

Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 2 (95), март 2022 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода януари и февруари 2022 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
КЗЛД отбеляза Деня за защита на личните данни	3
КЗЛД издаде две нови информационни брошури	4
Връчена е годишната “Награда за журналистика” на КЗЛД	16
Обявен е ежегодният студентски конкурс на КЗЛД	16
Заседания на Европейския комитет по защита на данните	17
Европейският комитет по защита на данните започна първото координирано правоприлагащо действие относно използването на облачните услуги от публичния сектор	19
Европейският надзорен орган по защита на данните нареди на Европол да изтрие данни за лица, които нямат установена връзка с престъпна дейност	20
Европейската комисия предлага декларация за цифровите права и принципи за всички в ЕС	21
КОНТРОЛНА ДЕЙНОСТ КЗЛД	23
РЕШЕНИЯ НА КЗЛД	24
СТАНОВИЩА НА КЗЛД	42

СЪБИТИЯ И ИНИЦИАТИВИ

КЗЛД ОТБЕЛЯЗА ДЕНЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ



На 28 януари 2022 г. КЗЛД отбеляза за 16-ти пореден път Деня за защита на личните данни. На тази дата през 1981 г. е приета Конвенция 108 на Съвета на Европа за защита на лицата при автоматизирана обработка на лични данни, която е първият правно обвързващ международен акт, приет в тази сфера. Възникнал като европейски, Денят за защита на данните вече се празнува в световен мащаб и извън Европа, където се нарича Ден на неприкосновеността (Privacy Day).

Информационните и комуникационни технологии през последните десетилетия създадоха нова реалност – дигитално общество и всеобхватна глобализация, в отговор на което през 2018 г. Конвенция 108 бе осъвременена с оглед на новите предизвикателства. Пандемията от Ковид-19 през последните две години доведе до революционен скок в налагането

на дигитални онлайн решения в редица аспекти на ежедневието – здравеопазване, образование, пазаруване, социални контакти, културен живот. Цифровите трансформации продължават да обхващат все по-голяма част от живота и носят безспорни предимства, но и редица предизвикателства, като едно от основните е защитата на информацията и в частност – защитата на личните данни на хората.

Една от основните задачи на съвременното общество е да се създадат условия за реализиране на технологичната революция при пълно зачитане на правата на хората. Необходимо е правилно разбиране за рисковете, гаранциите и правата, свързани с обработването и защитата на личните данни. Изграждането на надежден и сигурен цифров свят изисква ангажираност от всички и всеки трябва да оцени своето място в системата за защита на личните данни.

И тази година КЗЛД отбеляза Деня за защита на личните данни с **редица събития и постави начало на инициативи**, чиято основна цел е насърчаване на осведомеността и формиране на разбиране относно политиките за обработване на лични данни.

В сградата на КЗЛД бе организирана традиционната **приемна за администратори на лични данни и граждани**. В съответствие с извънредната епидемична обстановка тя се проведе при повишени мерки за защита относно допускането в сградата и начин на осъществяване на контакт със служители на КЗЛД.

По повод празника и изпълнявайки една от основните си задачи за повишаване осведомеността относно защитата на личните данни, КЗЛД издаде **2 броя информационни брошури**: „Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване” и „Големи бази данни (BIG DATA) и свързаната с тях възможност за профилиране” – с информационно-образователно съдържание и съвети към АЛД и граждани.

На 28 януари 2022 г. чрез сайта на КЗЛД бе обявен ежегодния конкурс за студентско есе, което тази година е на тема **„Трудности в практическото прилагане на защитата на личните данни в условията на пандемията”**.

Друго традиционно събитие по случай Деня за защита на личните данни бе **връчването на ежегодната годишна награда на КЗЛД за журналистика**. Председателят на КЗЛД Венцислав

Караджов връчи наградата на **Диян Божидаров, журналист във вестник „Сега“** за най-голям журналистически принос през 2021 година за популяризиране дейността на КЗЛД и правата на гражданите за неприкосновеност и защита на личните данни.

По случай Деня за защита на личните данни КЗЛД изпрати поздравителен мейл на всички Длъжностни лица по защита на данните и на всички абонати на Информационния бюлетин на Комисията, с който ги поздрави с празника и ги информира за горепосочените инициативи.

КЗЛД ИЗДАДЕ ДВЕ НОВИ ИНФОРМАЦИОННИ БРОШУРИ

Една от основните задачи на Комисията за защита на личните данни е да насърчава осведомеността и да формира на национално ниво ценностите на гражданите в областта на защитата на личните данни. Във връзка с това, както и по повод 28 януари - Деня за защита на личните данни, КЗЛД издаде **2 броя информационни брошури**: „Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване“ и „Големи бази данни (BIG DATA) и свързаната с тях възможност за профилиране“ – с информационно-образователно съдържание и съвети към АЛД и граждани.



„Големи бази данни (BIG DATA) и свързаната с тях възможност за профилиране“ е информационен материал, който има за цел да подпомогне практическото прилагане на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), да даде разяснения на някои ключови въпроси при обработването на „Големи информационни масиви“ („Големи бази данни“, Big Data) и свързаната с тях възможност за профилиране. Същият няма задължителен характер и не претендира за изчерпателност. Тъй като представлява информационно-образователно съдържание и съвети както към гражданите, така и към администраторите на лични данни, след преценка на целесъобразността от индивидуализиран подход към двете целеви групи, тази брошура е оформена в два варианта – „за граждани“ и „за администратори на лични данни“. В по-голямата ѝ част брошурата е еднаква и в двата варианта и съдържа общи

раздели – „Определение и видове“, „Източници на големи бази данни“, „Начини за обработка на големи бази данни“, „Ползи и рискове, свързани с големите информационни масиви“ и „Ключови аспекти за бъдещи действия“. Разликата между двата варианта на брошурата е, че в предназначения за граждани вариант има раздел „Права на физическите лица“, а в този за АЛД - „Задължения на администраторите на лични данни“

„Съвременни заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване“ има за цел да подпомогне практическото прилагане на изискванията за защита на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване. Основните му раздели са „Същност, определение и съдържание. Изкуствен интелект. Лицево разпознаване.“, „Ползи от развитието на изкуствения интелект и новите технологии за лицево разпознаване“, „Рискове от използването на изкуствения интелект и новите технологии за лицево разпознаване“, „Изисквания, на които трябва да отговорят приложенията с изкуствен интелект“, „Препоръки



по отношение използването на изкуствения интелект и новите технологии за лицево разпознаване“ и „Ключови аспекти за бъдещи действия“.

Брошурите са достъпни в електронен вид на сайта на КЗЛД – [ТУК](#).

Предстои издаването и разпространението им и на хартиен носител.

В настоящия бюлетин предоставяме текстовете на двете брошури.

Големи бази данни (Big Data) и свързаната с тях възможност за профилиране

Бързото технологично развитие, широкото използване на компютрите, интернет и цифровите технологии, глобализацията създават нови предизвикателства пред защитата на личните данни.

В ерата на цифровия свят, в който живеем днес, всяка дейност оставя цифрова следа, която може да бъде събрана, обработена и оценена или анализирана. С новите информационни и комуникационни технологии се събират, записват и анализират все повече данни.

Определение и видове

За първи път през 2001 г. Laney споменава трите V-та, които са в основата на определянето на „големите данни“: Volume (обем), Velocity (скоростта на нарастване) и Variety (многообразие).

„Големи информационни масиви“ („Големи бази данни“, Big Data) е модерен термин, който най-общо включва „нарастващата технологична способност за събиране, обработване и извличане на нова и прогнозна информация от голям обем, скорост и разнообразие от данни“.

Понятието „големи информационни масиви“ обхваща едновременно самите данни и анализа на данните. Според начина на представяне могат да се класифицират в три категории – структурирани, полуструктурирани и неструктурирани.

Източници на големи бази данни

Източниците на данните са най-различни по вид и включват:

- Хора и техни лични данни, електронни устройства, машини или датчици, информация за климата, спътникови изображения, цифрови снимки и видеоматериали или GPS сигнали;
- Данните, генерирани от хора чрез мобилни приложения, в интернет, през социалните мрежи или плащания, данни на публичната администрация;
- Интернет свързани устройства/интернет на предметите/интернет на вещите (Internet of Things, IoT);
- Метаданните;
- Данни от обществените сфери.

Начини за обработка на големи бази данни

Системите за работа с големи данни се използват за извличане и разкриване на неочевидни зависимости, скрити корелации между на пръв поглед неизвестни и несвързани една с друга величини или за обобщаването им по нови начини, които са разбираеми и полезни за потребителите. За тази цел се прилагат интелигентен анализ на данни и текст (Data Mining и Text Mining), различни аналитични техники и методи за мрежов анализ, анализ на мултимедии и социални медии и др.

За обработване на големите бази данни се използват:

- Паралелни и разпределени парадигми (напр. облачните технологии);
- Изкуствения интелект (AI);
- Други подходи и инструменти (например NoSQL бази данни).

Ползи и рискове, свързани с големите информационни масиви

При отговорно боравене големите масиви от данни може да донесат значителни ползи и ефективност за обществото и отделния човек. Сериозно безпокойство обаче предизвиква действителното и потенциалното въздействие на обработката на огромни количества данни върху правата и свободите на хората, включително неприкосновеността на личния им живот. Затова предизвикателствата и рисковете, свързани с големите масиви от данни, налагат по-ефективна защита на данните.

Ползи при обработването на големи бази данни:

- Обхващане на големи масиви от данни;
- Бързо импортиране на нови данни;
- Обработване в реално време на информацията при кратки срокове;
- Възможност за множество и едновременни искания;
- Анализиране на различни видове информация (снимки, текстове или номера);
- Осигуряване на нови средства за профилиране и целева реклама;
- Разкриване на закономерности между различните източници и масиви от данни;
- Анализът на информацията в реално време може да бъде използван за подобряване на въведените системи;
- Нарастване на броя на трансграничните потоци от данни;
- Значителни и видими ползи в ежедневието: интернет търсачките улесняват достъпа до значителни обеми информация и знания; услугите за социални мрежи дават възможност на хората в целия свят да общуват, да изразяват мнението си и да мобилизират подкрепа за различни каузи, възползване от ефективни и ефикасни маркетингови техники, които стимулират икономиката;
- Технологиите и обработването на лични данни представляват незаменими инструменти за държавните органи в борбата им срещу престъпността и тероризма.

