят обвързва преценката за допустимост на искането с наличие на посочените в текста изисквания. Приложимостта на Закона за защита на личните данни е свързана със защитата на физическите лица във връзка с обработването на техните лични данни от лица, имащи качеството „администратори на лични данни" по смисъла на легалната дефиниция на чл. 4, т. 3 от Регламент (ЕС) 2016/679, каквото качество безспорно притежават Т.О. и Ф.И. Това изискване се явява абсолютна процесуална предпоставка, с оглед на което следва да се прецени допустимостта на жалбата.

На проведено на 05.02.2020 г. закрито заседание на Комисията, жалбата е обявена за процесуално допустима. Конституирани са страни: жалбоподател – П.Б., ответни страни – Т.О. на Ф.И., редовно уведомени за насроченото на 25.03.2020 г. открито заседание.

Законът за защита на личните данни и Регламент (ЕС) 2016/679 урежда правилата по отношение защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни. Целта е да се защитят основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

Съгласно легалната дефиниция, дадена в чл. 4, пар. 1, т. 1 от Регламента „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. Съдържащите се в договорите за мобилни услуги данни за жалбоподателката – три имена, адрес и единен граждански номер, безспорно имат качеството лични данни за лицето по смисъла на посочената разпоредба, тъй като чрез тях г-жа П.Б. може да бъде пряко индивидуализирана.

Условията, при наличието на които е допустимо обработването на лични данни на физическите

лица, са определени в чл. 4, ал. 1, т. 3 и т. 7 от ЗЗЛД (отм.), аналогични с чл. 6, пар. 1 от Регламента. Обработването следва да се извършва при наличието на поне едно от алтернативно посочените условия, което е предпоставка за законосъобразност на обработването. За да е налице законосъобразно обработване на лични данни същото следва да се извършва при стриктното спазване на принципите за тяхното обработване, визирани в чл. 5 от Регламента.

Т.О. е обработвало личните данни на жалбоподателката за целите на изпълнение на сключен договор за мобилни услуги през 2017 г. и в изпълнение на легитимен интерес, а именно събиране на неизплатени задължения от страна на жалбоподателката – основания по чл. 4, ал. 1, т. 3 и т. 7 от ЗЗЛД (отм.), аналогични с чл. 6, пар. 1, б. „б" и „е" от Регламента.

От събраните доказателства се установи, че г-жа П.Б. е била клиент на Т.О. по договор № *** от 04.02.2017 г. за ползване на услуга домашен интернет, телевизия и домашен телефон и анекс към договора от 14.08.2018 г., за услуга мобилен интернет, в който е предоставила изричното си съгласие при неизпълнение от нейна страна личните ѝ данни да бъдат предоставени на трети страни за събиране на задълженията.

От предоставените доказателства по административната преписка, приемо-предавателни протоколи е видно, че г-жа П.Б. на 24.04.2019 г. е върнала „устройство за фиксирана услуга", а на 24.09.2019 г. е върнала "FIED DESK PHONE FD 3165".

От г-жа П.Б. не са предоставени доказателства в подкрепа на твърденията ѝ, че договорните ѝ отношения с Т.О. са прекратени през януари 2019 г., не са предоставени и фактури, от които да е видно, че е заплатила дължимите суми към оператора.

От събраните доказателства се установи, че лични данни на г-жа П.Б. са предоставени от Т.О. на Ф.И. В конкретния случай Т.О. има качеството на администратор на лични данни, а Ф.И. – на обработващ данните за администратора, което е видно от представения договор от 30.04.2013 г. (договор за възлагане), сключен между двете дружества. В т. 1 от договора за възлагане е определена целта, за която ще бъдат обработвани данните от страна на обработващия, а именно – да организира с всички позволени от закона средства събирането на неизплатени в срок суми от неизрядни длъжници на администратора – Т.О., съгласно предоставен от последния пакет със случаи на просрочени задължения, при условия и в срокове определени в договора. Възможността за обработване на данните чрез обработващ е предвидена и в чл. 28 от Регламента. От предоставения договор за мобилни услуги № *** от 04.02.2017 г., в точка 4.1.2 е разписано изрично съгласие за предоставяне на данните на абоната на трети лица с цел събиране на вземания, дължими по договори за услуги с оператора, от което следва че и за Ф.И. е налице основание за обработване на лични данни.

От събраните доказателства, Ф.И. обработва личните данни на жалбоподателя за целите, посочени в договора за възлагане – за събиране на изискуеми и непогасени задължения на г-жа П.Б. към Т.О.

От установеното в производството, а именно: основание за обработване на личните данни, формирани и непогасени задължения по договора за мобилни услуги, както и договор, уреждащ отношенията между администратор и обработващ данните, следва, че предаването на личните данни е законосъобразно.

Предвид изложеното и на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, § 1, б. „е" от Регламента и чл. 38, ал. 3 от Закона за защита на личните данни, Комисията се произнесе със следното

РЕШЕНИЕ:

Оставя жалба с рег. № ППН-01-272/14.03.2019 г., подадена от П.Б. срещу *телекомуникационен оператор* и *финансова институция*, без уважение като неоснователна.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ
№ ППН-02-475/2019
София, 20.05.2020 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов и Веселин Целков, на проведено на 01.04.2020 г. неприсъствено заседание по реда на чл. 12 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, 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 жалба рег. № ППН-02-475/30.08.2019 г., подадена от Ч.Д. срещу ***телекомуникационен оператор (Т.О.).***

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

Жалбоподателят информира, че на 25.08.2019 г., при проверка в сайта на Т.О., секция „М.Т.О.”, раздел „Сметки и фактури”, с огромна изненада видял общо задължение от 52481.34 лв.

При детайлно разглеждане установил, че към няколкото негови договора е добавен чужд договор № ***1 със задължение от 53381.16 лв. и опция „заплати” на юридическо лице „М“, с което дружество жалбоподателят твърди, че няма нищо общо.

Още по-смущаващо за г-н Ч.Д. било, че има и следното съобщение: „Вие имате сключени договори, които не са добавени към М.Т.О. За да ги управлявате онлайн, моля добавете ги: договор ***2, ***3, ***4, ***5.”

Жалбоподателят заявява, че никога не е сключвал тези договори, нито ги е добавял в потребителския си профил, който е защитен с дълга парола.

Г-н Ч.Д. се свързал със сътрудник на Т.О, след това посетил и офис на Т.О., но и от двете места не могли да му дадат обяснение. На 26.08.2019 г. получил обаждане от сътрудник на Т.О., който се извинил и заявил, че вероятно става въпрос за техническа грешка.

Жалбоподателят счита, че някой е проникнал в профила му, има достъп до личните му данни и добавя чужди договори, поради което иска проверка на случая – кой, кога, как и откъде е успял да пробие сигурността на сайта.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено лицето, срещу което е насочена жалбата. 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.

От Т.О. информират, че г-н Ч.Д. е абонат на няколко услуги, предоставяни от мобилния оператор.

На 03.06.2018 г. договорът за услуги, предоставян чрез номер *********3, е прекратен поради смяна на номера и номерът на ползване на услугата е станал *********7. На 12.09.2018 г. номер *********3 е предоставен от Т.О. на друг клиент – „М.".

В резултат на техническа грешка при актуализация на системата, в профила на г-н Ч.Д. се е визуализирало задължение, отнасящо се към услугата на „М". Проблемът е установен и премахнат успешно. С цел избягване на конкретния проблем, от Т.О. са подменили системата за нотифициране при спиране на услуги и понастоящем възможността за подобни спорадични грешки е минимизирана.

От мобилния оператор посочват, че г-н Ч.Д. не е абонат на цитираните в жалбата договори с номера ***2, ***3, ***4, ***5. Същите са сключени с „М.".

При така установеното, КЗЛД намира жалбата за неоснователна, въз основа на следнотоо:

Комисията е сезирана с домумент, наименован „сигнал", който по същество представлява „жалба" по смисъла на чл. 35 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА), тъй като с него се търси защита на нарушени права на сезиращия. Разглежданата жалба е съобразена в цялост с изискванията за редовност, съгласно чл. 28, ал. 1 от ПДКЗЛДНА, а именно: налице са данни за жалбоподателя, естеството на искането и въз основа на какво се основава, дата на узнаване на нарушението, срещу кое лице се подава жалбата, дата и подпис.

Жалбата е процесуално допустима – подадена в срока по 38, ал. 1 от ЗЗЛД от физическо лице с правен интерес. Същата има за предмет твърдение за неправомерно обработване на лични данни на жалбоподателя и е насочена срещу администратор на лични данни. 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 и чл. 38, ал. 1 ЗЗЛД разглежда жалби, подадени от субекти на данни при нарушаване на правата им по Регламент 2016/679 и ЗЗЛД.

Комисията за защита на личните данни е независим надзорен орган, който осъществява защита на лицата при обработване на техните лични данни и при осъществяване на достъпа до тези данни, както и контрола по спазване 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 (накратко „Регламента" или Регламент 2016/679) и Закона за защита на личните данни (ЗЗЛД). Една от задачите на КЗЛД по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е" от Регламент 2016/679 е да разглежда жалби, подадени от субекти на данни, и да разследва предмета на жалбата, доколкото това е целесъобразно. Целесъобразността при разглеждане на жалбите е прецесуално развита в чл. 38, ал. 4 ЗЗЛД – когато жалбата е очевидно неоснователна или прекомерна, с решение на Комисията жалбата може да бъде оставена без разглеждане.

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.

В жалбата се твърди нарушение на сигурността на сайт чрез неправомерен достъп от трети лица до онлайн профила на жалбоподателя в „М.Т.О.".

Действително, Т.О. като администратор на лични данни има задължението по чл. 32, параграф 1, буква „б" от Регламент 2016/679 да прилага подходящи технически и организационни мерки за осигуряване на съобразеното с риска за правата на субектите на данни ниво на сигурност,

включително способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване. Онлайн платформата „М.Т.О.” е именно такава система за обработване на лични данни.

Представените доказателства свидетелстват, че титуляр на телефонния номер *********3 първоначално е жалбоподателят. След смяната му, номерът е предоставен за ползване от Т.О. на регистрирания в Република България клон на дружеството „„„М.“. Вследствие смяната на титуляря на номера и възникнала техническа грешка, договорът за този номер се е визулизирал в профила на г-н Ч.Д. Видно и от самите екранните разпечатки към жалбата, титуляр на договора и задължението е „М.“, а не г-н Ч.Д. Същото се отнася и за договори ***2, ***3, ***4, ***5, които отново са с титуляр „М.“, но поради възникналата грешка системата прави запитване за прибавянето им към вече добавения договор на „М.“.

Предвид горното, промените в профила на г-н Ч.Д. са вследствие на техническа грешка в самата система, а не са извършени от трето – външно за системата лице, което неправомерно да е достъпило до системата на Т.О., каквито твърдения са наведени в жалбата. Следователно, не е нарушена поверителността на системата за обработватване на лични данни „М.Т.О.”, която да е довела до нарушаване правата на жалбоподателя, с оглед на което не е допуснато нарушение на чл. 32, параграф 1 от Регламент 2016/679.

Както беше посочено, договори с номера ***2, ***3, ***4, ***5, за които е направено запитване от системата дали да бъдат добавени в профила на жалбоподателя, са с титуляр клона на дружеството „М.“, а не г-н Ч.Д., поради което негови лични данни не се обработват за тази цел и не е налице неправомерно обработване личните данни на жалбоподателя.