Рискове при обработването на големи бази данни:

- Физическите лица все по-често оставят лична информация, която е публично достъпна и в световен мащаб;
- Неправомерна употреба на големите информационни масиви от лица с достъп до масивите от информация посредством манипулиране, дискриминация или потискане на отделни лица или на конкретни групи в обществото;
- По отношение на защитата на основните права като правото на неприкосновеност на личния живот и защитата и сигурността на данните;
- Във връзка със свободата на изразяване на мнение и недопускането на дискриминация;
- При обучаването на устройства с изкуствен интелект (AI), като невронни мрежи, и статистически модели с цел предвиждане на определени събития или поведение често данните за обучението са със съмнително качество и не са неутрални;

- Съвременните техники за обработка и анализ, вкл. без намесата на човека, предоставят безпрецедентен поглед върху човешкото поведение, личния живот и обществото;
- Чувствителна информация за лица може да се изведе и от нечувствителни данни;
- Технологичният напредък и възможностите за анализи на големи информационни масиви, изкуственият интелект (AI) и машинното самообучение улесниха създаването на профили и вземането на автоматизирани решения, които имат потенциал да окажат значително въздействие върху правата и свободите на физическите лица;
- Широко разпространената достъпност на лични данни в интернет и от интернет свързани устройства/интернет на предметите/интернет на вещите, както и възможността да се установяват корелации и да се създават връзки, могат да позволят определяне, анализ и предвиждане на личностни или поведенчески аспекти на даден човек и на неговите интереси и навици (профилиране);
- Информацията за поведението и нагласите днес се използва за определяне на личността на съответното лице. Комбинираната информация за „харесванията“ в социалните мрежи, данните от проследяването, слушаната музика или гледаните филми дава възможност да се изгради ясна картина на личността на дадено лице, позволявайки на предприятията да публикуват целеви реклами и/или информация в съответствие с „личността“ на това лице;
- Техниките и новият софтуер за обработване оценяват в реално време информацията за това какво харесва дадено лице, какво разглежда то, когато пазарува онлайн, или какво слага в кошницата с покупки онлайн и могат да предложат „продукти“, които може да представляват интерес въз основа на събраната информация (профилиране);
- Възможно е процесите на профилирането и автоматизираното вземане на решения да не са видими. Физическите лица може да не знаят, че са подложени на профилиране, или да не разбират какво включва това.

Псевдонимизацията, анонимизиране или криптиране на личните данни, са подходящи предпазни мерки за намаляване на рисковете за съответните субекти на данни, когато личните данни се използват в приложения за големи информационни масиви. Договорните задължения следва да гарантират, че анонимизираните данни няма да бъдат повторно идентифицирани чрез използване на допълнителни съотношения посредством комбиниране на различни източници на данни. Употребата на криптиране от край до край следва да се насърчава и когато е необходимо да се прави задължително, в съответствие с принципа на защита на данните при проектирането (чл. 25 от Регламент (ЕС) 2016/679).

Задължения на администраторите на лични данни

(текст във варианта на брошурата, предназначен за администратори на лични данни)

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

- Уведомят субектите на данни за съществуването на автоматизирано вземане на решения, включително профилиране (член 12), като уведомлението съдържа и съществена информация относно използваната логика при профилирането и предвидените последици от това обработване за лицата (член 13, параграф 2, буква е);
- Предприемат подходящи мерки, за да се гарантират правата, свободите и законните интереси на субектите на данни. Това включва най-малко правото на човешка намеса от страна на администратора и възможността субектът на данните да изрази гледната си точка и да оспори решение, което се основава на автоматизирано обработване на личните му данни (член 22, параграф 3);
- Изрично да предоставят подробности на вниманието на субекта на данни относно правото му на възражение (член 21, параграфи 1 и 2), както и да ги представят по ясен начин и отделно от всяка друга информация (член 21, параграф 4);

- Спазват принципа за свеждане на данните до минимум, както и изискванията за ограничение на целите и принципите за ограничение на съхранението (член 5);
- Личните данни в контекста на профилирането следва да бъдат обработвани добросъвестно, законосъобразно, пропорционално и за конкретни и легитимни цели (член 5);
- Предприемат мерки да коригират факторите, които водят до неточности в личните данни (член 5);
- Въведат надеждни мерки за постоянна проверка и гарантиране, че повторно използваните или получените по косвен път данни са точни и актуални;
- Демонстрират, че субектите на данни разбират с какво точно се съгласяват, и също така да помнят, че съгласието невинаги представлява подходящо основание за обработване;
- При наличие на легитимен интерес, трябва да се извърши балансиране, за да се оцени дали пред интересите на администратора преимущество имат интересите или основните права и свободи на субекта на данните;
- Ограничат рисковете или грешките, които профилирането може да предизвика;
- Периодично да оценяват качеството на използваните данни и алгоритми;
- Гарантират, че профилирането и автоматизираното вземане на индивидуални решения (независимо дали включва профилиране или не) не се използват по начини, които оказват необосновано въздействие върху правата на физическите лица;
- Ако от профилирането се извличат чувствителни предпочитания и характеристики, администраторът следва да гарантира, че: 1.обработването не е несъвместимо с първоначалната цел, 2.е определил законосъобразно основание за обработването на специалните категории данни, както и 3.е информирал субекта на данни относно обработването;
- Извършват анализ на риска и оценка на въздействието върху защитата на данните;
- Определят видовете потребители в информационните системи;
- Утвърдят правила за отделните потребители на информационните системи, функционалните им задължения и процедурите за тяхната дейност, в които достатъчно ясно да са разписани принципите на взаимодействие на отделните потребители;
- Утвърдят правила за обработка на личните данни за всяка една от поддържаните информационни системи;
- Утвърдят правила и процедури за защита на личните данни, в т. ч. информационната/киберсигурност;
- Утвърдят вътрешни правила за обучение и тренировка на служителите за действия в случай на незаконосъобразно обработване на лични данни;
- Поддържат системни дневници (логове) на действията на потребителите на информационните системи;
- Имат налична документация къде и как на етапа на проектиране на информационните системи е приложен чл. 25 от Регламент (ЕС) 2016/679 (защита на данните на етапа на проектиране и по подразбиране);
- Утвърдят политики и процедури за защита на личните данни, които гарантират спазването на Регламент (ЕС) 2016/679, при наемане на облачни услуги и тяхното управление по отношение на достъп / преносимост / възстановяване / унищожаване на данни в т. ч. извършване на анализ на риска при използването на външен доставчик.

Права на физическите лица

(текст във варианта на брошурата, предназначен за физическите лица)

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

- Да не бъдат обект на решение, което ги засяга в значителна степен и се основава единствено на автоматизирано обработване, без да се вземат предвид техните гледни точки (*Модернизирана Конвенция № 108, член 9, параграф 1, буква а*);
- Да предявяват иски срещу администратора, който е създал профила, и срещу администратора, който е взел автоматизирано решение относно субект на данни (със или без човешка намеса), ако тези две образувания са различни;
- Правото на достъп до личните данни, обработвани от администратора чрез автоматизирано вземане на решения, остава незасегнато (*Регламент (ЕС) 2016/679, член 15*);
- Да получат подробности относно лични данни, които се използват за профилиране, включително категориите данни, които се използват за създаване на профил;
- Да упражнят правата си на коригиране, изтриване и ограничаване на обработването. Администраторът на данни може да бъде освободен от задължението да съобщава на субекта на данните за всяко извършено коригиране или изтриване на неговите лични данни, когато такова уведомяване „е невъзможно или изисква несъразмерно големи усилия“ (*Регламент (ЕС) 2016/679, член 19*);
- Да оспорват решения, които се основават единствено на автоматизирано обработване. Те не могат да упражняват това право, ако автоматизираното решение е разрешено в закон, който е приложим спрямо администратора и в който се предвиждат и подходящи мерки за защита на правата, свободите и законните интереси на субектите на данни (*Регламент (ЕС) 2016/679, член 22*);
- Да бъдат уведомени за причините за извършването на обработване (*Модернизирана Конвенция № 108, член 9, параграф 1, буква в*));
- Да бъдат информирани от администратора и при определени обстоятелства да възразят срещу „профилирането“, независимо дали се извършва изцяло автоматизирано вземане на индивидуални решения, основано на профилиране;
- Да могат да оспорват евентуални неточности в използваните от администратора на лични данни и релевантността на прилагания към тях профил (*Обяснителен доклад към модернизираната Конвенция № 108, параграф 75*);
- Да възразят срещу обработването (включително при профилиране) на основания, свързани с неговата конкретна ситуация (*Регламент (ЕС) 2016/679, член 21*);
- Да възразят срещу обработване на техните лични данни за целите на директния маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг (*Регламент (ЕС) 2016/679, член 21*).

Ключови аспекти за бъдещи действия

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

Предизвикателствата пред големите данни включват тяхното регистриране, съхранение, анализ, търсене в тях, споделяне, трансфер, визуализация, правене на запитване/заявка в тях, обновяване,

сигурност и видове източници за работа с тях. Важно е да се определят ясни правила и процедури за работа с големи бази данни, съдържащи лични данни на физически лица, в целия процес по тяхното обработване. Обработката на големи данни изисква нов подход, базиран на изкуствения интелект (AI) и високоскоростни мрежи.

Като интегрират защитата на данните още в проектирането на системите и процесите си и я адаптират така, че да позволява по-истинска прозрачност и потребителски контрол, отговорните администратори на данните ще могат да се възползват и от предимствата на големите масиви от данни, като същевременно осигуряват зачитане на достойнството и свободите на хората.

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

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

1. Същност, определение и съдържание

Изкуствен интелект

Изкуственият интелект (ИИ) е набор от технологии, които съчетават данни, алгоритми и изчислителна мощ, и има потенциал да трансформира основни сектори на индустрията, услугите и обществото като цяло. Според възприетата дефиниция системите с изкуствен интелект са софтуерни (и евентуално хардуерни) системи, проектирани от хората, които, при зададена сложна цел, действат във физическото или цифровото измерение, възприемайки средата си чрез събиране на данни, интерпретиране на събраните структурирани или неструктурирани данни, разсъждавайки върху знанието или обработвайки информацията, извлечена от тези данни, в резултат на което вземат решения за най-добрите действия, които водят до постигане на поставената цел.

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

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

Лицево разпознаване

В духа на динамичното развитие на технологиите, важна роля оказват системите за разпознаване на лица или т.н. „лицево разпознаване”. Тъй като системите за лицево разпознаване включват измерване на физиологичните характеристики на човека, те се категоризират като „биометрични”.

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

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

2. Ползи от развитието на изкуствения интелект и новите технологии за лицево разпознаване

За съвременните програми изкуственият интелект е важен елемент на информационните технологии, използван за разрешаване на някои от най-трудните задачи в областта на информатиката. Изследванията в областта на изкуствения интелект са силно специализирани и обособени в няколко подобласти, които според някои критици в много случаи не успяват да взаимодействат ефективно. Общи за повечето подобласти на изследванията на ИИ са задачи като възможността за разсъждение, обучение и подобряване на ИИ чрез обучение, възприемане, планиране, общуване, а също и способността за движение, и управление на движението на обекти с ИИ като коли и други. Системите с изкуствен интелект са способни да адаптират поведението си до известна степен, като анализират резултатите от предишни действия, и работят автономно. Изкуственият интелект е интелектът, демонстриран от компютри, това е и науката за концепциите в компютърната наука, които правят възможно компютрите да извършват задачи, които могат да бъдат разглеждани като интелигентни.

Изкуственият интелект при поставяне на задача има способност да анализира обкръжаващата го среда и да предприема действия, които увеличават възможността за постигане на определени цели. Изучаването на възможностите за създаване на такива програми или устройства, наричани „интелигентни агенти“, е предмет на обособен дял от информатиката. Изкуственият интелект е един от основните двигатели на цифровата трансформация в Европа и значим фактор за осигуряване на конкурентоспособността на европейската икономика и високо качество на живот.

В основата на съвременните системи за видеонаблюдение се използват алгоритми и процеси на изкуствения интелект, които създават условия за автоматизирано вземане на решения с важни последици за субектите на данни. Такова е лицевото разпознаване. От създаването си системите за лицево разпознаване намират широко приложение в технологиите, една от които са системите за видеонаблюдение, които масово навлизат във всички сфери на живота и непрекъснато се използват поради тяхната достъпност и приложимост. Доскоро системите за видеонаблюдение са били приоритет за специални обекти, банкови офиси и големи предприятия, но днес те се използват за охрана на училища, жилищни комплекси, болници, хотели, офиси, магазини и др.