Така мотивирана и на основание чл. 38, ал. 4 от ЗЗЛД във връзка с чл. 38, ал. 1 от Правилника за дейността на КЗЛД и нейната администрация, Комисията за защита на личните данни

РЕШИ:

Оставя жалба рег. № ППН-02-475/30.08.2019 г., подадена от Ч.Д. срещу „Т.О. България” ЕАД, без разглеждане като очевидно неоснователна.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ
№ ППН-01-152/2020 г.
София, 19.05.2020 г.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав, председател – Венцислав Караджов и членове: Цанко Цолов и Веселин Целков на редовно заседание, проведено на 01.04.2020 г. и обективирано в протокол № 12/01.04.2020 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни (ЗЗЛД) във вр. с чл. 57, § 1, б. „е“ от Регламент (ЕС) 2016/679, разгледа жалба с рег. № ППН-01-152/21.02.2020 г., подадена от С.Р.

В Комисия за защита на личните данни е постъпила жалба, препратена от Регионална здравна инспекция – Р., подадена от С.Р.

В жалбата е посочено, че г-жа С.Р. от 2016 г. страда от онкологично заболяване, в хода на което за известен период от време била пациент на д-р Г. и д-р С.

В жалбата се сочи, че за заболяването се знаело само от ограничен кръг хора, освен лекувалите я лекари. Жалбоподателката много държала за заболяването ѝ да не разбират децата и родителите ѝ.

Сочи, че във фейсбук от д-р С. е публикуван материал, който недвусмислено я идентифицира, като пациент страдащ от онкологично заболяване. Твърди, че постовете довеждат до злостни коментари, включително от хора, които не я познават и стават достояние на неограничен кръг от хора.

Твърди, че поведението на д-р С. и причинява сериозно безпокойство и морални страдания. Информира, че д-р С. е разкрил без нейно разрешение факти относно здравето ѝ, които се опитала да запази в тайна.

Жалбата на С.Р. е редовна, налице са всички задължителни реквизити по чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни (ПДКЗЛДНА), а именно: налице са данни за жалбоподателя, естеството на искането, дата и подпис.

Редът за разглеждане на жалби пред Комисия за защита на личните данни не е уреден в Регламент (ЕС) 2016/679, а е оставен на преценката на всяка държава-членка. В Република България производството се развива по реда на Административнопроцесуалния кодекс (АПК) и завършва с индивидуален административен акт. Съгласно чл. 27, ал. 2 от АПК административният орган проверява предпоставките за допустимостта на искането, с което е сезиран, като съгласно т. 6 от разпоредбата преценката за допустимостта се обвързва с наличие на специални изисквания, уредени със закон. Такива изисквания са уредени в АПК и Регламент (ЕС) 2016/679.

Следва да бъде посочено, че в жалбата не е конкретизирано от жалбоподателката какъв обем лични данни счита, че са обработени. За да бъде изпълнена хипотезата на чл. 4, т. 1 от Регламента, е необходимо информацията, представляваща лични данни и отнасяща се до дадено физическо лице да води до неговото идентифициране- пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци. От изложеното се налага изводът, че не винаги посочването на един или няколко специфични признаци по отношение на дадено физическо лице може да доведе до неговото идентифициране. За да бъде осъществена неговата правна индивидуализация в обществото, следва да се посочат един или няколко признака, въз основа на които може да се направи ясен и недвусмислен извод, че информацията относно посочените признаци се отнася до точно конкретно лице, т.е. същото да може да се индивидуализира.

От предоставените по административната преписка екранни разпечатки, като доказателства не се установяват каквито и да било данни, които да идентифицират жалбоподателката, дори и имена. От предоставените доказателства става ясно, че жалбоподателката е „жена“ на д-р К. Не става ясно точно на кой д-р К., предвид факта , че д-р К. не е индивидуализиран с друго име, от което да може да се ясно и конкретно да се индивидуализира д-р К. От служебна справка в интернет се установява, че в гр. Р. има няколко лекари със същата фамилия, с различно първо име и различна специалност.

С оглед на гореизложеното, а именно - невъзможността да се индивидуализира жалбоподателката, се налага изводът за недопустимост на жалбата. В тази връзка следва да се отбележи, че обект на защита и предмет на производството развиващо се по реда на чл. 38 от ЗЗЛД са личните данни на физическите лица и тяхното обработване, какъвто предмет в конкретния случай не е налице.

Въз основа на изложеното, на основание чл. 27, ал. 2, т. 6 от АПК във връзка с 57, пар. 1, б. „е“ от Регламент 2016/679, Комисията се произнесе със следното:

РЕШЕНИЕ:

Обявява жалба с рег. ППН-01-152/21.02.2020 г., подадена от г-жа С.Р., за процесуално недопустима и прекратява производството.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Веселин Целков /п/

РЕШЕНИЕ
№ ППН-01-360/2019 г.
София, 22.05.2020 г.

Комисията за защита на личните данни (КЗЛД, Комисията) в състав, председател, Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на редовно заседание, проведено на 12.02.2020 г. и обективирано в протокол № 6/12.02.2020 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни (ЗЗЛД) във вр. с чл. 57, § 1, б. „е“ от Регламент (ЕС) 2016/679, разгледа по същество жалба с рег. № ППН-01-360/08.04.2019 г., подадена от А.П. срещу ***електронна медия (Е.М.).***

В жалбата е посочено, че на 19.02.2019 г., придружавана от съпруга си, г-жа А.П. е посетила ***здравно заведение (З.З.)***, за да ѝ бъдат направени медицински изследвания.

На 20.04.2019 г. при преглед на пресата, жалбоподателката установила, че на сайта на он лайн изданието на Е.М. е публикувана статия - без нейно знание и съгласие, в която са публикувани личните ѝ данни, в обем снимка на г-жа А.П. и съпруга ѝ, направена в лабораторията, без знанието на жалбоподателката, и медицински изследвания. Сочи се, че в статията е записано „тест за естрадиол, TSH, пролактин и др“, които са включени в листа с изследвания на жалбоподателката. Жалбоподателката счита, че публикуването на лабораторни изследвания е „изключително грубо навлизане в личното пространство“.

А.П. счита, че присъствието на личните ѝ данни в публичното пространство представлява нарушение на ЗЗЛД и Регламент (ЕС) 2016/679.

В условията на залегналото в административния процес служебно начало и задължението на административния орган за служебно събиране на доказателства и изясняване на действителните факти от значение за случая, с писмо изх. № ППН-01-360#1/16.06.2019 г. на управителя на Е.М. е предоставен срок за изразяване на становище и представяне на относими доказателства.

В отговор е постъпило становище, в което е посочено, че наистина на 19.02.2019 г., а не на 20.02.2019 г. е публикувана статия, в която не са използвани личните данни на А.П. Информират, че освен публикувани папарашки снимки на неизвестни на Е.М. лица, в статията не са публикувани лични данни на по смисъла на чл. 4 от Регламент (ЕС) 2016/679. Сочат, че не са виждали публикувано клинично изследване.

С писмо изх. № ППН-01-360#5/03.07.2019 г. е изискано от адвокатите на г-жа А.П., в 7-дневен срок от получаване на писмото да ангажират доказателства, относно твърденията в жалба с рег. № ППН-01-360/08.04.2019 г., предвид факта, че такива не са депозирани в Комисията с постъпването на жалбата, въпреки че са описани като приложения към нея. С писмо, постъпило по електронна поща в Комисията и заведено с рег. № ППН-01-360#6/08.08.2019 г. са постъпили незаверени копия от статии на Е.М.

Разглежданата жалба е съобразена в цялост с изискванията за редовност, съгласно чл. 28, ал. 1 от Правилник за дейността на Комисията за защита на личните данни и нейната администрация (ПДКЗЛДНА), а именно: налице са данни за жалбоподателя, естеството на искането, дата и подпис.

Жалбата е подадена в срока по пар. 44, ал. 2 от Преходните и заключителните разпоредби на ЗЗЛД от физическо лице с правен интерес срещу надлежна страна –администратор на лични данни по смисъла на чл. 4, пар. 7 от Общия регламент (ЕС) 2016 /679, предвид обстоятелството, че последните сами определят целите и средствата за обработване на лични данни чрез видеонаблюдение и е допустима.

Предвид гореизложеното и с оглед липсата на предпоставки от категорията на отрицателните по чл. 27, ал. 2 от АПК жалбата е обявена за допустима и като страни в административното производство са конституирани, А.П. и ответна страна Е.М., в качеството на администратор на лични данни. Насрочено е открито заседание за разглеждане на жалбата по същество на 18.12.2019 г., за което страните са редовно уведомени и им е указано разпределянето на доказателствената тежест в процеса. Поради липса на мнозинство при вземането на решението, Комисията е отложила жалбата за разглеждане в закрито заседание за вземане на решение от друг състав.

Съгласно чл. 10, ал. 1 във връзка с чл. 38 от Закон за защита на личните данни, при сезирането ѝ Комисията за защита на личните данни разглежда жалби срещу актове и действия на администраторите на лични данни, с които се нарушават правата на физическите лица по ЗЗЛД, както и жалби на трети лица във връзка с правата им по този закон.

Съгласно легалната дефиниция, дадена в чл. 4, пар. 1, т. 1 от Регламента „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.

С решение от 14 февруари 2019 г. по дело C−345/17 на съда на европейския съюз е посочено, че за да намери равновесната точка между правото на зачитане на личния живот и правото на свобода на словото, Европейският съд по правата на човека е разработил поредица от относими критерии, които трябва да бъдат взети предвид, по-специално приноса към дебат от обществен интерес, известността на засегнатото лице, предмета на репортажа, досегашното поведение на съответното лице, съдържанието, формата и последиците от публикацията, начина и обстоятелствата, при които е била получена информацията, както и нейната достоверност. Също така трябва да се вземе предвид възможността на администратора на данни да приеме мерки за намаляване на обхвата на намесата в правото на личен живот.

От предоставените по административната преписка доказателства се установи, че в публикуваните статии се съдържат две имена на жалбоподателката, снимка, вида на изследванията

и възраст. Не е публикувана информация за резултатите от проведени изследвания, каквито са оплакванията в жалбата.

В съображение 153 от Регламента е предвидено, че правото на държавите-членки следва да съвместява разпоредбите, уреждащи свободата на изразяване на мнение и свободата на информация, включително за журналистически, академични, художествени и литературни цели с тези за защита на личните данни.

Понятието „журналистически цели" не е дефинирано от законодателя, но е тълкувано в съдебната практика. Съществото за журналистическата дейност е събирането, анализирането, интерпретирането и разпространяването чрез средствата за масова информация на актуална и обществено значима информация. Всяка журналистическа дейност е проява на свободата на словото в правовата държава. Ограничаване свободата на изразяване и информация е допустимо само в рамките на необходимото в едно демократично общество съгласно чл. 10, § 2 от Конвенцията за защита правата на човека и основните свободи.

По своята същност журналистическата дейност изисква разпространяване на информация по въпроси от обществен интерес. Публикуването на информация на интернет страницата на медията представлява нейното публично оповестяване. Публичното разпространяване на информация за тези цели е журналистическа дейност, тъй като самият факт на разпространение е изява на мнение, становище, възглед, преценка на публичната информация и значението ѝ за интересите на обществото. За да се обработва информация за целите на журналистическата дейност, информацията трябва да касае въпроси относно ценности, които с оглед на засегнатите отношения са действително обществено важни.

Следва да се посочи, че свободата на печата и другите средства за масова информация са конституционно гарантирани със забраната за цензура - чл. 40, ал. 1 от Конституцията на Република България. Свободата на словото е един от фундаменталните принципи, върху които се гради всяко демократично общество. Правото си на информация, на свободно изразяване, обществото е делегирало в професионален ангажимент на журналистите, които в името на общественото благо се занимават със събирането, подреждането и разпространението на информация. Задължението на журналистите да предоставят информация и идеи, засягащи въпроси от обществен интерес, произтича от правото на обществеността да я получава. В този смисъл свободата на словото, свободата да се разпространява информация без цензура е оправдано дотолкова, че да се гарантира демократичността на обществените процеси и възможността на гражданите за изграждане на мнение и позиция относно проблеми, касаещи обществен интерес.