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

- **Развиващи изкуствен интелект** (такива са съвременните информационно-комуникационните технологии/софтуер, роботиката и научните изследвания);
- **Консуматори на изкуствен интелект** (това са всички проявления на съвременния начин на живот, като напр. производство, логистика, цифрови платформи, електронна търговия,

селско стопанство, публична администрация, здравеопазване, интелигентни градове, транспорт, финанси и др.);

▪ Създаващи условия за развитието и внедряването на изкуствен интелект (правна рамка и образование).



3. Рискове от използването на изкуствения интелект и новите технологии за лицево разпознаване

Развитието на изкуствения интелект и на новите технологии за лицево разпознаване ще доведат до цялостна промяна на парадигмата, до революционен обрат, който ще постави на преразглеждане основни обществени отношения, лични избори и човешки ценности.

Динамичното развитие на технологиите и все по-широкото използване на различни алгоритми за изкуствен интелект, лицево разпознаване и др., създават възможности за безпрецедентно по обем и дълбочина навлизане в личното пространство и личната неприкосновеност на физическите лица.

Използването на технологиите на изкуствен интелект крие редица потенциални рискове, като непрозрачност на процеса на вземане на решения, нарушаване на личното пространство и употреба на тези технологии за извършване на незаконосъобразни действия. ИИ може да доведе до предубеждения и по този начин до различни форми на дискриминация, основана на пол, раса, цвят на кожата, етнически или социален произход, генетични характеристики, език, религия или убеждения, политически или други мнения, принадлежност към национално малцинство, имотно състояние, рождение, увреждане, възраст или сексуална ориентация.

4. Изисквания, на които трябва да отговорят приложенията с изкуствен интелект

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

Човешки фактор и надзор

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

Техническа стабилност и безопасност

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

Управление на данните и неприкосновеност на личния живот

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

Обяснимост и прозрачност

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

Многообразие, недискриминация и справедливост

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

Обществено и екологично благополучие

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

Отчетност

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

5. Препоръки по отношение използването на изкуствения интелект и новите технологии за лицево разпознаване

Основните изводи и препоръки по отношение на съвременните заплахи и предизвикателства пред защитата на личните данни в контекста на тенденциите в развитието на изкуствения интелект и новите технологии за лицево разпознаване, биха могли да се обобщят в следното:

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

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

- Възможността, осигурявана от тези технологии, за използването на лични данни с цел категоризиране и насочване към определени лица, откриване на уязвимите страни на отделни лица или извличане на полза от точни предвидими знания, трябва да бъде неутрализирана чрез ефективно прилагане на принципите за защита на данните и неприкосновеността на личния живот, като

например свеждане на данните до минимум, правото на възражение във връзка с профилирането и контрола върху ползването на данните, правото на получаване на обяснение за решение, основаващо се на автоматизирана обработка, и защита на неприкосновеността на личния живот още на етапа на проектиране на дадена технология, както и чрез прилагане на принципите на пропорционалност, необходимост и ограничение въз основа на строго определени цели, в съответствие с Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

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

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

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

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

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

- ИИ не следва никога да замества хората, като решенията, които се основават единствено на автоматизирана обработка и произвеждат правно действие по отношение на физически лица или засягат тези лица в значителна степен, трябва винаги да включват съдържателно оценяване и преценка, извършена от човек.

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

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

6. Ключови аспекти за бъдещи действия

Повишаването на обществената осведоменост относно заплахите и възможностите, които виртуалното пространство създава пред субектите на данни и относно защитата на информационните им права в цифровата ера са от първостепенно значение за надзорните органи по защита на данните. За да се реализира тази амбиция в контекст, в който потоците от данни преминават безпроблемно през границите и дигиталният бизнес достига до клиентите в световен мащаб, следва разработващите системи с изкуствен интелект да станат все по-ефективни в предвиждането, тълкуването и влиянието на подобен напредък в начина на използване на данните, с което да се изгради доверие, подкрепено от високите стандарти за защита на данните.

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

- за налагане на мораториум върху масовото наблюдение чрез системи за изкуствен интелект;
- за недопускане на автоматизираното лицево разпознаване на обществени места или за целите на граничния контрол;
- за строги гаранции за физическите лица, когато инструментите на изкуствения интелект се използват в правоприлагането, особено в случаите с прогнозиране на извършители на престъпления;
- за определяне на хармонизирани правила относно изкуствения интелект и за насърчаване разглеждането на проблемите с използването на системи с ИИ, включително използването им от институциите, органите и агенциите на ЕС;
- за изграждане на регулаторна рамка, основаваща се на „етика по подразбиране” и „етика при проектирането”, която да гарантира, че всеки пуснат в действие ИИ изцяло зачита и спазва законодателството в областта на защитата на личните данни;
- за прилагане на подход, основан на риска, уеднаквен с правната рамка на ЕС в областта на защитата на личните данни, съобразно който се търси пресечната точка и баланса между развитието на технологиите и правата на човека (*необходимост и пропорционалност*);
- за оценка и намаляване на обществения риск за групите от физически лица;
- за обща забрана върху използването на ИИ за автоматично разпознаване на човешки черти на обществено достъпни места и на някои други употреби на ИИ, които могат да доведат

до несправедлива дискриминация, например разпознаване на лица, походка, пръстови отпечатащи, ДНК, глас, натискане на клавиши и други биометрични или поведенчески данни, в какъвто и да било контекст поради изключително високия риск, свързан с дистанционната биометрична идентификация на лица на обществено достъпни места;

- за забрана върху използването на биометрични данни в рамките на системи с ИИ за категоризиране на отделни лица в групи въз основа на етническа принадлежност, пол, политическа или сексуална ориентация или на други основания, при които има забрана на дискриминация;
- за забрана върху използването на ИИ за всякакъв вид социална оценка и за съставяне на изводи за емоциите на физически лица (освен в много специфични случаи, например по здравословни причини, когато разпознаването на емоциите е важно).

КЗЛД ВРЪЧИ СВОЯТА ГОДИШНА „НАГРАДА ЗА ЖУРНАЛИСТИКА“ НА ДИЯН БОЖИДАРОВ, КОРЕСПОНДЕНТ НА ВЕСТНИК „СЕГА“

Ежегодната „Награда за журналистика“ (грамота и медал на КЗЛД) е учредена на 28 януари 2016 г. и се дава за публикации, предавания и обществено значими прояви през предходната календарна година, с които активно, обективно и добронамерено са отразявани както дейността на КЗЛД, така и национални и наднационални събития, свързани със защита на правата на гражданите и тяхната неприкосновеност.

На 28 януари 2022 г., в Деня за защита на личните данни, председателят на КЗЛД Венцислав Караджов връчи за шеста поредна година учредената от КЗЛД „Награда за журналистика“. Комисията награди Диян Божидаков, журналист във вестник „Сега“ за най-голям журналистически принос през 2021 година за популяризиране дейността на КЗЛД и правата на гражданите за неприкосновеност и защита на личните данни. Институцията благодари на Диян Божидаков и на целия екип на вестник „Сега“ за поредицата журналистически материали, отразяващи обществено значими теми, свързани със защитата на личните данни.

Други медии също имат голям принос в отразяване на актуални теми по защитата на личните данни и на работата на българския надзорен орган по защита на данните, като някои от тях вече са притежатели на „Годишната награда за журналистика“ през предходните пет години.

ОБЯВЕН Е ЕЖЕГОДНИЯТ СТУДЕНТСКИ КОНКУРС НА КЗЛД

Организираният от КЗЛД ежегоден студентски конкурс за есе бе обявен по случай Деня за защита на личните данни – 28 януари. През 2022 година темата на конкурса е **„Трудности в практическото прилагане на защитата на личните данни в условията на пандемията“**.

Конкурсът за студентско есе е първата по рода си ежегодна инициатива, организирана от национален орган по защита на данните на територията на Европейския съюз. Целта му е приобщаване на младите хора към търсенето на решения на предизвикателствата пред защитата на личните данни в контекста на дигитализацията и глобализацията, обхващащи всички сфери на живота. Младите хора, в частност студентите, винаги са били една от най-адаптивните, отворени за новостите и напредничави групи на обществото. Есето пък е форма за излагане на лични разсъждения, изразяване на новаторски дух и творческа самобитност по актуален проблем.

Тази година КЗЛД кани студенти от всички специалности, в последните три години от обучението им във висше училище, да участват в конкурса. Класираните на първо, второ и трето място ще бъдат включени в програмата на КЗЛД за едномесечен платен стаж в Комисията.

Конкурсът ще се проведе в два етапа.

Първи етап: Електронно кандидатстване с есе – до 15 април 2022 г.

Изисквания към есето:

- Executive Summary in English (резюме) на английски език в рамките на половин машинописна страница, представящо основните идеи на кандидата.
- Да представя аргументирано мнението на автора по темата;
- Да се цитирани всички използвани източници (Не се допуска плагиатство!);
- Обем на есето от 5 до 10 страници по БДС – 30 реда с 60 знака на ред, шрифт Times New Roman с големина на буквите 12 и разредка 1,5, като използваните фигури и графики не се включват в него;

Да бъде изпратено на електронна поща halaminov@cpdp.bg в срок до 15 април 2022 г., 24.00 ч.

Втори етап: Презентация пред конкурсната комисия (съгласно действащите към конкретната дата противоепидемични мерки) – **15 май 2022 г.**

До този етап на конкурса ще бъдат допуснати 10-те най-добри есета. Допуснатите до втори етап студенти ще трябва да представят изложение в рамките на 10 минути чрез предварително подготвена презентация (до 6 слайда) и изложение (до 2 страници).

С оглед гарантирането на равнопоставеност между участниците в конкурса за есе, консултации, предварителни оценки и информация относно приложимостта на предложените теми и текстове няма да се предоставяни

Победителите ще бъдат наградени на официална церемония на 28 май 2022 г. в зала „Заседателна“ на КЗЛД, бул. „Проф. Цветан Лазаров“ 2.

КЗЛД приканва всички, които отговарят на изискванията за участие и мислят, че има какво да ни кажат, да участват в нашия конкурс!

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ



European Data Protection Board

През януари и февруари 2022 г. се състояха три заседания на Европейския комитет по защита на данните (ЕКЗД).

На своето януарско заседание ЕКЗД прие „**Насоки 01/2022 относно правата на субектите на данни - Право на достъп**“. Насоките са предмет на обществена консултация до 11 март 2022 г. Целта им е да се анализират

различните аспекти на правото на достъп и да се предоставят по-точни инструкции относно начина, по който правото на достъп трябва да се прилага в различни ситуации. В документа са предоставени разяснения относно обхвата на правото на достъп, информацията, която администраторът трябва да представи на субекта на данните, формата на искането за достъп, основния начин за предоставяне на достъп и понятието за явно неоснователни, прекомерни искания. През ноември 2019 г. по тази тема беше проведено събитие за заинтересованите страни, като техните мнения и становища бяха взети

предвид при изготвянето на насоките. Според Андреа Йелинек, председател на ЕКЗД *„Правото на достъп дава възможност на физическите лица да се запознаят с начина и причините, поради които се обработват техните лични данни. В насоките са предоставени примери, които да помогнат на администраторите да отговарят на исканията за достъп по начин, който е в съответствие с ОРЗД.“*

На същото заседание ЕКЗД прие писмо в отговор на исканията за последователно тълкуване на **съгласието за приемане на бисквитки**. В писмото ЕКЗД отново заявява, че е поел ангажимент да гарантира хармонизираното прилагане на правилата за защита на данните в целия Европейски съюз. В тази връзка ЕКЗД наскоро създаде **Работна група относно банерите, с които се иска съгласие за приемане на бисквитки**, която да координира отговорите на жалби относно тези банери. Освен това ЕКЗД актуализира **Насоките относно съгласието**, за да гарантира хармонизиран подход по отношение на условията за съгласие и недвусмисленото волеизявление.