Предвид всичко изложеното Комисията счита, в конкретния случай е безспорно, че личните данни на жалбоподателката са обработени, в хипотезата на употреба и разпространение, с журналистически цели. В тази връзка счита, че при обработването на личните данни на жалбоподателката за целите на статията не е намерен разумния баланс между правото на неприкосновеност на засегнатото лица, правото на свобода на печата и правото на обществото да бъде информирано, т.е. не е намерен баланса между обществения интерес и личен живот на лице, сезирало Комисията.

Не е намерен балансът между значимостта на обществения интерес, който налага това обработване и степента, до която се засяга правото на неприкосновеност на личния живот на физическото лице, за което се отнасят данните.

Предвид изложеното, КЗЛД счита, че обработването на личните данни на г-жа А.П. от Е.М. е в нарушение на принципа на „свеждане на данните до минимум", посочен в чл. 5, пар. 1 , „в" Регламент (ЕС) 679/2016, съгласно който обработваните лични данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите за които се обработват.

Комисията счита, че следва да се прави разлика между обществен интерес и обществено интересно. Обществено интересно може да бъде всяка информация, но тя не представлява обществен

интерес. Въпросът е когато се обработват лични данни за журналистически цели, да се спазват изискванията за удовлетворяване на обществен интерес.

Безспорно, като осигуряващи обективен поглед на обществото към важни за него прояви на журналистите се полага съответното уважение и защита, но не и когато действията им граничат с т. н „папарашко“ поведение, нямащо нищо общо с нещо значимо за обществото като цяло. Дейността на журналистите изисква спазването на определена етика, при което следва да се съобразяват с основните права на гражданите и да не навлизат безпричинно в личната им сфера.

Предвид всичко изложено, оперативната самостоятелност на административния орган и в съответствие с предоставените ѝ функции преценява кое от корективните правомощия по чл. 58, пар 2 от Регламент 679/2016 г. да упражни, Комисията счита, че в конкретния случай корективните мерки по букви „а“ – „з“ и буква „й“ на чл. 58, параграф 2 от Регламента са приложими Преценката се основава на целесъобразност и ефективност на решението при отчитане на особеностите на всеки отделен случай и степента на засягане на интересите на конкретно физическо лице – субект на данни, като и на обществения интерес. Комисията, при определяне на корективното правомощие, взе предвид факта, че нарушението е първо за администратора, както и факта, че за жалбоподателката не са настъпили значителни вредни последици.

Предвид изложеното и на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, § 1, б. „е“ от Регламента и чл. 38, ал. 3 от Закона за защита на личните данни, Комисията се произнесе със следното

РЕШЕНИЕ:

1. Обявява жалба с рег. № ППН-01-360/08.04.2018 г., подадена от А.П. срещу Е.М. за основателна, за нарушение на разпоредбата на чл. 5, пар. 1, б. „в“ от Регламент (ЕС) 2016/679.

2. На основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679 разпорежда на Е.М., да съобрази обработването на личните данни с разпоредбата на чл. 5, пар. 1, б. „в“ и да изтрие всички данни на жалбоподателката от сайта.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

РЕШЕНИЕ
№ ППН-01-498/2019
София, 20.05.2020 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 04 и 06 март 2020 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 рег. № ППН-01-498/23.05.2019 г., подадена от А.Ст.

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

На 16.05.2019 г., след предаден болничен и опит да бъде подаден в НОИ, г-жа А.Ст. установила след направена справка в ГРАО, че е със сменена фамилия. В списъците излиза под името А.Сю. и че се е омъжила в Р.

Жалбоподателката заявява, че никога не е била на територията на Р. и никога не е сменяла фамилията си. Заради тази грешка или измама, която е била направена, г-жа А.Ст. се опасява, че няма да може да упражни правото си на глас на изборите.

Счита, че са нарушени правата ѝ по ЗЗЛД.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено Министерството на регионалното развитие и благоустройството (МРРБ), което поддържа ЕСГРАОН. 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.

От МРРБ посочват, че е извършена проверка, при която е установено, че при обработване на електронни документи е допусната техническа грешка от длъжностно лице по гражданско състояние в Общинска администрация гр. В.

Съгласно чл. 41а от Закона за гражданската регистрация, за всеки съставен акт за гражданско състояние на хартиен носител се създава електронен еквивалент – електронен акт за гражданско състояние на национално ниво. Задължение на длъжностното лице по гражданското състояние в общинската администрация е след като свери данните от акта за гражданско състояние в писмен и в електронен вид, да подпише електронния еквивалент на акта с квалифициран електронен подпис (КЕП). В този смисъл е и разпоредбата на чл. 59 от Наредба № РД-02-20-9 от 21 май 2012 г. за функциониране на Единната система за гражданска регистрация (обн. ДВ бр. 43 от 2012 г.). Веднага след като електронният еквивалент на акта за гражданско състояние е създаден в Националния електронен регистър на актове за гражданско състояние (НЕРАГС), длъжностното лице по гражданското състояние сверява данните от него и от акта в писмен вид и при установено съответствие на данните подписва електронния еквивалент с КЕП. При промяна, допълнение, вписване или отбелязване в акт за гражданско състояние, съставен в писмен вид, длъжностното лице по гражданското състояние в общинската администрация създава електронен документ за отразяване на променените данни в електронния еквивалент на акта за гражданско състояние в НЕРАГС. След отразяване на промените в електронния еквивалент на акта, длъжностното лице по гражданското състояние задължително сверява данните от него и от акта в писмен вид и при установено съответствие на данните подписва електронния еквивалент с КЕП.

При създаване на електронния еквивалент на Акт за сключен граждански брак № ****, между С.С. с ЕГН 82******** и М.К. с дата на раждане ****.1991 г., съставен в Общинска администрация - гр. В., длъжностното лице по гражданското състояние технически погрешно е въвело в данните ЕГН 91********, който е на А.Ст. В резултат на това, при актуализацията на данните автоматизирано в

електронния личен регистрационен картон на А.Ст. се променят фамилното й име (от Ст. на Сю.) и семейното й положение (от неомъжена на омъжена).

На 20.05.2019 г. длъжностното лице по гражданското състояние в Община В. е извършило техническа корекция, като е въвело верните данни в електронния еквивалент на акта за сключен граждански брак между С.С. и М.К.

Към настоящия момент, съгласно данните в Регистъра на населението – Национална база данни „Население“ лицето А.Ст. с ЕГН 91********* е със семейно положение неомъжена и фамилно име Ст.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомена Община В., срещу която е потвърдена жалбата. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения. В Комисията не постъпи отговор на жалбата.

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

Разглежданата жалба съдържа задължително изискуемите реквизити, посочени в чл. 30, ал. 1 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация (ДВ, бр. 10 от 2016 г.), а именно: налице са данни за жалбоподателя, естество на искането, дата и подпис, с оглед на което същата е редовна.

Жалбата е процесуално допустима – подадена в срока по § 44, ал. 2 от ПЗР на ЗЗЛД от физическо лице с правен интерес. Същата има за предмет твърдение за неправомерно обработване на лични данни на жалбоподателя и е насочена срещу администратор на лични данни. 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 и чл. 38, ал. 1 ЗЗЛД разглежда жалби, подадени от субекти на данни при нарушаване на правата им по Регламент 2016/679 и ЗЗЛД.

На проведено на 12.02.2020 г. заседание на Комисията жалбата е обявена за процесуално допустима и като страни в административното производство са конституирани: жалбоподател А.Ст. и ответна страна Община В. Страните са редовно уведомени за насроченото за 04.03.2020 г. заседание на Комисията за разглеждане на жалбата по същество.

На проведеното открито заседание за разглеждане на жалбата по същество жалбоподателката се явява лично и поддържа жалбата. Отбелязва, че много хора не ѝ вярвали, включително и приятелят ѝ. Той бил в чужбина, тя в отпуск, а ѝ казват, че на тази дата се е омъжила във В. Тя твърдяла, че не е така, но по телефона жена от ГРАО твърдяла, че се е омъжила. Така в продължение на седмици, докато не се решил проблемът след подаване на жалбата, след което отишла в общината и извадила документ, че не е омъжена. Посочва, че са ѝ причинени неудобства няколко месеца – с болничния, с работата, с личния живот. Претендира обезщетение.

Ответната страна – 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, по-специално тяхното право на защита на личните им данни.

Съгласно чл. 1, ал. 3 от Закона за гражданската регистрация (ЗГР) гражданската регистрация включва съвкупност от данни за едно лице, които го отличават от другите лица в обществото и в семейството му в качеството на носител на субективни права, като име, гражданство, семейно положение, родство, постоянен адрес и др.

В чл. 2 от ЗГР е посочено, че гражданска регистрация е вписване на събитията раждане, брак и смърт в регистрите на актовете за гражданско състояние и вписване на лицата в регистъра на населението. Актовете за гражданско състояние са официални писмени документи. В тях по законов ред длъжностните лица по гражданското състояние регистрират събитията раждане, брак и смърт.

Съгласно чл. 41а от ЗГР за всеки съставен акт за гражданско състояние се създава електронен еквивалент – електронен акт за гражданско състояние на национално ниво. Електронният акт за гражданско състояние се създава от общинската администрация, където е съставен актът за гражданско състояние в писмен вид. След сверяване на данните от акта за гражданско състояние в писмен и електронен вид длъжностното лице по гражданското състояние подписва акта с квалифициран електронен подпис.

Видно от цитираните разпоредби на ЗГР, длъжностните лица по гражданско състояние в общините имат нормативно предоставените правомощия да регистрират събитието брак в писмен акт за гражданско състояние и да направят негов електронен еквивалент.

Обработване на лични данни при упражняване на официални правомощия, които са предоставени на администратора на лични данни от националното законодателство, представлява условие за обработване на лични данни по чл. 6, параграф 1, буква „д“, предложение второ от Регламент 2016/679.

Видно от представената от МРРБ справка, в изпълнение на нормите на ЗГР длъжностното лице по гражданска регистрация от Община В. е предприело действия за създаване на електронен еквивалент на акт за сключен граждански брак между две лица, които са различни от жалбоподателката. Поради допусната техническа грешка е въведено ЕГН на жалбоподателката, при което при автоматизираната актуализация на данните в електронния личен регистрационен картон на г-жа А.Ст. са променени фамилното ѝ име и семейното ѝ положение.

Освен наличие на основание за обработване на лични данни, за администратора на лични данни е предвидено задължение по чл. 25, параграф 1 от Регламент 2016/679 да въведе към момента на обработването необходимите технически и организационни мерки, за да спазят изискванията на регламента и да се осигури защита на правата на субектите на данни.

Една от организационните мерки при въвеждане на промени в гражданското състояние на лицата в електронните регистри е посочена в самия закон – чл. 41, ал. 3 от ЗГР и чл. 59, ал. 2 от Наредба № РД-02-20-9 от 21 май 2012 г. за функциониране на единната система за гражданска регистрация, съгласно които длъжностното лице по гражданското състояние следва да свери данните от електронния акт за гражданско състояние и от акта за гражданско състояние в писмен вид и при установено съответствие на данните да подпише електронния еквивалент с квалифициран електронен подпис. В разглеждания случай това не е направено, което е довело до промяна в личните данни на жалбоподателката в регистрите на ЕСГРАОН, които не отговарят на действителното правно положение, с което е нарушен чл. 25, параграф 1 от Регламент 2016/679.

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.