На състоялото се в началото на февруари заседание ЕКЗД прие становището си относно схемата за сертифициране GDPR-CARPA, внесена от люксембургския надзорен орган. Това е първият случай, в който ЕКЗД приема становище по механизма за съгласуване относно критериите за национална схема за сертифициране. Схемата за сертифициране GDPR-CARPA е обща схема, която не е насочена към конкретен сектор или вид обработване. Тя включва изисквания относно управлението на защитата на данните в организация във връзка с дейностите по обработване. Целта на становището на ЕКЗД е да се гарантират последователността и правилното прилагане на критериите за сертифициране сред надзорните органи в Европейското икономическо пространство. За тази цел Комитетът счита, че трябва да бъдат направени редица промени в проекта на критерии за сертифициране. След одобрение от надзорния орган механизмът за сертифициране ще бъде добавен и в регистъра на механизмите за сертифициране и печатите за защита на данните в съответствие с член 42, параграф 8 от ОРЗД. В прессъобщение във връзка с приетото становище председателят на ЕКЗД Андреа Йелинек заявява: *„Това становище е важна стъпка към подобряване на спазването на ОРЗД. Основната цел на механизмите за сертифициране е да се помогне на администраторите и на обработващите лични данни да спазват Регламента. Администраторите и обработващите лични данни, които се придържат към механизъм за сертифициране, се възползват от повече видимост и надеждност, тъй като той позволява на физическите лица бързо да оценяват нивото на защита на операциите по обработване.“*

На състоялото се на 22 февруари 2022 г. заседание ЕКЗД прие окончателния вариант на Насоки относно кодексите за поведение като инструмент за международни трансфери, писмо относно отговорността на изкуствения интелект и отговор до Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE) относно втория допълнителен протокол към Конвенцията за борба с киберпрестъпността.

На състоялото се на 22 февруари 2022 г. заседание ЕКЗД прие окончателния вариант на Насоки относно кодексите за поведение като инструмент за международни трансфери, писмо относно отговорността на изкуствения интелект и отговор до Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE) относно втория допълнителен протокол към Конвенцията за борба с киберпрестъпността.

ЕКЗД прие окончателния вариант на **Насоките относно кодексите за поведение като инструмент за трансфер**, като взе предвид получените от заинтересованите страни отзиви. Основната цел на насоките е да се изясни прилагането на член 40, параграф 3 и член 46, параграф 2, буква д) от ОРЗД. В тези разпоредби се посочва, че след като бъде одобрен от компетентен надзорен орган и след като получи от Европейската комисия обща валидност в рамките на Европейското икономическо пространство (ЕИП), даден кодекс може да бъде спазван и използван и от администратори и обработващи лични данни в трета държава, за да се осигурят подходящи гаранции при предаването на данни извън ЕИП.

Прието бе **писмо относно отговорността на изкуствения интелект (ИИ)**, в което се приветства инициативата на Европейската комисия за адаптиране на правилата за отговорността към цифровата ера и изкуствения интелект (ИИ) в светлината на оценката на Директивата за отговорността

за вреди, причинени на продукти (Product Liability Directive). ЕКЗД счита, че е уместно да се засили режимът на отговорност на доставчиците на системи за изкуствен интелект, така че обработващите лични данни и администраторите да могат да се доверят на тези системи. Освен това системите с изкуствен интелект следва да могат да бъдат обяснени при проектиране, а доставчиците им трябва да въграждат сигурността при проектиране през целия им жизнен цикъл.

Комитетът прие **писмо в отговор на Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE) на Европейския парламент относно Втория допълнителен протокол към Конвенцията за престъпления в кибер пространството**, с оглед на двете предложения на Европейската комисия за решения на Съвета за упълномощаване на държавите членки да подпишат и ратифицират протокола. В писмото се припомня, че нивото на защита на личните данни, предавани на трети държави в резултат на протокола, трябва да бъде по същество равностойно на нивото на защита в ЕС. ЕКЗД се позовава също така на становището на Европейския надзорен орган по защита на данните относно предложенията на Комисията и подчертава някои от неговите ключови точки. Приветстват се гаранциите, включени в протокола, като например разпоредбите за надзор. Изразява се съжаление, че протоколът не гарантира, че като общо правило информацията за лицата, до която е поискан достъп, се предоставя безплатно. ЕКЗД препоръчва държавите-членки да си запазят правото да не прилагат разпоредбата за пряко сътрудничество, която дава възможност на органите на трети държави да изискват пряко от доставчиците на услуги от ЕС да разкриват определени видове данни. Това би помогнало да се осигури по-съществено участие на съдебните или други независими органи на ЕС в разглеждането на такива искания.

ЕВРОПЕЙСКИЯТ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ ЗАПОЧНА ПЪРВОТО КООРДИНИРАНО ПРАВОПРИЛАГАЩО ДЕЙСТВИЕ ОТНОСНО ИЗПОЛЗВАНЕТО НА ОБЛАЧНИТЕ УСЛУГИ ОТ ПУБЛИЧНИЯ СЕКТОР

На 15 февруари 2022 г. започна първото координирано правоприлагащо действие на Европейския комитет по защита на данните (ЕКЗД). През следващите месеци, 22 национални надзорни органа в ЕИП, включително Европейският надзорен орган по защита на данните, ще започнат разследвания относно използването на облачни услуги от публичния сектор.

Тази поредица от действия следва решението на Комитета за създаване на Координирана рамка за прилагане (Coordinated Enforcement Framework - CEF), която, заедно със създаването на Група за подкрепа от експерти (Support Pool of Experts - SPE), е ключово действие в рамките на стратегията на ЕКЗД за 2021-2023 г. Двете инициативи имат за цел да рационализират прилагането и сътрудничеството между надзорните органи.

В своето прессъобщение по този повод ЕКЗД отбелязва, че според EuroStat усвояването на облачните услуги от предприятията се е удвоило в целия ЕС през последните 6 години.

Пандемията от COVID-19 е предизвикала ръст на дигиталната трансформация на организациите, като много организации от публичния сектор са се обърнали към облачните технологии. Това от своя страна е възможно предизвикателство при получаването на облачни продукти и услуги, които отговарят на правилата на ЕС за защита на данните. Надзорните органи имат за цел чрез координирани насоки и действия да насърчават най-добрите практики и по този начин да осигуряват адекватна защита на личните данни.

Ще бъдат включени общо над 80 публични органа в ЕИП, включително институции на ЕС, обхващащи широк спектър от сектори (като здравеопазване, финанси, данъци, образование, централни купувачи или доставчици на ИТ услуги). Въз основа на обща подготвителна работа от всички участващи надзорни органи, координираната рамка ще се прилага на национално ниво по един или

няколко от следните начини: проучване за установяване на факти; въпросник за установяване дали е оправдано официално разследване; започване на официално разследване; проследяване на текущите официални разследвания. Надзорните органи ще проучат предизвикателствата пред публичните органи по отношение спазването на Общия регламент относно защитата на данните при използване на базирани в облак услуги, включително процеса и предпазните мерки, прилагани при придобиване на облачни услуги, предизвикателствата, свързани с международните трансфери и разпоредбите, регулиращи отношенията администратор-обработващ.

Резултатите ще бъдат координирано анализирани и надзорните органи ще вземат решение за възможни по-нататъшни национални надзорни и правоприлагащи действия. Освен това резултатите ще бъдат обобщени, генерирайки по-задълбочен поглед върху темата и позволявайки целенасочени последващи действия на ниво ЕС.

Преди края на 2022 г. Европейският комитет по защита на данните ще публикува доклад за резултатите от този анализ.

ЕВРОПЕЙСКИЯТ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ НАРЕДИ НА ЕВРОПОЛ ДА ИЗТРИЕ ДАННИ ЗА ЛИЦА, КОИТО НЯМАТ УСТАНОВЕНА ВРЪЗКА С ПРЕСТЪПНА ДЕЙНОСТ



На 3 януари 2022 г. Европейският надзорен орган по защита на данните (ЕНОЗД) уведоми Европол за свое нареждане за изтриване на данни на лица без установена връзка с престъпна дейност (категоризация на субектите на данни).

С това решение приключва започналото през 2019 г. по негова инициатива разследване на ЕНОЗД относно обработването на големи масиви от данни от Европол за целите на стратегическия и оперативния анализ. Развитието на дейностите на Европол по обработване на лични данни на големи масиви от данни породи опасения, свързани със спазването на правилата за защита на данните на Европол,

определени в Регламента за Европол, по-специално с принципите на ограничаване на целите, свеждане на данните до минимум, точност на данните, ограничаване на съхранението, въздействие на потенциални нарушения на сигурността на данните, място на съхранение, общо управление и информационна сигурност.

През септември 2020 г. ЕНОЗД отправи забележка на Европол за продължаващото съхранение на големи обеми данни без категоризация на субектите на данните, което представлява риск за основните права на физическите лица. Въпреки че оттогава Европол е въвел някои мерки, той не е изпълнил исканията на ЕНОЗД да определи подходящ период на съхранение на данните, с цел филтриране и извличане на личните данни, разрешени за анализ съгласно Регламента за Европол. Това означава, че Европол е съхранявал тези данни по-дълго от необходимото, в противоречие с принципите за свеждане до минимум на данните и ограничаване на съхранението, залегнали в Регламента за Европол.

Правилата за защита на данните, приложими към Агенцията на ЕС за сътрудничество в областта на правоприлагането (Европол), както и надзорните правомощия на Европейския надзорен орган по защита на данните, са определени в Регламент (ЕС) 2016/794 (**Регламент за Европол**). Правомощията на ЕНОЗД по отношение на Европол са определени в член 43 от Регламент (ЕС) 2016/794.

С оглед на гореизложеното ЕНОЗД реши да използва своите корективни правомощия и да наложи 6-месечен период на съхранение (за филтриране и извличане на личните данни). Наборите от данни, по-стари от 6 месеца, които не са преминали през тази категоризация на субекта на данни, трябва да бъдат изтрити. Това означава, че Европол вече няма да има право да запазва данни за хора, които не са свързани с престъпление или престъпна дейност, за дълги периоди от време без определен срок. ЕНОЗД предостави 12-месечен срок на Европол да се съобрази с решението относно наборите от данни, които вече са получени преди Европол да бъде уведомен за това решение.

В прессъобщение от 10 януари 2022 г. Войчех Виевиоровски, ЕНОЗД, заявява: „Европол се е справил с няколко от рисковете за защитата на данните, установени в първоначалното разследване на ЕНОЗД. Въпреки това не е постигнат значителен напредък в преодоляването на основното притеснение, че Европол непрекъснато съхранява лични данни за физически лица, когато не е установил, че обработката е в съответствие с ограниченията, определени в Регламента за Европол. Такова събиране и обработване на данни може да представлява огромен обем информация, чието точно съдържание често не е известно на Европол до момента, в който тя бъде анализирана и извлечена - процес, който често продължава с години. Шестмесечен период за предварителен анализ и филтриране на големи масиви от данни следва да позволи на Европол да отговори на оперативните изисквания на държавите-членки на ЕС, които разчитат на Европол за техническа и аналитична подкрепа, като същевременно сведе до минимум рисковете за правата и свободите на физическите лица. Освен това, разбирайки оперативните нужди на Европол и обема на събраните до момента данни, реших да предоставя на Европол срок от 12 месеца, за да се гарантира спазването на решението за наборите от данни, с които Европол вече разполага.“

ЕНОЗД е убеден, че нареждането ще гарантира спазването от страна на Европол на задълженията му по Регламента за Европол, като същевременно ще се запазят оперативните му възможности.

За повече информация може да се запознаете с [решението на ЕНОЗД](#) и документа „Често задавани въпроси“, публикувани на уебсайта на ЕНОЗД.

ЕВРОПЕЙСКАТА КОМИСИЯ ПРЕДЛАГА ДЕКЛАРАЦИЯ ЗА ЦИФРОВИТЕ ПРАВА И ПРИНЦИПИ ЗА ВСИЧКИ В ЕС



На 26 януари 2022 г. Европейската комисия предложи на Европейския парламент и на Съвета да подпишат **Декларация за правата и принципите, които ще направляват цифровата трансформация в ЕС.**

Проектът на декларация цели да предостави на всички ясна отправна точка за вида цифрова трансформация, която Европа насърчава и защитава. Европейският парламент и Съветът се приканват да обсъдят проекта и да го одобрят на най-високо равнище до лятото на 2022 г. След съвместното ѝ одобряване, декларацията ще определи и подхода

към цифровата трансформация, който ЕС ще насърчава в целия свят.

По думите на комисаря по въпросите на вътрешния пазар Тиери Бретон европейците трябва да знаят, че „който живее, учи, работи или развива бизнес в Европа, може да разчита на свързаност от най-висока класа, безпрепятствен достъп до обществени услуги и безопасно цифрово пространство при справедливи условия. Декларацията за цифровите права и принципи също така определя веднъж

завинаги, че онова, което е незаконно офлайн, следва да бъде незаконно и онлайн. Ние също така се стремим да популяризираме тези принципи като стандарт за света.“

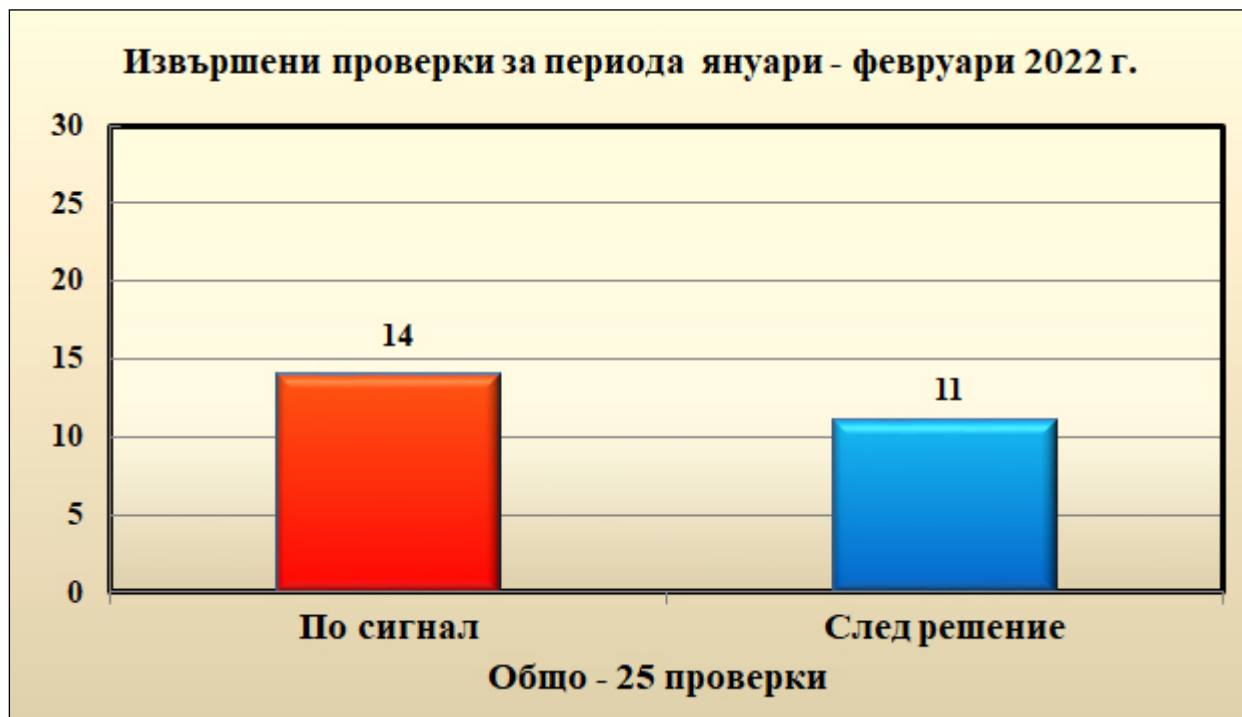
В прессъобщение на Европейската комисия се заявява: „Проектът за декларация обхваща ключови права и принципи за цифровата трансформация, като поставяне на хората и техните права в центъра ѝ, подкрепа за солидарността и приобщаването, гарантиране на свободата на избор онлайн, насърчаване на участието в цифровото публично пространство, повишаване на безопасността, сигурността и овластяването на индивида и насърчаване на устойчивостта на цифровото бъдеще. Тези права и принципи следва да са част от ежедневието на хората в ЕС: достъпна и високоскоростна цифрова свързаност навсякъде и за всички, добре оборудвани класни стаи и учители с цифрови умения, безпрепятствен достъп до обществени услуги, безопасна цифрова среда за децата, ..., контрол върху начина, по който се използват личните данни и с кого се споделят.“

Насърчаването и прилагането на принципите, залегнали в декларацията, ще бъде споделян политически ангажимент и отговорност както на равнището на Съюза, така и на равнището на държавите членки в рамките на съответните им области на компетентност.

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА ЯНУАРИ - ФЕВРУАРИ 2022 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците януари и февруари 2022 г. са извършени общо 25 проверки – 14 след постъпили в КЗЛД сигнали и 11 след решение на КЗЛД.



Разгледани са 69 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

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

РЕШЕНИЯ ПО ЖАЛБИ

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

РЕШЕНИЕ № ППН-02-343/2020 г. София, 12.01.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: Цанко Цолов, Мария Матева и Веселин Целков на заседание, проведено на 17.11.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента, ОРЗД), разгледа по същество жалба № ППН-02-343/21.08.2020 г.

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

Комисията за защита на личните данни е сезирана с жалба подадена от Я.Б. с изложени твърдения за неправомерно обработване на лични данни, в хипотезата на осъществявано видеонаблюдение от брат му Р.Б. в съсобствен имот – къща находящ се на адрес гр. С., ползван от двете лица.

Твърди, че видеонаблюдението се осъществява без негово знание и съгласие и в нарушение на личната му неприкосновеност. Моли за проверка по случая, като конкретизира, че видеонаблюдението се осъществява от пет камери за видеонаблюдение монтирани „покрай“ къщата и „в общите части на стълбището“. В допълнение, в телефонен разговор, обективиран в протокол ППН-02-343#1/21.10.2020 г., сочи, че къщата е на три етажа, от които той изцяло ползва третия етаж, вторият етаж се ползва от брат му, а първия етаж е за общо ползване.

Към жалбата не са приложени доказателства.

Съгласно принципите на равенство на страните в производството и истинност, Р.Б. е уведомен за подадената жалба, като му е указана възможността да представи писмено становище и относими по случая доказателства.

С оглед изясняване на случая от фактическа страна е извършена проверка по предмета на жалбата, резултатите от която са обективирани в констативен акт ППН-02-333/29.06.2021 г., с приложения към него Констативен протокол от 10.06.2021 г., графични изображения на местоположението на камерите и попълнен въпросник.

Проверката е открита на 10.06.2021 г. на посочения в жалбата адрес, с връчване на заповедта за проверка на Л.Б., син на Р.Б.

От извършената проверка е установено следното:

На посочения в жалбата адрес се намира поземлен имот, в който е изградена масивна четириетажна жилищна сграда – къща с един вход и прилежащо дворно място. Пред къщата, в рамките

на имота, са изградени допълнителни постройки (гаражи), като жалбоподателят е собственик на два от тях, а Р.Б. е собственик на третия, върху който е изградена веранда с покривна конструкция (тип беседка). Жалбоподателят Я.Б. и неговият брат Р.Б. са съсобственици на по 1/2 (една втора) идеални части от имота, по един апартамент към първия етаж и половината помещения от таванския (четвърти) етаж в сградата. Вторият етаж е собственост на Р.Б., като той се ползва от сина му Л.Б. и неговото семейство, а третият етаж е собственост на жалбоподателя Я.Б. Къщата разполага с приземен етаж, който също е разделен между собствениците, като в своята част Р.Б. е изградил гараж, достъпът до който се осъществява през отделен вход към имота.

Констатирано е, че на проверявания обект е изградена система за видеонаблюдение, състояща се от пет броя HIKVISION DS-2CD1331-I 3MP, 1/3" progressive scan CMOS, Up to 3.0 megapixel, 2.8 mm/4 mm/6 mm fixed focal lens, Up to 30 m IR range, Mobile monitoring via Hik-Connect or iVMS-4500 видеокамери, разполагащи с възможност за звукозапис, които към момента на проверката не са свързани към електрическата мрежа и не функционират. В хода на проверката не е установено видеокамерите да са свързани към записващо устройство. На Л.Б. е предоставен за попълване „Въпросник за извършване на проверки с предмет видеонаблюдение“, който е попълнен собственоръчно и е предаден на проверяващия екип. От наличната в него информация става ясно, че на адреса през лятото на 2019 г., с цел охрана на имота, от Л.Б. е изградена система за видеонаблюдение, която от влизането ѝ в експлоатация е функционирала за около един, два месеца, след което записващото устройство е премахнато и е свързано към система за видеонаблюдение, изградена в друг негов имот отново с охранителна цел, а камерите на проверявания обект са изключени от захранващата мрежа. Л.Б. твърди, че до системата за видеонаблюдение е осъществявал отдалечен достъп единствено и само той, посредством софтуерно приложение, инсталирано на мобилния му телефон. Установено е, че на проверявания обект се извършва охрана по реда на Закона за частната охранителна дейност от „В.С.“ ЕООД, като дружеството няма достъп до видеокамерите и не осъществява видеонаблюдение с охранителна цел на имота.

Камерите са разположени и са насочени, както следва:

- Камера № 1 е монтирана на предната фасада, под козирката на допълнителната постройка (гараж) ползван от Р.Б. и е насочена към подстъпа на допълнителната постройка, подстъпа към входа на ползвания от него вътрешен гараж в къщата, както и част от улица и прилежащите ѝ тротоари;

- Камера № 2 е разположена на предната фасада, под козирката на допълнителната постройка (гараж) ползван от Р.Б. от срещуположната страна на Камера № 1 и е насочена към подстъпа на допълнителната постройка, подстъпът към допълнителните постройки, в които се помещават двата гаража на жалбоподателя и към общия вход на имота, както и част от улица и прилежащите ѝ тротоари;

- Камера № 3 е монтирана на страничната фасада на допълнителната постройка (гараж) ползван от Р.Б. и е насочена към вътрешния му гараж и подстъпа към него;

- Камера № 4 е разположена до вътрешния гараж на Р.Б. и е насочена към обособения вход в имота водещ към него и малка част от улица;

- Камера № 5 е монтирана на втория етаж в къщата, над входната врата на жилището ползвано от Л.Б. и е насочена към вътрешното стълбище на къщата.