Предвид горното и при преценка на всички факти и обстоятелствата по преписката, Комисията намира, че за извършеното нарушение следва да бъде наложено административно наказание „имуществена санкция" на Община В. в размер близък до минималния. Конкретните за случая обстоятелства в съответствие с чл. 83, параграф 2 от Регламента са следните:

Буква „а" – обработването се състои в грешно въвеждане на данни в национален електронен регистър, до който достъп за проверка на данни във връзка с правомощията си имат много държавни органи, което е довело до промяна в личните данни на лице, различно от това, за което се отнася промяната. Това е довело до неблагоприятни последици за два субекта на данни – жалбоподателката, за която са възникнали проблеми с обработването на болничния ѝ лист, с упражняването на правото на глас на избори, в личния живот. Освен за жалбоподателката, е било възможно да възникнат неблагоприятни последици и за лицето, за което е следвало да бъде въведена промяната – до поправяне на грешката същото не се е водело омъжено с произтичащите от това последици;

Буква „б" – администраторът, извършил нарушението, е юридическо лице – орган на местно самоуправление, което не формира вина. Извършените от служителя на администратора действия са поради небрежност;

Буква „в" – администраторът е предприел действия за поправяне на грешката, макар почти 3 месеца след извършеното нарушение;

Буква „г" – нарушението е именно за непредприемане на дължимите по закон организационни мерки, допуснати от администратора;

Буква „д" – няма нарушение на сигурността на данните по смисъла на член 33 от Регламента или други свързани нарушения;

Буква „е" – нарушението е отстранено от администратора преди произнасянето по жалбата;

Буква „ж" – нарушението е довело до промяна в семейно положение и фамилията на засегнатото лице в национален регистър;

Буква „з" – КЗЛД е узнала за извършеното нарушение след сезирането ѝ от субекта на данни;

Буква „и" – на администратора не са налагани предходни мерки по чл. 58, пар. 2 от Регламента или по чл. 38 от ЗЗЛД;

Буква „й" – към момента на извършване няма одобрени кодекси за поведение;

Буква „к" – администраторът на лични данни е малка община, което също следва да се вземе предвид при определяне размера на санкцията.

В открито заседание е направено искане за обезщетение вследствие неправомерното обработване и възникналите неблагоприятни последици. Съгласно чл. 82, параграф 6 от Регламент 2016/679 и чл. 39, ал. 2 от ЗЗЛД такъв иск може да бъде предявен пред компетентния съд. Правомощие за присъждане на обезщетения не е предоставено на надзорния орган – видно от чл. 58 от Регламент 2016/679, чл. 38 от ЗЗЛД, поради което е недопустимо в административното производство.

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

РЕШИ:

1. Обявява жалба рег. № ППН-01-498/23.05.2019 г., подадена от А.Ст., за основателна за нарушение на чл. 25, параграф 1 от Регламент 2016/679. На основание чл. 58, параграф 2, буква „и" от Регламент 2016/679 във връзка с чл. 83, параграф 4, буква „а" налага на администратора на лични данни Община В. административно наказание „имуществена санкция" в размер на 2 000 (две хиляди) лв;

2. Отхвърля като недопустимо искането за присъждане на обезщетение.

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-02-31/2019
София, 03.06.2020 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 11.03.2020 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 рег. № ППН-02-31/24.01.2019 г., подадена от В.Т. срещу „П." ЕАД (накратко П.).

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

Жалбоподателят информира, че след като през лятото на 2018 г. кандидатствал за работа в компания „П." и не получил отговор на кандидатурата си, на 30 август 2018 г. изпратил писмо до официалния им имейл адрес със заявление за заличаване на личните му данни от системата им, както и от системите на техните представители или трети страни, на които може да са предадени. В заявлението посочил, че би искал да получи потвърждение, когато личните му данни бъдат изтрити.

След дълго чакане без отговор, на 31.12.2018 г. отново изпратил имейл. В отговор получил имейл от г-н К.П., от който не става ясно дали конкретно негови лични данни са били изтрити, като

се казва, че по принцип всички заявления към тях по GDPR са обработени, а данните изтрити от системата на компанията, както и че компанията им няма практика да отговаря на подобни имейли, които също съдържат лични данни.

Г-н В.Т. моли КЗЛД да провери наистина ли неговото заявление е било взето под внимание и дали личните му данни действително са заличени, както и да се прецени дали е законосъобразно компанията да не изпраща отговор на заявлението.

Към жалбата е приложена кореспонденция по електронна поща.

В условията на залегналото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомено лицето, срещу което е насочена жалбата. 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.

От П. посочват, че кандидатурата за работа на жалбоподателя не е получена от него, а от трето лице – понастоящем бивш служител на дружеството, който бил помолен да го препоръча като подходящ кандидат.

От дружеството се противопоставят на твърдението на г-н В.Т., че не е получил своевременен отговор на подаденото искане за заличаване на лични данни. Това твърдение не се подкрепя от приложения към сигнала имейл с текст за заличаване, тъй като той не съдържа датата 30.08.2018 г., както твърди субектът на данни, а датата 21.01.2019 г. Видно от разменените между страните имейли от 31.12.2019 г., дружеството не само че е взело под внимание заявлението за заличаване на лични данни, но е отговорило веднага на г-н В.Т., потвърждавайки изтриването на личните му данни от системите на дружеството.

Към становището е приложен Протокол за заличаване на лични данни.

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

В КЗЛД постъпи иницииращ документ, наименован „сигнал“, с който се търси защита на нарушени права на искателя, поради което по същество представлява „жалба“ по смисъла на чл. 36, ал. 1 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация (ДВ, бр. 10 от 2016 г.).

Разглежданата жалба съдържа задължително изискуемите реквизити, посочени в чл. 30, ал. 1 от ПДКЗЛДНА (ДВ, бр. 10 от 2016 г.), а именно: налице са данни за жалбоподателя, естество на искането, дата и подпис, с оглед на което същата е редовна.

Жалбата е процесуално допустима – подадена в срока по § 44, ал. 2 от ПЗР на ЗЗЛД от физическо лице с правен интерес. Същата има за предмет твърдение за неправомерно обработване на лични данни на жалбоподателя и е насочена срещу администратор на лични данни. 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 и чл. 38, ал. 1 ЗЗЛД разглежда жалби, подадени от субекти на данни при нарушаване на правата им по Регламент 2016/679 и ЗЗЛД.

На проведено на 05.02.2020 г. закрито заседание на Комисията жалбата е обявена за допустима и като страни в производството са конституирани: жалбоподател В.Т. и ответна страна „П.“ ЕАД. Страните са уведомени за насроченото за 11.03.2020 г. открито заседание за разглеждане на спора по същество.

На проведеното заседание за разглеждане на жалбата по същество жалбоподателят не се явява, не се представлява.

За ответната страна се явява надлежно упълномощен процесуален представител. Оспорва жалбата и я счита за неоснователна. Представя допълнително становище.

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, по-специално тяхното право на защита на личните им данни.

Страните не спорят, че лични данни са предоставени доброволно за обработване от жалбоподателя на администратора за целите на подбор на персонал, която по сведения от администратора е неофициална процедура – чрез препоръка от служител на дружеството.

От сведенията в жалбата и представената към нея кореспонденция с П. е видно, че на 30.08.2018 г. жалбоподателят е отправил до администратора оттегляне на съгласие за обработване на личните му данни и искане за заличаването им.

Поради липса на отговор, на 31.12.2018 г. е отправено запитване до администратора относно резултата от подаденото заявление.

Комуникацията между жалбоподателя и администратора е осъществена между август и декември 2018 г. В този период вече се прилага Регламент 2016/679 (от 25.05.2018 г.), но измененията в ЗЗЛД, направени с ДВ, бр. 17 от 26.02.2019 г., които следва да синхронизират вътрешното национално законодателство с европейското, все още не приети. Поради това, към момента на подаване на искането разпоредбите за упражняване на права по Глава пета от ЗЗЛД все още не са отменени, въпреки че същите са вече уредени с Регламент 2016/679. При това положение следва да приложат разпоредбите на общносното право – Регламент 2016/679, предписани с нормативен акт от по-висок ранг.

Съгласно чл. 17 от Регламент 2016/679 субектът на данни има право да поиска от администратора изтриване на свързани с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни при наличие на някое от основанията по букви „а“ до „е“ от същия член, освен ако не е налице някое от основанията за отказ по параграф 3 на същия член.

В случая са предприети действия по заявлението и видно от представения протокол от 03.09.2018 г., заявлението е уважено и личните данни са заличени.

Освен предприемане на действия по заявлението, в срок от един месец от получаване на искането администраторът на лични данни дължи предоставяне на информация на заявителя относно действията, предприети във връзка с искането, съгласно чл. 12, параграф 3 от Регламент 2016/679.

В конкретния случай липсва отговор до жалбоподателя относно предприетите действия. Такъв е предоставен едва след повторно запитване от страна на субекта. Неоснователно е твърдението на П., че на жалбоподателя е отговорено в срок, тъй като заявлението не е от 30.08.2018 г., а от по-късна дата – второто запитване от жалбоподателя от 31.12.2018 г. В самия протокол за заличаване, който е от 03.09.2018 г., е посочено, че заличаването се прави по искане на жалбоподателя, отправено по имейл, т.е. искането от 30.08.2018 г. е получено от администратора и е прието, че заявлението е надлежно подадено.

Предвид изложеното, администраторът на лични данни е предприел действия по заявлението за изтриване на данните по чл. 17 от Регламент 2016/679 в законоустановения срок, но в нарушение на чл. 12, параграф 3 от Регламент 2016/679 не е изпълнил задължението си за уведомяване на субекта на данни за предприетите действия.

При така констатираното нарушение жалбата следва да бъде уважена.

В допълнение към горното, процесуалният представител на П. заяви, че дружеството е сертифицирано по ISO за информационна сигурност. Въпреки това е допуснато нарушение. Няма спор, че личните данни са предоставени на администратора за обработване от самия жалбоподател, макар и в една неофициална процедура за подбор. Не е ясно обаче как се обработват тези данни –

не е представена политика за обработване на личните данни, която да посочва какви лични данни се обработват, за какви цели, по какъв начин се обработват, за какъв срок се съхраняват (в рамките на чл. 25к от ЗЗЛД) и др. Предвид изложеното, администраторът следва да изготви ясни правила за обработване на лични данни при подбор на персонал, включително и при специфични ситуации като разглежданата неофициална процедура.

Освен горното, липсват правила как се обработват постъпили по електронната поща, посочена в Търговския регистър, искания за упражняване на права по чл. 15-22 от Регламент 2016/679. От една страна, съгласно чл. 37б, ал. 2 от ЗЗЛД заявленията за упражняване на права могат да бъдат подадени по електронен път при спазване на съответните правила за идентификация (напр. с електронен подпис по Закона за електронния документ и електронните удостоверителни услуги). От друга страна, съгласно чл. 12, параграфи 2 и 6 от Регламент 2016/679, администраторът съдейства за упражняването на правата по чл. 15-22 от Регламента, но когато има основателни опасения във връзка със самоличността на физическото лице може да поиска допълнително информация за идентификация. В случай че не е в състояние да идентифицира лицето, администраторът може да откаже разглеждането на отправеното до него искане. **И в двете хипотези администраторът дължи отговор на искателя.** Освен това самото заявление следва да бъде заведено в регистратурата на администратора, за да бъде спазен принципът за отчетност по чл. 5, параграф 2 от Регламент 2016/679 – т.е. следва да има информация, че има постъпило заявление от субект на данни, какво е искането и какви са предприетите действия. В разглеждания случай заявлението е подадено без електронен подпис, но администраторът го е приел за надлежно и го е изпълнил, но не е отговорил. Предвид изложеното, администраторът следва да изготви и правила при получаване на заявления за упражняване на права по Регламента.

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.

В допълнение към горното, 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. Това следва да се вземе предвид при преценката дали да се наложи административното наказание „имуществена санкция" вместо друга корективна мярка по чл. 58, параграф 2 от Регламента или в допълнение към нея. Анализ на публикуваните данни на дружеството показва, че по смисъла на чл. 3 от Закона за малките и средните предприятия администраторът е средно предприятие.