Така изградената система за видеонаблюдение, въпреки че към момента на проверката не функционира, би могла във всеки един момент да бъде въведена отново в експлоатация, позволявайки идентификация на физически лица, но без възможност за тяхното лицево разпознаване (посредством ползване на база с биометрични данни).

Категориите физически лица, чиито лични данни биха могли да се обработват посредством изградената система за видеонаблюдение са: живущи и посетители в имота, както и случайно преминаващи по улицата и прилежащите ѝ тротоари физически лица.

Проверяващият екип установи, че няма поставени информационни стикери/табели, предупреждаващи за осъществяване на видеонаблюдение.

В хода на производството, след проверката осъществена от екип на комисията, Р.Б. информира, че след проверката е сключил договор с охранителна фирма „С.1“ за охрана на имота и предоставя копие на Приложение № 2/22.06.2021 г. подписано от „С.“ ЕООД, като изпълнител, и „Б.“ ООД – възложител, представляван от Л.Б., за охрана на имот находящ се в гр. С.

Предвид предоставената информации и приложени доказателства, от Р.Б. е изискано да конкретизира функционират ли камерите за видеонаблюдение след извършената на 10.06.2021 г. проверка от екип на КЗЛД, има ли промяна в обхвата и местоположението им и да уточни кой има достъп до изображение/записи от камерите за видеонаблюдение и как се осъществява достъпа. Изискано е и заверено копие на сключения договор за охрана, доколкото в КЗЛД е изпратено само копие на Приложение № 2/22.06.2021 г. към него.

В отговор и с писмо ППН-02-343#6/16.09.2021 г. Р.Б. информира, че след проверката на комисията камерите функционират, няма промяна в местоположението и обхвата им, а „достъп до камерите има само охранителната фирма чрез видеомониторинг“. Прилага копие на договор № 279478/21.12.2015 г., едно с Приложение № 1 към него и декларация, както и Приложение № 2/22.06.2021 г.

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

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

Жалбата съдържа задължително изискуемите реквизити, а именно: налице са данни за жалбоподателя, естеството на искането, дата и подпис, посочено е лицето срещу което е подадена, с оглед което е редовна.

Жалбата има за предмет неправомерно обработване на личните данни на жалбоподателя, в хипотезата на осъществявано видеонаблюдение в съсобствен имот находящ се в гр. С.

Жалбата е депозирана в срока по чл. 38 от ЗЗЛД, доколкото не е спорно, че видеонаблюдение е осъществявано преди сезирана на КЗЛД, а се осъществява и след 22.06.2021 г. Макар проверката на КЗЛД да е констатира, че към 10.06.2021 г. видеонаблюдение не се осъществява, пасивно легитимираната страна признава, че е осъществявано видеонаблюдение на адреса преди сезиране на КЗЛД, в рамките на месец, два след монтиране на камерите през лятото на 2019 г., както и че след дата на осъществена от КЗЛД проверка същото е възобновено.

Жалбата е подадена е от физическо лице с правен интерес срещу физическо лице за което се твърди, че е администратор на лични данни по смисъл чл. 4, ал. 7 Регламент ЕС 2016/679. В хода на проверката обаче е установено, че достъп до видеонаблюдението осъществявано 2019 г. е имал Л.Б. - синът на пасивно легитимираната страна, обстоятелства отразени в констативния акт от проверката и попълнения от Л.Б. въпросник, с оглед на което същият следва да участва в производството като ответна, служебно конституирана страна.

По преписката са представени доказателства за осъществявано на адреса видеонаблюдение от 22.06.2021 г., въз основа на договор Приложение № 2/22.06.2021 г. за охрана на имот находящ се в гр. С., със страни „С.“ ЕООД - изпълнител, и „Б.“ ООД – възложител, представляван от Л.Б. Предметът на договора е „сигнално-охранителна дейност 24 ч. по защита на имущество, чрез наблюдение и техническо поддържане на СИОС в обекта и реакция с МОП“. Предвид последното и с оглед служебното начало, като ответни страни в производството служебно следва да се конституират „С.“

ЕООД и „Б.“ ООД. Липсват доказателства соченото от пасивно легитимираната страна дружество с наименование „С.1“ да има отношение към договора за охрана, като следва да се приеме че по-скоро се касае за грешка при посочване на наименованието на дружеството, предвид обстоятелството, че в приложения договор дружеството, страна по договора, е „С.“ ЕООД.

Сезиран е компетентен да се произнесе орган – КЗЛД, която съгласно правомощията си по чл. 10, ал. 1 от ЗЗЛД във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679, разглежда жалби срещу актове и действия на администраторите на лични данни, с които се нарушават правата на субекти на данни свързани с обработване на личните данни, като не са налице изключенията по чл. 2, § 2, буква „в“ и чл. 55, § 3 от регламента предвид обстоятелството, че случая не касае дейности по обработване извършвани от физическо лице в хода на чисто лични или домашни занимания и/или дейности извършвани от съдилищата при изпълнение на съдебните им функции.

По горните съображение и предвид липсата на отрицателните предпоставки по чл. 27, ал. 2 от АПК, на проведено на 29.09.2021 г. заседание на комисията жалбата е приета за допустима и като страни в производство са конституирани: жалбоподател – Я.Б. и ответни страни – Р.Б. – пасивно легитимиран и Л.Б., „Б.“ ООД и „С.“ ЕООД – служебно конституирани.

Насрочено е открито заседание за разглеждане на жалбата по същество на 17.11.2021 г. от 13:00 часа, за което страните са редовно уведомени. Информирани са за извършена служебна проверка относно видеонаблюдението, обективизирана в констативен акт с № ППН-02-333/29.06.2021 г., заверено копие от който, ведно с приложения към него е предоставен на страните за запознаване.

От „С.“ ЕООД са изискани конкретна информация и доказателства кой има достъп до камерите за видеонаблюдение, как се осъществява достъпа, както и графични изображения от камерите за видеонаблюдение и информация осъществява ли се запис на кадрите от видеонаблюдение, в какъв срок се съхранява и кой има достъп до него, поставени ли са, кога и от кого информационни табели на обекта за осъществяваното видеонаблюдение.

От жалбоподателя, Р.Б. и Л.Б. са изискани заверено копие на нотариален акт за собственост в имота (със заличени лични данни на лица различни от участващите в производството), респективно за делба на дворното място, и скица на имота.

В отговор и с придружително писмо ППН-02-343#13/02.11.2021 г. Р.Б. представя копие на издадена от АГКК, служба по геодезия, картография и кадастър скица № *** за поземлен имот с идентификатор *** с адрес гр. С., нотариален акт за констатиране право на собственост № ***, нотариален акт върху недвижим имот придобит по обстоятелствена проверка № ***. и нотариален акт за дарение на недвижим имот № ***.

В хода на производството е депозирано писмено становище ППН-02-343#14/02.11.2021 г. от Л.Б., с приложения към него относими доказателства, а именно копие на – нотариален акт за дарение на недвижим имот № ***; нотариален акт за дарение на недвижим имот № *** и приложение № 2 от 22.06.2021 година към договор за охрана № *** между „С.1“ ЕООД и „Б.“ ЕООД.

Л.Б. оспорва жалбата, като неоснователна. Информира, че камерите са поставени през лятото на 2019 година с цел охрана на имота от посетители в него и случайно преминаващи. Сочи, че в жилищната сграда притежава гараж, в който съхранява нови автомобилни гуми. Твърди, че камери са поставени с цел охрана и са работели без записващо устройство само около 3 /три/ месеца, като към дата на осъществената от КЗЛД проверка не са функционирали. Твърди, че от 22.06.2021 година с камерите оперира „С.“ ЕООД, с което „Б.“ ЕООД има сключен договор от 21.12.2015 година и заявява, че той и семейството му нямат достъп до тях.

Писмено становище по жалбата е изразено и от „С.“ ЕООД, заведено с рег. № ППН-02-343#14/02.11.2021 г. с приложения към него относими доказателства – графични изображения на изходящ образ от камери 1, 2, 3 и 4 за видеонаблюдение, същите от 11.11.2021 г. Изходящ образ от камери 5 не е предоставен. Информират, че „С.“ ЕООД осъществява охрана със сигнално охранителни

системи за денонощно наблюдение и реакция с въоръжени мобилни екипи на гараж, находящ се на адрес: ***, по договор №*** от 21.12.2015г. с възложител „Б. ООД, сключен с един от управителите на дружеството г-н Л.Б. Допълват, че на 22.06.2021 г. предоставяната по договора услуга е променена, като е добавено видеонаблюдение на обекта посредством 5 броя видеокамери, волеизявление обективизирано в ново Приложение № 1 към договора. Твърдят, че камерите са собственост на възложителя и не са монтирани и позиционирани от „С.“ ЕООД и уточняват, че дружеството е предоставило само радиопредавател за връзка с дежурен център.

Твърдят, че достъп до видеокамерите има възложителят по договора за охрана „Б.“ ООД, чрез представляващите дружеството, като неговите управители решават на кого да предоставят достъп. Уточняват, че в случая, те са предоставили на „С.“ ЕООД статичен IP адрес на записващото устройство (DVR), необходим за осигуряване на отдалечен достъп на Националния дежурен център на „С.“ / НОДЦ до записите в устройството, при установени от алармената система нарушения в охранявания обект. Твърдят, че „С.“ ЕООД използва отдалечения достъп за преглед на камерите автоматизирано и за много кратко време, само след получен алармен сигнал, посредством софтуерно решение в мониторинговата система на НОДЦ. Отдалечен достъп може да се извършва и ръчно, само когато се изясняват обстоятелства и действия на нарушители или на мобилните екипи на дружеството след взлом и инциденти в обектите, каквито досега не е имало в този обект.

Твърдят, че записите от камерите се съхраняват в DVR устройството и се изтриват автоматично. Няма информация за колко време могат да се съхраняват, тъй като дружеството не поддържа системата и нямаме информация за обема на паметта на записващото устройство. Допълват, че дружеството не е поставяло информационни табла за осъществяваното наблюдение на обекта, тъй като „С.“ ЕООД не е монтирало камерите и не администрира системите за видеонаблюдение, като на възложителя са предоставени само стикери, обозначаващи охраната на гаража. Сочат, че дружеството е търговско дружество с основен предмет на дейност охрана на имуществото на физически и юридически лица, за което притежава лиценз съгласно Закона за частната охранителна дейност /ЗЧОД/, където изрично е указано, че охраната може да се извършва и с помощта на технически средства. В тази връзка считат, че извършването на охранителни услуги е законосъобразно, със спазени изисквания на ЗЧОД и при наличие на условията за допустимост на обработването на лични данни, доколкото обработването е необходимо, за да се защити животът и здравето на физическите лица, обект на видеонаблюдението и по искане на самия възложител, и е необходимо за изпълнение на договора за защитата и гарантирането на сигурността и имуществото му. Считат, че обработването на лични данни е необходимо за реализиране на законните интереси на администратора на лични данни, който в случая е търговско дружество. Намират твърденията на жалбоподателя за неоснователни, вероятно дължащи се на личен конфликт.

На проведено на 17.11.2021 г. открито заседание на КЗЛД, жалбата е разгледана по същество.

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

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в административното производство, съгласно чл. 7 от Административно-процесуалния кодекс, изискващ наличието на установени действителни факти, имайки предвид събраните доказателства и наведените от страните твърдения, комисията приема, че разгледана по същество жалба № ППН-02-343/21.08.2020 г. е частично основателна.

От събраните по преписката доказателства се установи, а и между страните в производството не е спорно, че на адрес в гр. С. се намира поземлен имот, в който е изградена масивна четириетажна жилищна сграда – къща с един вход и прилежащо дворно място. Пред къщата, в рамките на имота, са изградени допълнителни постройки (гаражи), като не е спорно, че жалбоподателят е собственик на два от тях, а Р.Б. е собственик на третия, върху който е изградена веранда с покривна конструкция (тип беседка). Не е спорно, че жалбоподателят Я.Б. и неговия брат Р.Б. са съсобственици на по ½ (една втора) идеални части от имота, на по един апартамент към първия етаж и половината помещения

от таванския (четвърти) етаж в сградата. Вторият етаж е собственост на Р.Б., но се ползва от сина му Л.Б. и неговото семейство. Не е спорно, че третият етаж е собственост на жалбоподателя Я.Б. Къщата разполага с приземен етаж, за който не е спорно че е разделен между собствениците, като в своята част Р.Б. е изградил гараж, достъпът до който се осъществява през отделен вход към имота.

По преписката са приложени копие на нотариални актове за собственост, видно от които втори етаж, с площ 109, 55 кв. м., от жилищната сграда – къщата с идентификатор *** и самостоятелен обект с площ 66, 74 кв. м., втори етаж от сграда с идентификатор ***, находящи се в поземления имот, са дарени на Л.Б. от родителите му Р.Б. и В.Б. Дарен на Л.Б. от родителите му е и самостоятелен обект – „гараж в сграда“ с идентификатор *** и застроена площ с площ 41, 76 кв. м.

Материалите по преписката свидетелстват, че масивната четириетажна жилищна сграда – къща е в режим на етажна собственост, доколкото в обекта има повече от три самостоятелни обекта, собственост на различни лица – Я.Б., Р.Б. и Л.Б., предвид което приложими са нормите на Закона за управление на етажната собственост. При справка в ТРРЮЛНЦ е констатирано, че на адреса е регистрирано и търговско дружество „Б.“ ООД с управители Л.Б. и Р.Б., като няма данни дружеството да притежава собственост на адреса.

Не е спорно, че на адреса, гр. С., е изградена система за видеонаблюдение, състояща се от пет броя HIKVISION DS-2CD1331-I 3MP, 1/3” progressive scan CMOS, Up to 3.0 megapixel, 2.8 mm/4 mm/6 mm fixed focal lens, Up to 30 m IR range, Mobile monitoring via Hik-Connect or iVMS-4500 видеокамери, разполагащи с възможност за звукозапис. Констатирано е, че в обхвата на камерите попадат както общи части – стълбищна площадка на ет. 2 и стълбище от жилищната сграда (камера № 5), така и обществени места - част от улица и прилежащите ѝ тротоари (камери 1, 2 и 4). Констатирано е, че в обхват на видеонаблюдение (камера 3) попадат и входа към гаража на Р.Б.

Доказателствата по преписката и изявленията на страните, обективирани в попълнен въпросник приложен към констативен акт от проверка на КЗЛД, свидетелстват, че достъп до личните данни събирани посредством системата за видеонаблюдение в периода от монтирането ѝ през 2019 г. до 10.06.2021 г. е имал Л.Б., предвид което същият има качеството на администратор на лични данни по смисъла на чл. 4, ал. 7 от ОРЗД. Липсват доказателства останалите ответници, пасивно легитимирани страни в производството, да имат отношение към наблюдението осъществявано до 10.06.2021 г., респективно да имат достъп до събраните чрез него лични данни, предвид което по отношение на тях – Р.Б., „Б.“ ООД и „С.“ ЕООД, жалбата следва да бъде оставена без уважение като неоснователна касателно видеонаблюдението осъществявано до 10.06.2021 г.

Съгласно Приложение № 2 към договор за охрана, същото от дата 22.06.2021 г., сключено между „Б.“ ООД и „С.“ ЕООД на последното дружество, регистрирано по ЗЧОД, е възложено осъществяване на охрана със сигнално охранителни системи за денонощно наблюдение на гараж, находящ се на адрес: гр. С., посредством пет камери. Предвид съдържанието на договора от 22.06.2021 г. като администратор на лични данни по отношение на осъществяването, въз основа на договора, видеонаблюдение следва да се квалифицира възложителя „Б.“ ООД, доколкото именно последния определя целите и средствата за обработване на лични данни посредством изградената на адреса система за видеонаблюдение. „С.“ ЕООД следва да бъде третирано като обработващ лични данни, доколкото обработва – достъпва лични данни събрани чрез системата за видеонаблюдение, от името на администратора срещу възнаграждение и в изпълнение на договора за охрана, като камерите са собственост на възложителя и не са монтирани и позиционирани от „С.“ ЕООД. Обстоятелството, че възложителя „Б.“ ООД няма достъп до кадрите не променя това обстоятелство и качеството му на администратор на лични данни, доколкото именно „Б.“ ООД е предоставило на „С.“ ЕООД статичен IP адрес на записващото устройство (DVR), необходим за осигуряване на отдалечен достъп на Националния дежурен център на „С.“ /НОДЦ до записите в устройството, при установени от алармената система нарушения в охранявания обект. Двете дружества, възложител и изпълнител, не следва да се третират като съвместни администратори доколкото целите и средствата за обработване се определят от възложителя „Б.“ ООД, а не съвместно.

Предвид целта на осъществявано видеонаблюдение, а именно охрана на собствеността на администратора, местоположението и обхвата на камера 5 се налага извода за видеонаблюдение осъществявано в нарушение на принципите на по чл. 5, § 1, буква „а“ и „в“ от ОРЗД, на законосъобразност и свеждане на данните до минимум, доколкото в обхвата на видеонаблюдение попадат общи части от ЕС.

Доказателства за взето решение от Общо събрание на етажната собственост за осъществяване на видеонаблюдението не са ангажирани, наличието на такова не се и твърди, предвид което следва да се приеме, че решение липсва. Видеонаблюдението е незаконосъобразно, доколкото не е налице и нито едно от останалите условия посочени чл. 6, § 1 от Регламента, като доказателства в обратен смисъл не са ангажирани. Липсват доказателствата които да обосноват приложимостта на чл. 6, § 1, буква „б“ от ОРЗД - наличие на сключен между страните договор за изпълнението на който да е необходимо обработване на лични данни посредством процесната камера или за предприемане на стъпки по искане на субекта на данни преди сключване на договора. Основания по чл. 6, § 1, буква „г“ и „д“ от ОРЗД са неотнормирани - приложими са в други, различни и несъвместими с настоящата хипотези касаещи обработване на лични данни за защита на жизненоважни интереси, изпълнение на задача от обществен интерес, както и при упражняването на официални правомощия, каквито не се делегирани на администраторите на лични данни. Не може да се приеме, че е налице и преимуществен интерес на Л.Б. и „Б.“ ООД за видеонаблюдение осъществявано извън рамките на собствеността на г-н Б., като доказателства в обратна насока липсват, поради което следва да се приеме, че преимущество намира интересът на физическите лица, за които се отнасят данните, пред този на лицето, поставило съответната камера, още повече че не се сочат наличието на причини - посегателства, извършени престъпление или конфликти или други които да обосноват осъществяването на видеонаблюдение на обща част в етажната собственост. Аргументите, че същото се използва за охрана на имота – апартамент на Л.Б. над входната врата на който е поставена камерата, са несъстоятелни доколкото в обхвата на наблюдение не попада същия.

Предвид целта на осъществявано видеонаблюдение от камери 1, 2 и 4 и неговия обхват, същото е незаконосъобразно, а и в нарушение на принципа на свеждане на данните до минимум – чл. 5, § 1, буква „а“ и „в“ от ОРЗД. Противно на видеонаблюдението осъществявано рамките на собствения имот (камера 3), не може да се приеме, че видеонаблюдението на обществени места представлява легитимен интерес на администратора предвид липсата на преимуществен интерес на последния пред интереса на физическите лица обект на наблюдението – неограничен и неопределен брой лица свободно преминаващи по улицата. В обхвата на видеонаблюдение на камери 1, 2 и 4 обаче попадат освен подстъпа към гаража на ответника и обществени места, прилежаща улица и тротоари видеонаблюдението на които е незаконосъобразно, а и в нарушение на принципа на свеждане на данните до минимум предвид целта на осъществявано видеонаблюдение и обстоятелството, че видеонаблюдението не е ограничено до необходимото във връзка с целите за неговото осъществяване – охрана на гаража, съгласно предмета на сключения между страните договор, като твърденията, че в гаража се съхраняват скъпи вещи не променя това обстоятелство.

Предвид характерът и видът на констатираното нарушение и обстоятелството, че същото е преустановено от Л.Б. и след 22.06.2021 г. същия не осъществява видеонаблюдение, а също и че засегнатите лични данни не са чувствителни по смисъла на закона и няма данни за настъпили вреди от обработването, комисията счита за целесъобразно, пропорционално и ефективно налагането на корективна мярка по чл. 58, § 2, буква „б“ от Регламент ЕС 2016/679 на администратора Л.Б., като намира, че същата ще постигне целта на закона. Останалите мерки за по чл. 58, § 1, буква „а“, „в“, „д“, „г“, „е“, „ж“, „з“ и „й“ от ОРЗД са неприложими и нецелесъобразни поради естеството на нарушението и обстоятелството, че към момента на произнасяне същото е преустановено от Л.Б. и същия няма достъп до видеонаблюдението, а след 22.06.2021 г. няма и качеството на администратор на лични данни. Доколкото нарушението е първо за администратора налагането на глоба за констатираното нарушение би била прекомерна и в нарушение на принципа на съразмерност по чл. 6 от АПК съгласно

който „когато с административния акт се засягат права или се създават задължения за граждани, се прилагат онези мерки, които са по-благоприятни за тях, ако и по този начин се постигне целта на закона.“

По отношение на констатираното нарушение на „Б.“ ООД обстоятелството, че същото не е преустановено, а също и че засегнатите лични данни не са чувствителни по смисъла на закона и няма данни за настъпили вреди от обработването, комисията счита за целесъобразно, пропорционално и ефективно налагането на корективна мярка по чл. 58, § 2, буква „г“ от Регламент ЕС 2016/679 на администратора, като намирам, че същата ще постигне целта на закона - ще преустанови нарушението и ще възстанови установения правов ред по отношение на обработването на личните данни. Останалите мерки за по чл. 58, § 1, буква „а“, „б“, „в“, „д“, „е“, „ж“, „з“ и „й“ от ОРЗД са неприложими и нецелесъобразни поради естеството на нарушението и обстоятелството, че към момента на произнасяне същото не е преустановено. Доколкото нарушението е първо за администратора налагането на глоба за констатираното нарушение би била прекомерна и в нарушение на принципа на съразмерност по чл. 6 от АПК съгласно който „когато с административния акт се засягат права или се създават задължения за граждани, се прилагат онези мерки, които са по-благоприятни за тях, ако и по този начин се постигне целта на закона.“ Следва обаче да се отбележи, че неизпълнението на даденото от комисията разпореждане, в указания срок, е скрепено със санкция за неизпълнение с оглед неговата ефективност и възможността за допълнителен санкционен механизъм по проверка и контрол на изпълнението. Целта е постигане на генерална превенция и пропорционално и законосъобразно обработване на лични данни. Така разпореждания са ефективни, тъй като са скрепени със съответните санкции при неизпълнение, като законодателя предвижда при неспазване на влязло в сила разпореждане на надзорния орган да бъде наложено административно наказание „глоба“ или „имуществена санкция“ по чл. 83, параграф 6 от Регламент 2016/679 в размери до 20 000 000 EUR.