С оглед посочените общи изисквания при определяне на корективна мярка, в разглеждания случай са налице и следните смекчаващи обстоятелства – нарушението е първо за администратора, нарушени са правата на един субект, освен това действия по заявлението му са предприети и при повторното запитване е получил отговор (макар и не конкретен), че заявленията са разгледани и личните данни са изтрити.

Предвид горното, най-целесъобразна мярка, която има за цел да предотврати бъдещи нарушения, е по чл. 58, пар. 2, буква „г” от Регламента – разпореждане до администратора на лични данни да съобрази операциите по обработване с изискванията на Регламента, като изготви и представи политика за обработване на лични данни в процедура за подбор на персонал, както и обработване на искания по чл. 15-22 от Регламент 2016/679, постъпили по електронен път.

При неспазване на разпореждане по чл. 58, параграф 2 от Регламент 2016/679 може да бъде наложена имуществена санкция по чл. 83, параграф 6 от Регламент 2016/679.

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

РЕШИ:

1. Обявява жалба рег. № ППН-02-31/24.01.2019 г., подадена от В.Т. за основателна за нарушение на чл. 12, параграф 3 от Регламент 2016/679;

2. На основание чл. 58, параграф 2, буква „г” от Регламент 2016/679 разпорежда на администратора „П.” ЕАД в едномесечен срок от влизане в сила на решението да изготви и представи пред КЗЛД политика за обработване на лични данни при подбор на персонал и за администриране на искания за упражняване на права по чл. 15-22 от Регламент 2016/679, получени по електронен път.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-17-151/2020 г.
гр. София, 15.05.2020 г.

ОТНОСНО: ***Групово тестване на служители за COVID-19***

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов и Веселин Целков, на заседание, проведено по реда на чл. 12 от Правилника за дейността на КЗЛД и на нейната администрация, разгледа писмо с вх. № ПНМД-17-151/09.04.2020 г. от адвокатско дружество с искане на основание чл. 80, ал. 1, т. 8 от Закона за защита на личните данни (ЗЗЛД), във връзка с чл. 51, т. 2 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация. С писмото се отправя молба за официално становище на Комисията, в контекста на предприеманите мерки за ограничаване разпространението на новия тежък остър респираторен синдром коронавирус 2 (SARS-CoV-2) и свързаната с него болест COVID-19.

От адвокатското дружество поставят редица въпроси относно груповото тестване с PCR тестове, т.нар. Pool PCR, като излагат свои мотиви по разглеждания казус, както следва:

1. Противоречи ли на приложимите в страната правила за защита на личните данни (Общ регламент относно защитата на данните (“ОРЗД”), Закон за защита на личните данни (“ЗЗЛД”)) груповото анонимизирано тестване за установяване дали са заразени с или преносители на COVID-19, когато се извършва в изпълнение на заповед на работодателя и при спазване на следните условия:

- Тестването се извършва в групи от 3 до 20 служителя;
- Във всяка група се вземат 3 - 20 единични намазки/тампони с проба от всеки служител поотделно;
- Намазките/тампоните се поставят заедно/едновременно в един активен разтвор, който се поставя в PCR машина за изследване;
- В резултат на изследването груповата проба е:
  - Отрицателна - не се предприемат последващи стъпки; пробите и резултатите се унищожават незабавно;
  - Положителна и тъй като не е известно кое лице/а са дали положителен резултат - данните остават анонимни. Като последваща стъпка всеки член на групата е поканен да се тества самостоятелно в независима лаборатория (като само той ще знае крайния резултат).

2. От адвокатското дружество очакват КЗЛД да даде указания при какви условия извършването на описания протокол за групово тестване в рамките на трудовото правоотношение не би противоречало на приложимите правила за защита на личните данни (например необходимо ли е съгласие на служителя; какво следва да се предприеме при установяване на заразен служител в предприятието на работодателя; в рискови производства, при които прекъсването на процеса на работа поради голям брой заболели служител би било критично за сигурността на страната и би създало допълнителни рискове от инциденти; в други случаи)?

За удобство на Комисията, от адвокатското дружество предоставят и следната допълнителна информация:

“ 1. Допустимост на обработването на чувствителни лични данни съгласно ОРЗД.

На 20.03.2020 г. Европейският комитет по защита на данните („ЕКЗД“) публикува официално Изявление относно обработването на лични данни в контекста на разпространението на COVID-19, в което потвърди, че ОРЗД урежда хипотези и правни основния (като чл. 9, пар. 2, букви „б“, „в“, „ж“ и „и“), въз основа на които е допустимо обработването на здравословни лични данни от страна на работодателите, без да е необходимо съгласие от страна на служителите. По-конкретно ЕКЗД посочва, че:

„В контекста на трудовите правоотношения, обработването на лични данни може да е необходимо за спазването на правно задължение, което се прилага спрямо работодателя, като напр. задължения, свързани с осигуряването на здравословни и безопасни условия на труд или с обществен интерес, напр. контрол на заболявания и други заплахи за здравето. В ОРЗД се предвижда също законосъобразността на обработването на специални категории лични данни, напр. здравни данни, когато това е необходимо по съображения от обществен интерес (член 9, параграф 2, б. „и“) въз основа на правото на Съюза или националното законодателство или когато е необходимо да се защитят жизненоважните интереси на субекта на данните (чл. 9, параграф 2, б. „в“), тъй като съображение 46 изрично се отнася до контрола на епидемия.“

2. Становища на националните надзорни органи по защита на личните данни на държавите членки.

Редица национални органи по защита на личните данни в ЕС вече издадоха насоки или становища относно допустимостта на обработването на лични данни в условията на COVID-19 пандемията и основните принципи, които трябва да се спазват при такова обработване. Например в:

• Австрия: националният орган приема категорично, че в контекста на задължението на работодателя да ограничава рисковете за здравето на служителите си той има право да запитва служителите дали попадат в рискова група от заразяване.

• Обединеното Кралство: съгласно официалните насоки с оглед на задължението на работодателите да осигурят безопасни условия на труд е допустимо да се събират данни дали служителите имат симптоми на заразяване с COVID-19. Ако това обаче не е достатъчно, националният орган допуска събирането на допълнителен набор здравословни данни при спазване на принципите на ОРЗД.

• Германия: в обща позиция на контролните органи на отделните федерални провинции се приема, че е допустимо „събиране и обработка на лични данни (включително здравни данни) на служителите от работодателя, за да се предотврати или ограничи разпространението на вируса сред служителите възможно най-добре“, особено ако е установено заразено лице или лице, по отношение на което е налице висок риск от заразяване съгласно официалните данни.

• Ирландия: допуска се попълване на здравни въпросници, особено при отчитане на организационни фактори, като например служителите, които често пътуват по работа или наличието на уязвими лица на работното място.

Като цяло, националните органи по защита на личните данни на държавите членки допускат събирането на индивидуални декларации за наличието на симптоми на заразяване (и потенциално прилагането на други подходящи мерки), чиято ефективност като превенция срещу заразяване е спорна, а по същество е свързана и със събиране на по-широк кръг лични данни (за пътувания, наличие на симптоми у служителя или негови контактни лица и пр.), отколкото при групови намазки, които ще се унищожават веднага.

3. Задължение на работодателя да осигурява здравословни условия на труд съгласно българското законодателство.

В България полагането на труд при наличието на здравословни и безопасни условия е конституционно признато право на работника и задължение на работодателя (срв. чл. 48, ал. 5 от

Конституцията на Република България). Конкретно изражение на това правило в националното законодателство са нормите на чл. 127, ал. 1, т. 3, чл. 275, ал. 1 и чл. 289 от Кодекса на труда и разпоредбите на Закона за здравословните и безопасни условия на труд ("ЗЗБУТ"), съгласно които работодателят е длъжен да осигури здравословни и безопасни условия на труд, така че опасностите за живота и здравето на работника или служителя да бъдат отстранени, ограничени или намалени. Тези задължения на работодателя кореспондират с уредбата в горепосочените национални режими и следва да се възприемат като основание по смисъла на чл. 9, пар. 2, б. „б" ОРЗД, даващо право на работодателя да прилага превантивни мерки, за която цел обработва чувствителни лични данни на служителите си.

4. Минимизиране и анонимизиране на здравословните лични данни при прилагане на предложения Протокол за групово тестване.

Видно от приложения Протокол за групово тестване, пробите на отделните служители (представляващи техни лични данни) ще бъдат анонимизирани чрез агрегиране и К-анонимност. В Становище 05/2014 относно техническите способи за анонимизиране, прието на 10 април 2014 г. от Работната група по чл. 29 („Становището"), агрегирането на данни и прилагането на К-анонимност са едни от признатите способи за трайно анонимизиране на лични данни:

• *„Полученият масив от данни може да бъде квалифициран като анонимен само ако администраторът на данни агрегира данните до ниво, на което събитията, касаещи отделни лица, вече не подлежат на идентифициране."* - стр. 10 от Становището;

• *„Когато става дума за k-анонимност, параметърът от решаващо значение е прагът на k. Колкото по-голяма е стойността на k, толкова по-стабилни са гаранциите за неприкосновеността на личния живот."* - стр. 19 от Становището.

Съгласно съображение (26) на ОРЗД: *„принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран. Ето защо настоящият регламент не се отнася за обработването на такава анонимна информация, включително за статистически или изследователски цели."*

5. Предимства на предложения протокол за групово тестване.

• Работодателят използва анонимизиран агрегиран масив от данни (групови проби), чрез които прилага единствената доказано ефективна мярка за превенция срещу заразяване с COVID-19 - тестване с PCR тест, като при това реализира до 1/20 по-малко разходи;

• Здравословните данни се вземат и обработват от лаборатории в качеството им на независими администратори на лични данни и в рамките на обичайната им дейност;

• При положителен резултат в дадена групова проба, служителите се канят доброволно да се изследват в лаборатория без задължение да предоставят резултатите на работодателя. Работодателят има право единствено отново да ги подложи на анонимизирано групово тестване, включвайки ги в друга тестова група;

• При нормални условия, работодателят така или иначе обработва идентичен набор от данни:

  ○ При представяне на болничен лист служителят с положителна проба разкрива лични данни, които е длъжен по закон да разкрие, за да може да се ползва от правото да излезе в болничен, а работодателят е длъжен да ги обработи;

  ○ При групова отрицателна проба, работодателят научава само, че служителите му са здрави, която информация се презюмира и от факта, че последните не са му предоставили болничен лист и не отсъстват от работа.

• При прилагане на Протокола за Групово тестване в много по-голяма степен се спазват принципите на ОРЗД (доколкото се счетат за приложими с оглед на анонимизирания характер на груповата проба): данните са сведени до минимум (само тези, които са изрично необходими за преследваната цел, без анализ на пътувания, контакти през последните седмици и др.), като се ограничава възможността да бъдат използвани за други цели - тъй като се предават на сертифицирани лаборатории и самите проби трудно биха намерили приложимост за други цели, преследвани от работодателя.“

С оглед на срока от един месец от постъпване на искането в дирекция „Правно- нормативна и международна дейност” за изготвяне и представяне на Комисията на предложение за становище, както е предвидено в член 52 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация, но най-вече с оглед на необходимостта от спешни мерки и решения за ограничаване разпространението на COVID-19 от адвокатското дружество учтиво молят Комисията да изрази своето официално становище по въпросите по-горе във възможно най-кратък срок.

Към искането е приложен Протокол за групово тестване със следното съдържание:

Механизъм за доброволно тестване на фирмени служители срещу COVID-19

Защо е важно да се диагностицира рано COVID-19?

Средният инкубационен период - времето от заразяването до проявата на първите признаци на болестта COVID-19 е 5-6 дни на база на статистика от Световната здравна организация. Научни статии показват, че средно на четвъртия ден след заразяването COVID-19 може да се предава, което е 1-2 дни преди първите симптоми. Този период може да бъде и по-дълъг, защото при 2.5% от населението първите симптоми се проявяват чак на 12 ден. Точно този различно дълъг „мълчалив“ период е най-опасен - без да подозира, заразеният (но без оплаквания) може да предава вируса.

Точният метод за детекция през PCR дава възможност за откриване на заразени лица 1-3 дни преди първите симптоми. Това означава, че средно PCR детекцията може да засече позитивен пациент от 2-3 дни след заразяване.

Тези данни показват, че средностатистически сроковете при заразяване с COVID-19 са следните:

Ден 0: заразяване;

Ден 2-3: PCR тестване може да открие позитивните случаи на заразяване;

Ден 4-5: заразеният служител може да предава заразата на други служители;

Ден 5-6: първи признаци на болестта се проявяват и рискът от предаване на заразата се увеличава.

При тестване всеки ден с PCR, реално могат да се засекат заразени служители и да се изолират, преди да заразят останалия колектив на съответната компания.

Оптимизация на разходите за тестване на служителите чрез (Pool PCR)

Изследвания в Германия и Израел показват, че могат успешно да се тестват групи от 5 до 64 човека в зависимост от използвания тест с единични Real-time PCR тестове (Pool PCR). Протоколът за работа при този тип групови тестове включва вземане на секрет от гърлото и носа на всеки член от група от хора, използвайки стандартните достъпни тампони и събирането им в една обща транспортна среда, която е част от набора на използваните и в момента консумативи за

пробовземане и транспортиране на пробите за последващ PCR тест. На практика с увеличаване на броя хора в тестваната група, възможността за детекцията на коронавируса в общата група се увеличава, защото една и съща среда се обогатява с допълнителните индивидуални проби на всеки отделен член на групата, а не се разрежда, надвишавайки по този начин минималните нива в пробата, необходими за точна детекция.

Ако компания реши да пуска по един тест два пъти на седмица, събирайки пробите от 20 служителя, разходът за един PCR тест се разпределя върху 20 служителя, което го прави приемливо за повечето работодатели. Така компанията ще може да тества 20 служителя на цената на един и в същото време да не преустановява работа.

Протокол на тестването:

1) Подготвят се 2 милилитра вирусна транспортна среда заедно с тестови тампони за взимане на носови и гърлени проби. (Установено е, че най-рано вирусът се открива в носната лигавица, а едва по-късно - гърлената. Именно затова за ранно откриване на инфекцията е важно да се вземе т.нар. назо-фарингеален секрет.) За период от 3 последователни дни, всеки ден медицинско лице взима носен и гърлен секрет на групи от по 10 до 20 служителя и всеки ден поставя/потапя тампоните с гърлен секрет в подготвената предварително транспортна среда, като по този начин набогатява допълнително транспортната среда през тридневния период. В някои случаи може и самите служители да си взимат секрет доброволно сами на себе си, но съществува риск от намаляване на точността на теста поради грешно взимане на пробата.

2) На третия ден, транспортната среда (заедно с поставените в нея тампони с гърлен секрет от съответната група служители) се изпраща за изследване в PCR лаборатория.

3) При отрицателна проба, работодателят знае, че цялата група от 10 до 20 служителя е отрицателна. При положителна проба, работодателят може да препоръча на служителите в съответната група да си направят индивидуални тестове в лаборатория, за да разберат кой е източникът на положителната проба (като поеме или не разноските за това тестване).

На работодателя се препоръчва колко служителя да сложи в група за една лабораторна проба в зависимост от чувствителността на използвания PCR тест. Разбира се, колкото по-голяма е групата, толкова по-ниска е цената за тестване на отделен служител. При положителна групова проба ще бъде необходимо да се правят по-голям брой индивидуални тестове. По отношение на служители, попадащи в рисковите групи от заразяване с COVID-19, по-оптимално би било да се включват в по-малки на брой първоначални групи; при по-ниско рискови служители по-голямата първоначална група е по-подходяща.

Протоколът може да варира в зависимост от разходите, които работодателят е склонен да направи.

Възможни са следните вариации:

1) Всеки ден се взима по една проба от всеки служител в съответната група и се набогатява транспортната вирусна среда, и всеки 3 дни тази среда се изпраща за тест (срв. по-горе). Този протокол дава възможност за най-нисък риск от предаване на неиндефицирана инфекция от COVID-19 между служителите. Този протокол изисква и най-голяма инвестиция от работодателя и спокойно може да бъде заменен от следващите.

2) Един път на всеки 3 дни се взима по една проба от всеки служител в групата и се набогатява транспортната вирусна среда, и всеки 3 дни тази среда се изпраща за тест. Този протокол дава възможност за нисък риск от предаване на неиндефицирана инфекция от COVID-19 между служителите. Този протокол изисква също сравнително голяма инвестиция от работодателя и заедно със следващия е най-подходящ за практиката.

3) Всеки ден се взема по една проба от всеки служител в групата и се набогатява транспортната вирусна среда, и всяка седмица тази среда се изпраща за тест. Този протокол дава възможност за намаляване на риска от предаване на неиндефицирана инфекция от COVID-19 между служителите, но вече има опасност в края на седмицата някой от служителите да е заразен и да заразява другите служители.

4) Един път на седмица се взима по една проба от всеки служител в групата и се набогатява транспортната вирусна среда, и всяка седмица тази среда се изпраща за тест. Този протокол е с най-ниската инвестиция от работодателя, намалява риска от заразяване на служителите, но допуска съществуването на риск в края на седмицата някой от служителите да е заразен и да заразява другите служители.

Приложения: Към искането са приложени редица линкове към цитираните материали, които са на разположение на КЗЛД.

Правен анализ:

В разпоредбата на чл. 4, т. 7) от Регламент (ЕС) 2016/679 е разписана дефиницията на понятието „администратор“, което означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка. Ако разгледаме подробно представения казус, може да се установи, че в конкретния случай е налице администратор на лични данни – даден работодател, който с оглед създалата се кризисна обстановка решава да предприеме действия по ограничаване и/или предотвратяване на заразяването на своите служители с пандемичната болест. За да бъдат законосъобразни действията на работодателя, същият трябва да действа в хипотезата на възможните законови основания за това, и тъй като ще се обработват лични данни в този контекст, следва да се спазят всички принципи и задължения, произтичащи от Регламент (ЕС) 2016/679.

Съгласно чл. 275, ал. 1 от Кодекса на труда (КТ) работодателят е длъжен да осигури здравословни и безопасни условия на труд, така че опасностите за живота и здравето на работника или служителя да бъдат отстранени, ограничени или намалени. С разпоредбата на чл. 282 от КТ се въвежда задължението работодателят да осигурява условия за санитарно-битово и медицинско обслужване на работниците и служителите съобразно санитарните норми и изисквания.

Законът за здравословни и безопасни условия на труд (ЗЗБУТ) регламентира правата и задълженията на работодателите и работещите за осигуряване на здравословни и безопасни условия на труд. Мерките, които може да прилага работодателят в съответствие с чл. 4, ал. 1 от ЗЗБУТ са изчерпателно изредени:

1. превенция на професионалните рискове;

2. предоставяне на информация и обучение;

3. осигуряване на необходимата организация и средства.

В условията на извънредно положение, Министърът на труда и социалната политика издаде Заповед № РД01-219 от 02.04. 2020 год. (На основание чл. 276, ал. 1 от Кодекса на труда, във връзка с чл. 36, т. 2 от Закона за здравословните и безопасни условия на труд и обявеното извънредно положение с решение на Народното събрание от 13 март 2020 г.), с която определя мерките за превенция на риска от разпространяване на COVID-19 и включва инструкции за осигуряване на подходящи условия на

труд. Заповедта не предвижда задължения за работодателите да тестват своите служители. Съгласно Изявлението на Европейския комитет по защита на данните относно обработването на лични данни в контекста на пандемията от COVID-19 (прието на 19 март 2020 г.), „възможността работодателите да извършват медицински прегледи (в широк смисъл и изследвания) на служителите си като цяло зависи от уредбата в националните законодателства в областта на трудовата заетост или здравето и безопасността.“ Тъй като българското законодателство не предвижда изрично такива мерки, за работодателите остава възможността да организират изследването, но не и да го извършват сами. В този смисъл за тях отпада необходимостта да обработват на този първоначален етап данни за здравето, включително данни за генетичния материал, какъвто се съдържа в пробите за PCR-теста. Въпросните тестове се извършват в лицензирани лаборатории от медицински специалисти, като към всички изследвани лица се пристъпва като към заразени, с оглед превенция на здравните работници и разпространение на заразата. Тъй като към момента на вземането на решение за тестване, работодателят не обработва данни за здравето или друг вид специални категории данни, може да се направи обосновано предположение, че воден от своите легитимни интереси да планира и да осигурява непрекъснатост на трудовия процес, работодателят предприема мерки за запазването на здравето на своите служители в условията на здравна криза, като осигурява тяхното тестване. В този смисъл, може да се търси приложение на хипотезата на чл. 6, пар. 1, б. „е“ от Регламент (ЕС) 2016/679 - обработването е необходимо за целите на легитимните интереси на администратора …, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни. Когато се позовава на това основание за обработване на лични данни, администраторът (в случая работодателят) следва да извърши тест за балансиране, за да прецени доколко интересите му биха имали преимущество пред правата и свободите на субектите на данни – негови служители. С оглед специфичния характер на ситуацията, в която се намираме, при извършването на теста за балансиране следва да се отчетат и рисковете, произтичащи от икономическата дейност, възможността за по-голямо взривно разпространение на заразата, ако не се приложат планираните мерки и т.н.

Само след като тестът за балансиране установи, че преимущество имат легитимните интереси на работодателя, същият би могъл да пристъпи към издаване на акт, с който да задължи служителите си да се подложат на PCR-тест за COVID-19.

Работодателят ще обработва данни за здравето на следващ етап, евентуално когато негов служител представи болничен лист, за да удостовери, че се е лекувал от COVID-19. До този момент, за работодателят не възниква необходимост за обработване на данни за здравето.

Обработването на данни за здравето (дали едно лице е заразено или не, изследване на генетичния материал, съдържащ се във взетите проби и т.н.) се извършва от лицензирани лаборатории, които при наличие на положителна проба, макар и при групово изследване, имат протоколи за откриване на заразеното лице и уведомяване на властите за последващи мерки. В този смисъл не може да се разчита на съгласието за последващо изследване, поради високия риск от разпространението на болестта. За съответните лаборатории, както и за здравните власти, като администратори на лични данни, се прилагат подходящите основанията на чл. 9, пар. 2 от Регламент (ЕС) 2016/679, включително обществения интерес, който е присъщ обикновено на публичните органи.

Доколкото целта е разкриването на заразените лица от компетентните здравни власти, не може да се разсъждава по посока на каквото и да е анонимизиране на пробите. Следва да се отбележи, че агрегирането на известен брой проби на точно определен малък брой лица (5-20), които за съответния пул по протокол трябва да са идентифицирани, не може да доведе до анонимизиране на данните, защото вероятността лицето да бъде идентифицирано пряко или косвено е голяма. Същото не е и необходимо, тъй като не кореспондира с целта на обработването на този вид данни в конкретния случай, а именно установяването на заразения.

Следва да се обърне внимание, че в конкретния случай КЗЛД се произнася на основание чл. 58, пар. 3, буква б) от Регламент (ЕС) 2016/679, тъй като Глава VIII от ЗЗЛД, към която принадлежи чл. 80, транспонира Директива (ЕС) 2016/680 и не се прилага за разрешаването на настоящия казус.

Настоящият анализ е базиран изцяло на трайната практика на КЗЛД, свързана с обработването на лични данни на субекти на данни за здравни цели, както и на съдебната практика по жалби с такъв предмет и на указанията на Европейския комитет по защита на данни в тази насока. Становището на КЗЛД има консултативен характер за администратора на лични данни при прилагане на относимите правни норми. Това становище има единствено разяснителен характер по приложението на коментираните в него норми, без да поражда права и/или задължения за заинтересованите страни. Съгласно Регламент (ЕС) 2016/679 - Общ регламент относно защитата на данните, администраторът на лични данни сам или съвместно с друг администратор определя правилата и процедурите за обработване на данни, които трябва да са съответстват на закона и регламента. За предприетите от администратора или съвместните администратори действия по обработване на данните се прилагат както правилата на отчетност, прозрачност, добросъвестност, така и нормите отнасящи се до носене на административнонаказателна отговорност по отношение на законосъобразността на осъществяваните от него/тях обработвания.

Предвид горното и на основание чл. 58, пар. 3, б. „б“ от Общия регламент относно защитата на данните вр. с чл. 10а, ал. 1 от Закона за защита на личните данни, КЗЛД изразява следното

СТАНОВИЩЕ:

1. Работодателят може да издаде заповед за задължително групово тестване за установяване на заразени или приносители на COVID-19 сред своите служители при условията на чл. 6, пар. 1, б. е) от Регламент (ЕС) 2016/679, само ако тестът за балансиране покаже, че неговите легитимни интереси имат преимущество пред правата и свободите на субектите на данни (неговите служители).

2. Обработването на данни за здравето и данни от пробите, съдържащи генетичен материал на изследваните лица за COVID-19 чрез групови PCR-тестове, може да се извърши само от компетентните здравни власти, които са обвързани със задължението за професионална тайна и съобразно приложимото законодателство.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-17-114/2020 г.
гр. София, 26.05.2020 г.

ОТНОСНО: ***Обработване на лични данни относно здравето и степен на информиране на служителите в случай на наличие на инфектиран с COVID-19 служител***

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 19.05.2020 г., разгледа преписка с вх. № ПНМД-17-114/17.03.2020 г., с която управителят на Е. ЕООД – д-р П.В. се обръща към Комисията с искане за изразяване на становище във връзка с обработване на данни за здравето на служителите в контекста на пандемията от COVID-19. Във връзка с това към Комисията се отправят следните въпроси:

1. Има ли право работодателят да изисква от служителите си (които работят от домовете си) информация за това дали са заразени с COVID-19, те или членовете на техните домакинства, а също и дали се намират в карантина поради съмнения за заболяване, при положение, че до петък 13 март са били на работните си места и предприятието е функционирало в нормален порядък и всеки служител е бил контактен със своите колеги (уточнява се, че броят на служителите е над 100)?

2. В случай, че се установи по категоричен начин заразен с COVID-19 служител на дружеството или член на неговото домакинство, имаме ли право да уведомим останалите служители за този факт, както и по какъв начин трябва да се осъществи това обработване на данни (споделяне на информация относно здравословното състояние с останалите служители) така, че да не се нарушават разпоредбите на Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД)?

Правен анализ:

Съгласно чл. 275, ал. 1 от Кодекса на труда (КТ) работодателят е длъжен да осигури здравословни и безопасни условия на труд, така че опасностите за живота и здравето на работника или служителя да бъдат отстранени, ограничени или намалени. С разпоредбата на чл. 282 от КТ се въвежда задължението работодателят да осигурява условия за санитарно-битово и медицинско обслужване на работниците и служителите съобразно санитарните норми и изисквания.

Законът за здравословни и безопасни условия на труд (ЗЗБУТ) регламентира правата и задълженията на работодателите и работещите за осигуряване на здравословни и безопасни условия на труд. Мерките, които може да прилага работодателят в съответствие с чл. 4, ал. 1 от ЗЗБУТ са изчерпателно изредени:

1. превенция на професионалните рискове;

2. предоставяне на информация и обучение;

3. осигуряване на необходимата организация и средства.

В условията на извънредно положение, Министърът на труда и социалната политика издаде Заповед № РД01-219 от 02.04. 2020 год. (На основание чл. 276, ал. 1 от Кодекса на труда, във връзка с чл. 36, т. 2 от Закона за здравословните и безопасни условия на труд и обявеното извънредно положение с решение на Народното събрание от 13 март 2020 г.), с която определя мерките за превенция на риска от разпространяване на COVID-19 и включва инструкции за осигуряване на подходящи условия

на труд. Въпросната заповед има действие на работното място в помещенията на работодателя. Доколкото въпросът се отнася до информация за здравословното състояние на служителите, които работят от вкъщи, не е подходящо заложените мерки да са задължително приложими в домашни условия, с оглед на това, че контролът на работодателя не може да се разпростре и върху дома и семейството на неговите служители. В този смисъл липсва правно основание работодателят да изисква предоставянето на такава информация от страна на служителите, тъй като те към този момент, намирайки се в социална изолация, не застрашават здравето на колектива. Това зависи от режима на работа и от срещите между служителите. Възможно е поради особеностите на заболяването, самият служител да не знае, че е заразен и поради това евентуално предоставена от него информация да не отговаря на истината.

На работодателите се дава възможност да проверяват температурата на служителите, които посещават работното си място и при наличието на симптоми да отстранят евентуално заразения служител. Работодателят е длъжен да въведе пропускателен режим, който да гарантира контрол и недопускане на територията на предприятието на работници и служители, както и на външни лица, с прояви на остри заразни заболявания. В случай, че се установи заразен служител на територията на предприятието, работодателят може да уведоми здравните власти, които в рамките на своята компетентност да предприемат определени действия. Законосъобразното обработване на лични данни се извършва единствено при наличие на поне едно от основанията, посочени в чл. 6, пар. 1 или чл. 9, пар. 2, когато става въпрос за специални категории данни, както и при задължителното спазване на принципите за обработване, посочени в чл. 5 от Регламент (ЕС) 2016/679. В конкретния случай здравните власти могат да извършват своята дейност на основание чл. 9, пар. 2, буква и) от Регламент (ЕС) 2016/679 - обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето …, въз основа на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна.

Работодателят може да предостави информация на колектива за наличието на заразен служител, без да предоставя данни за неговото идентифициране, когато такъв е установен по безспорен начин на основание чл. 4, ал. 1 от ЗЗБУТ. Здравните власти следва да извършат действията по откриването на контактните лица и съответното им изследване.

По отношение на лицата, които работят от вкъщи, тъй като няма правно основание да се изисква информация за здравословното състояние, такава информация може да се обработва единствено в хипотезата на чл. 9, пар. 2, буква д) от Регламент (ЕС) 2016/679, когато обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните, т.е. когато самото лице е споделило за наличието на заразата. Друга хипотеза е когато работодателят обработва данни за здравето, когато негов служител представи болничен лист, за да удостовери, че се е лекувал от COVID-19. До работодателя може да достигне информация за заболяването на член на домакинството на служителя, в случай че болничният лист е издаден във връзка с грижата за него. Такова обработване на данни за здравето се основава на разпоредбата на чл. 9, пар. 2, буква б) от Регламент (ЕС) 2016/679 - обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотолкова, доколкото това е разрешено от правото на Съюза или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните. До представянето на болничния лист, за работодателя не възниква необходимост за обработване на данни за здравето на лицето, което работи от вкъщи.

Обработването на данни за здравето (дали едно лице е заразено или не, изследване на генетичния материал, съдържащ се във взетите проби и т.н.) се извършва от лицензирани лаборатории, които

при наличие на положителна проба, макар и при групово изследване, имат протоколи за откриване на заразеното лице и уведомяване на властите за последващи мерки. В този смисъл не може да се разчита на съгласието за последващо изследване, поради високия риск от разпространението на болестта. За съответните лаборатории, както и за здравните власти, като администратори на лични данни, се прилагат подходящите основанията на чл. 9, пар. 2 от Регламент (ЕС) 2016/679, включително обществения интерес, който е присъщ обикновено на публичните органи.

Настоящият анализ е базиран изцяло на трайната практика на КЗЛД, свързана с обработването на лични данни на субекти на данни за здравни цели, както и на съдебната практика по жалби с такъв предмет и на указанията на Европейския комитет по защита на данни в тази насока. Становището на КЗЛД има консултативен характер за администратора на лични данни при прилагане на относимите правни норми. Това становище има единствено разяснителен характер по приложението на коментираните в него норми, без да поражда права и/или задължения за заинтересованите страни. Съгласно Регламент (ЕС) 2016/679 - Общ регламент относно защитата на данните, администраторът на лични данни сам или съвместно с друг администратор определя правилата и процедурите за обработване на данни, които трябва да са съответстват на закона и регламента. За предприетите от администратора или съвместните администратори действия по обработване на данните се прилагат както правилата на отчетност, прозрачност, добросъвестност, така и нормите отнасящи се до носене на административнонаказателна отговорност по отношение на законосъобразността на осъществяваните от него/тях обработвания.

Във връзка с горепосоченото и на основание чл. 58, § 3, б. „б“ от Регламент (ЕС) 2016/679, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Няма правно основание за изискването на информация от служителите, които работят от вкъщи, относно тяхното здравословно състояние и това на членовете на семейството им. Работодателят може да въведе пропускателен режим на територията на предприятието, само когато конкретната трудова дейност налага това. Всички останали мерки свързани с издирването на контактните лица на заразения са в правомощията на здравните власти.

2. Работодателят може да предостави информация на колектива за наличието на заразен служител, без да предоставя данни за неговото идентифициране, и когато такъв е установен по безспорен начин на основание чл. 4, ал. 1 от ЗЗБУТ. Здравните власти следва да извършат действията по откриването на контактните лица и съответното им изследване.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Рег. № ПНМД-01-41/14.04.2020 г.
гр. София, 26.05.2020

Относно: ***Предоставяне на данни на общините от регистри Национална база данни „Население" и Класификатор на настоящите и постоянните адреси с първичен администратор Министерството на регионалното развитие и благоустройството, чрез средата за междурегистров обмен Regix с цел проверка на подаваната от родителите информация, която се ползва единствено за приема на децата в общинските детски градини и ясли и на учениците в първи клас на общинските училища.***

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 19.05.2020 г., във връзка с постъпили в Комисия за защита на личните данни (КЗЛД) няколко идентични искания за изразяване на становище от страна на същата, обсъди въпроса за наличието на правна възможност за получаване на справки от общини от регистър Национална база данни „Население" и Класификатора на настоящите и постоянните адреси с първичен администратор Министерството на регионалното развитие и благоустройството (МРРБ), чрез средата за междурегистров обмен Regix, с цел проверка на подаваната от родителите информация, която се ползва за приема на децата в общинските детски градини и ясли и на учениците в първи клас на общинските училища. Исканията са свързани с получен отказ или прекратяване на подаването на такива справки от страна на Държавната агенция „Електронно управление" и Главна дирекция „Гражданска регистрация и административно обслужване" към Министерство на регионалното развитие и благоустройството. Като мотив се посочва липсата на законово основание.

КЗЛД счете, че е целесъобразно да изрази принципно становище по посочения проблем, като с него официално да бъдат запознати председателя на Държавната агенция „Електронно управление" и директора на Главна дирекция „Гражданска регистрация и административно обслужване" към МРРБ.

Настоящият анализ е базиран изцяло на трайната практика на КЗЛД, свързана с обработването на лични данни на субекти на данни от регистър ГРАО, както и на съдебната практика по жалби с такъв предмет и на указанията на Европейския комитет по защита на данни в тази насока. Становището на КЗЛД има консултативен характер за администратора на лични данни при прилагане на относимите правни норми. Това становище има единствено разяснителен характер по приложението на коментираните в него норми, без да пораждат права и/или задължения за заинтересованите страни. Съгласно Регламент (ЕС) 2016/679, администраторът на лични данни сам или съвместно с друг администратор определя правилата и процедурите за обработване на данни, които трябва да са съответстват на закона и регламента. За предприетите от администратора или съвместните администратори действия по обработване на данните се прилагат както правилата на отчетност, прозрачност, добросъвестност, така и нормите отнасящи се до носене на административно-наказателна отговорност по отношение на законосъобразността на осъществяваните от него/тях обработвания.

Правен анализ:

Гражданската регистрация включва съвкупност от данни за едно лице, които го отличават от другите лица в обществото и в семейството му, в качеството на носител на субективни права, като име, гражданство, семейно положение, родство, постоянен адрес и др. Гражданската регистрация на физическите лица в Република България се основава на данните в актовете за тяхното гражданско състояние и на данните в други актове, посочени в закон. Вписването в регистъра на населението

се извършва в общините по постоянен адрес на физическите лица. В регистрите на актовете за гражданското състояние се вписват (в населеното място, в което е настъпило събитието) събитията раждане, брак и смърт за всички лица, които към момента на настъпване на събитието са български граждани, и за лицата, които не са български граждани, но към момента на настъпване на събитието се намират на територията на Република България, като отговорността за гражданската регистрация на територията на конкретната община е на кмета на общината, съобразно разпоредбата на чл. 4, ал. 3 от Закона за гражданската регистрация (ЗГР).

Съгласно чл. 22 от ЗГР, регистърът на населението се поддържа в електронен вид и формира Национална база данни „Население". Регионална база данни „Население" е част от регистъра на населението и се състои от електронните лични регистрационни картони на физическите лица с постоянен и/или настоящ адрес в областта. Локална база данни „Население" е част от регистъра на населението и се състои от електронните лични регистрационни картони на физическите лица с постоянен и/или настоящ адрес в общината. В чл. 24 от ЗГР е разписано, че общинската администрация издава удостоверения въз основа на регистъра на населениетоРегистрите за гражданското състояние и регистърът на населението се създават и поддържат от Единната система за гражданска регистрация и административно обслужване на населението (ЕСГРАОН), която е национална система за гражданска регистрация на физическите лица в Република България и източник на лични данни за тях (чл. 100-101 ЗГР).

Съгласно чл. 3 от Закона за електронното управление (ЗЕУ) първичният администратор на данни изпраща служебно и безплатно данните на всички административни органи, на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, които въз основа на закон също обработват тези данни и са заявили желание да ги получават. По смисъла на чл. 2, ал. 2 от ЗЕУ първичен администратор е административен орган, който по силата на закон събира или създава данни за гражданин или организация за първи път и изменя или заличава тези данни. Той предоставя достъп на гражданите и организациите до цялата информация, събрана за тях. Същевременно чл. 8, ал. 2 от ЗЕУ задължава административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги, да предоставят всички услуги в рамките на своята компетентност и по електронен път, освен ако закон предвижда особена форма за извършване на отделни действия или издаване на съответни актове. Това задължение е скрепено и с изрично нормативно изискване за събиране, обработване и предоставяне на лични данни само в минимално необходимия обем за предоставяне на съответната услуга, като е гарантирано обработване на данните само за посочените цели, освен при наличие на изрично съгласие на субектите на данни (чл. 16 от същия закон). ЗЕУ вменява задължение на Държавната агенция „Електронно управление" да подсигури и поддържа техническа инфраструктура и информационна система, която да позволи фактическото и ефективно прилагане на електронното предоставяне на услуги. Съгласно Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, подаването на електронни документи се осъществява чрез публично достъпно уеб базирано приложение в Единния портал за достъп до електронните административни услуги и в официалните интернет страници на доставчиците на електронни административни услуги.

С оглед на приетата от Министерски съвет Стратегия за развитие на държавната администрация 2014 – 2020 год. и пътна карта към нея е заложено въвеждането на комплексно административно обслужване като иновативна форма в полза на гражданите и бизнеса. В тази връзка, с протоколно Решение № 23.8 от заседание на Министерски съвет, проведено на 19 юни 2013 г. е приет Базисен модел на комплексно административно обслужване, представляващ обща универсална рамка за въвеждане на комплексно административно обслужване в държавната администрация. Съгласно него, следва да се прилага служебното събиране на доказателства, регламентирано в чл. 36 от Административнопроцесуалния кодекс във връзка с изискването за еднократно събиране и създаване на данни и служебно уведомяване, предвидени в чл. 2, ал. 1 и чл. 3 от Закона за електронното управление.

С Решение № 338 на Министерския съвет от 23 юни 2017 г. са предприети мерки за намаляване на административната тежест върху гражданите и бизнеса чрез премахване на изискването за представяне на някои официални удостоверителни документи на хартиен носител. В приложението към т. 1, б. „а" на ПМС са дефинирани съответните удостоверителни услуги. За издаването на удостоверенията от списъка на услугите, администрациите използват справки от регистри, като съдържащите се в тях данни се извличат от администрациите автоматизирано по електронен път.

Възможността за предоставяне на тези услуги е реализирана чрез средата за междурегистров обмен (RegiX), която предоставя интерфейс за автоматизирано подаване и обслужване на стандартизирани заявки за административни услуги по електронен път. С разработените компоненти, необходими за свързване на информационните системи на администрациите, е осигурена възможността за потребителите на информация да извличат данни от основни регистри, сред които са Национална база данни „Население", регистър БУЛСТАТ, Имотен регистър, Търговски регистър.

Посредством междурегистровия обмен е създадената възможност за реализиране на вътрешни електронни административни услуги, което е предпоставка за постигане на една от основните цели на електронното управление, залегнало и в чл. 58а, т. 5 от ЗЕУ – комплексно административно обслужване на гражданите и бизнеса. Този обмен се осъществява след идентифициране на всеки административен орган, регистриран в обща система за достъп, поддържана от Министерския съвет (Regix), която издава уникален идентификационен код за достъп на отделната администрация, който позволява проследяване на всяко влизане в системата за междурегистърен обмен и установяване на вида и обема данни, черпени от съответните достъпни регистри.

Регламент (ЕС) 2016/679 е нормативният акт, определящ правилата, свързани със защитата на физическите лица при обработването на личните им данни и относно свободното движение на тези данни.

Съгласно чл. 4, т. 1 от Регламент (ЕС) 2016/679, „лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни") 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. „Обработване на данните" на субекта е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване (чл. 4, т. 2 от Общия регламент относно защитата на данните).

Във всички случаи на осъществяване на действия по предоставяне на лични данни на субекта или на трети лица от регистрите на населението или от регистрите на актовете за гражданското състояние, същите съставляват действия по обработване на лични данни по смисъла на Общия регламент относно защитата на данните.

Предоставянето на информация, съдържаща лични данни, от страна на администратор, в конкретния случай МРРБ, на друг администратор в лицето на община, би могло да се извърши само при наличието на една от хипотезите, визирани в чл. 6, пар. 1 от Регламент (ЕС) 2016/679 (условия за законосъобразно обработване на данни) и при стриктното спазване на принципите, разписани в чл. 5, пар. 1 от същия (принципи, свързани с обработването на данните). От особена важност в конкретния случай е да се определи изчерпателно обемът от данни, достатъчен и необходим за изпълнението на поставените пред администраторите цели

Съгласно чл. 106, ал. 1 от Закона за гражданската регистрация (ЗГР), данните от ЕСГРАОН се предоставят на:

1. българските и чуждестранните граждани, както и на лицата без гражданство, за които се отнасят, а също така и на трети лица, когато тези данни са от значение за възникване, съществуване, изменение или прекратяване на техни законни права и интереси;

2. държавни органи и институции съобразно законоустановените им правомощия;

3. български и чуждестранни юридически лица - въз основа на закон, акт на съдебната власт или разрешение на Комисията за защита на личните данни.

Съгласно чл. 256, ал. 1, т. 2 от Закона за предучилищното и училищното образование (ЗПУО) органите на местното самоуправление осигуряват и контролират обхвата на подлежащите на задължително предучилищно и училищно образование деца и ученици.

Съгласно разпоредбите на чл. 59. ал.1 от Закона за предучилищното и училищното образование - условията и редът за записване, отписване и преместване в общинските детски градини се определят с наредба на общинския съвет, а за държавните детски градини - с акт на съответния финансиращ орган. Във връзка с чл. 7, ал. 1 от Наредба № 5 от 03.06.2016 г. за предучилищното образование - записването, отписването и преместването в общинските детски градини за всеки вид организация се извършват съгласно наредба на общинския съвет, а за държавните детски градини - с акт на съответния финансиращ орган.

Предвид чл. 24, ал. 1 от ЗПУО, където се посочва, че детската градина е институция в системата на предучилищното и училищното образование и следователно попада в хипотезата на чл. 106, ал. 1, т. 2 от ЗГР, съгласно който данните от ЕСГРАОН се предоставят на държавни органи и институции съобразно законоустановените им правомощия.

Идентично е съдържанието на чл. 25, ал. 1 от ЗПУО, определящо статута на училищата (чл. 25, ал. 1. *Училището е институция в системата на предучилищното и училищното образование, в което...*)

От гореизложеното следва, че общините обработват лични данни на основание чл. 6, пар. 1, б. „в" от Регламент (ЕС) 2016/679, когато обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора. В случая следва да се вземе предвид съображение 41 от Общия регламент относно защитата на данните, съгласно което, когато се прави позоваване на правно основание или законодателна мярка, това не налага непременно приемането на законодателен акт от парламент, без с това да се засягат изискванията съгласно конституционния ред на съответната държава членка. Такова правно основание или законодателна мярка обаче следва да бъдат ясни и точни и прилагането им следва да бъде предвидимо за лицата, за които се прилагат. Нещо повече, доколкото МРРБ попада в обхвата на легалната дефиниция на „първичен администратор" по смисъла на ЗЕУ, за него е налице задължение за служебно и безплатно предоставяне на исканите от общините данни по силата на чл. 3 от същия закон, след като тези данни вече се обработват от заявителя и той, в качеството си на административен орган, е изразил желание за получаването им с цел поддържане в актуален вид.

При спазването на принципите за обработване на личните данни, по-специално принципът за ограничаване на данните, е необходимо да се изясни обемът от данни, които са нужни на общините, за да изпълнят поставените цели, а именно – да проверят декларираните от родителите факти и обстоятелства.

Същевременно, съгласно чл. 5, пар. 1, б „г" от Общия регламент относно защитата на данните, задължение на общините, в качеството им на администратор на лични данни, е да поддържат данните точни и при необходимост да ги актуализира, както и да предприемат всички разумни мерки, за да гарантират своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

Предвид горното, и на основание чл. 58, ал. 3 от Регламент (ЕС) 2016/679, Комисията за защита на данните изрази следното

СТАНОВИЩЕ:

1. В изпълнение на нормативно установените си задължения, общините осъществяват справки чрез еднократен достъп от регистрите на ЕСГРАОН на основание чл. 106, ал. 1, т. 2 от Закона за гражданската регистрация във вр. чл. 6, пар. 1, б. „в" от Регламент (ЕС) 2016/679, от следните полета: справка за валидност на физическо лице, справка за постоянен адрес и справка за настоящ адрес от регистри Национална база данни „Население", единствено за лицата, чиито данни вече се съдържат в електронната система за прием на ученици в първи клас и в електронната система за прием на деца в общинските детски градини и ясли.

2. На посоченото основание общините нямат право на директен достъп до регистрите на ЕСГРАОН.

3. При съблюдаване на принципите, визирани в чл. 5, пар. 1, б. „б" и „г" от Регламент (ЕС) 2016/679, общините следва да обработват достъпените данни за целите на извършване на проверка за тяхната достоверност.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

.

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

Информационен бюлетин № 4 (85) 2020 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