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

РЕШИ:

1. Приема жалба ППН-02-343/21.08.2020 г. за основателна по отношение на Л.Б. относно осъществявано видеонаблюдение на адрес гр. С. от лятото на 2019 г. до 10.06.2021 г. от камери 1, 2, 4 и 5.

2. На основание чл. 58, § 2, буква „б“ от ОРЗД отправи официално предупреждение до Л.Б. за обработване на лични данни посредством видеонаблюдение осъществявано на адрес гр. С. от лятото на 2019 г. до 10.06.2021 г. от камери 1, 2, 4 и 5 в нарушение на чл. 5, § 1, буква „а“ и „в“ от ОРЗД.

3. Приеме жалбата за основателна по отношение на „Б.“ ООД, администратор на лични данни, относно осъществявано от 22.06.2021 г. видеонаблюдение на адрес гр. С. от камери 1, 2, 4 и 5 в нарушение на чл. 5, § 1, буква „а“ и „в“ от ОРЗД.

4. За нарушение на чл. 5, § 1, буква „а“ и „в“ от Регламент ЕС 2016/679 и на основание чл. 58, § 2, буква „г“ от Регламента разпорежда на администратора на лични данни „Б.“ ООД да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като преустанови наблюдението на общи части от сграда в режим на етажна собственост и обществени места – прилежаща улица, като демонтира камера № 5, а камери 1, 2 и 4 препозиционира или пренасочи, така че в обхватът им да попада охранявани имот - гараж, без да обхваща обществени места. Срок за изпълнение на разпореждането – 14-дневен от влизането на решението в сила, след което да уведоми комисията за изпълнението като представи съответните доказателства.

5. Приеме жалбата за неоснователна по отношение на видеонаблюдението осъществявано посредством камера № 3.

6. Приема жалбата за неоснователна по отношение на Р.Б. и „С.“ ЕООД.

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

ЧЛЕНОВЕ:**Цанко Цолов /п/****Мария Матева /п/****Веселин Целков /п/****РЕШЕНИЕ****№ ППН-01-778/2020 г.****София, 12.01.2022 г.**

Комисията за защита на личните данни (КЗЛД) в състав: Председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на заседание, проведено на 03.11.2021 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента, ОРЗД), разгледа по същество жалба № ППН-01-778/04.11.2020 г.

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

Комисията за защита на личните данни е сезирана с жалба подадена от М.Ч., Т.Ч. и Ст.С., чрез адв. М.А. с изложени в същата твърдения за неправомерно обработване на лични данни, в хипотезата на осъществявано видеонаблюдение от С.П.С., Ж.С., П.С. и Л.С., с които са в „силно влошени отношения“.

Твърди се, че жалбоподателите М.Ч. и Т.Ч. са съсобственици на недвижим имот – жилищна сграда и прилежащо към нея дворно място находяща се в гр. ***, с идентификатор ***, който обитават заедно със жалбоподателят Ст.С., син на Т.Ч. Посочено е, че дворното място е облагородено и се ползва ежедневно по предназначение от жалбоподателите за отдиш и отглеждане на плодове и зеленчуци. Твърди се, че в съседство на имота живеят С.П.С., Ж.С. и техните синове П.С. и Л.С., същите монтирали през април 2020 г. камера за видеонаблюдение, в обхвата на видеонаблюдение на която попада дворното място на жалбоподателите, входа на сградата която обитават и прозорци на фасадата, обстоятелство обективизирано в приложен към жалбата Констативен протокол от 29.07.2020 г. по чл. 593 от ГПК с рег. № ***.

Към жалбата са приложени относими доказателства – копие на нотариален акт за дарение № ***; нотариален акт за недвижим имот, придобит по регулация № ***, нотариален акт за собственост на недвижим имот придобит по регулация № ***; нотариален акт за собственост на недвижим имот № ***, удостоверение за наследници № ***, удостоверение за наследници № ***, Скица на ПИ № *** и пълномощно.

Съгласно принципите на равенство на страните в производството и истинност, С.П.С., Ж.С., П.С. и Л.С. са уведомени за подадената жалба, като им е указана възможността да представят писмено становище и относими по случая доказателства.

В отговор е изразено становище от Ж.С., П.С. и Л.С., чрез адвокат, които възразяват, че не следва да бъдат конституирани като страна в производството доколкото не са собственици на имота, в който е монтирана камерата и не са монтирали същата. Информират, че камерата е монтирана от С.П.С., съпруг на Ж.С. и баща на П.С. и Л.С., същия собственик на апартамента на който е монтирана камерата и ползвател на дворното място, в обхвата на което попада видеонаблюдението. Сочат, че целта на осъществяваното видеонаблюдение е охрана на собствеността на С.П.С. - паркиран „под камерата микробус, който винаги е пълен със стока, както и на гараж, разположен в югозападния ъгъл на парцела“. Оспорват твърденията, че в обхвата на видеонаблюдение попадат имота на жалбоподателите – входа на жилищната сграда, прозорци по фасадата и двора“ и сочат, че макар камерата да е насочена по посока на имота на жалбоподателите „в действителност самия имот не попада в рамките на обхвата на видеозаснемане“.

Информират за издадена Заповед № **** на зам. кмета на община Б. за учредено на жалбоподателите Т.Ч. и М.Ч. право на преминаване за срок от 12 месеца, от влизане в сила на заповедна, през общински поземлен имот № ****, в който е построена кооперацията, в която собственост притежава С.П.С. и където е монтирана камерата, във връзка с издадено разрешение за строеж на масивна ограда по имотна граница между ПИ № *** и № ****. Допълват, че заповедта е обжалвана от С.П.С., но е оставена в сила, а производството прекратено, като г-н С.П.С. е уведомен от общинската администрация, че следва да осигури достъп до имота от към ул. Т. А.“ и „е предупреден да не паркира микробуса си през времето от 08:00 до 18:00 часа в тази част на имота, с оглед осигуряване на достъп на работници и на строителна техника в имота“. Допълват, че „именно поради предстоящо строителство, изискващо разграждане на двора откъм ул. „Т.А.“/премахване на входната врата откъм тази улица, премахване на оградата между двата имота, влизане на камиони и тежка строителна техника, безпрепятствено влизане на непознати строителни работници/“ С.П.С. е поръчал, закупил и монтирал камера за видеонаблюдение „с цел защита на имуществото си, находящо се в гараж № 6 и стоката в микробуса, който паркира в тази част на имота, както и евентуални повреди по фасадата на сградата“.

Към становището са приложени относими доказателства, а именно копие на Определение *** на Административен съд – Б., Заповед № **** на кмета на община Б., писмо изх. № **** на заместник-кмета на икономика и финанси на община Б., нотариален акт № ****, разрешение за строеж № ****, удостоверение за наследници № ****. и пълномощно.

С оглед изясняване на случая от фактическа страна е извършена проверка по предмета на жалбата, резултатите от която са обективирани в Констативен акт ППН-02-332/29.06.2021 г., с приложения към него в това число Констативен протокол от 09.06.2021 г., графични изображения на местоположението и обхвата на камерите и попълнен въпросник от С.П.С.

Проверката е открита на 09.06.2021 г. на посочения в жалбата адрес, с връчване на заповедта за проверка на С.П.С., в присъствието на сина му П.С. и В.П. – адвокат, които съдействат и осигуряват възможност за достъп и събиране на доказателства от страна на проверяващия екип.

От извършената проверка е установено следното:

На посочения в жалбата адрес се намира жилищна сграда – етажна собственост и прилежащо дворно място, в което са изградени и допълнителни постройки, използвани от живущите за гаражи. Сградата е триетажна с по два апартамента на етаж, като жилището, собственост на С.П.С., в което живеят той, съпругата му Ж.С. и синът му П.С. заедно със семейството му, се намира на първия етаж. Имотът на жалбоподателите се намира в съседство, като двата имота са разделени от ограда – телена мрежа. Между жилищната сграда, в която живеят С. и имота на жалбоподателите, в прилежащото към жилищната сграда дворно място, се намира алея, използвана от живущите в жилищната сграда за достъп до гаражите им. Тази алея се намира точно под прозорците на жилището на С. често е използвана от С.П.С. за паркиране на личния му микробус.

На адреса е констатирано наличието на един брой видеокамера IP Automat, модел V380-522, 2MPix – Full Hd 1080p, Обектив 3.6мм., инсталирана през месец май 2020 г. от приятел на П.С., с цел охрана на жилището и микробуса. Камерата е монтирана на фасадата на остъклена тераса на жилището на С. и има възможност за 360° панорамна гледка, като може да се върти на 320° хоризонтално и 90° вертикално. Към момента на проверката е установено, че хоризонталното въртене не функционира и камерата може да се върти само на 90° вертикално. С.П.С. твърди, че от самото инсталиране на камерата, функцията за хоризонтално въртене не била активна. Видеокамерата има възможност за запис на видеокадри на ONVIF TF – карта памет, каквато към момента на проверката липсва и по твърдения на С. – никога не е била поставяна, а винаги се е осъществявало видеонаблюдение само в реално време и не са осъществявани записи на видеокадри. Камерата разполага с възможност за запис и предаване на звук. Достъпът до изходящия образ в реално време се осъществява единствено от П.С. – отдалечено посредством софтуерно приложение, инсталирано на мобилния му телефон. Няма взето решение на общо събрание на етажната собственост за изграждане на система за видеонаблюдение в жилищната сграда, но С. твърдят, че никой от живущите в жилищната сграда нямат против инсталираната видеокамера, като посочват, че в сградата има поставени още видеокамери, констатирани от проверяващия екип при външния оглед, които са собственост на други живущи. С.П.С. заявява, че смята своевременно да свика общо събрание на етажната собственост, с оглед взимане на легитимно решение, съгласно чл. 11 от Закона за управление на етажната собственост.

Проверяващият екип установява, че когато е насочена в крайната си позиция надолу по вертикала, видеокамерата заснема прозорците на остъклената тераса на С. и алеята в имота, използвана за достъп на автомобили до гаражите, където понякога С.П.С. паркира микробуса си. Когато камерата е в крайната си позиция нагоре по вертикала, тя заснема отново прозорците на терасата и алеята, но обхваща и входа на имота за автомобили, малка част от оградата, разделяща имота от този на жалбоподателите, както и много малка част от имота на жалбоподателите, в т. ч. част от къщата им и подстъпа към вход ѝ.

Категориите физически лица, чиито лични данни се обработват посредством изградената система за видеонаблюдение са: посетители и живущи в жилищната сградата – етажна собственост, като в крайна позиция нагоре по вертикала на видеокамерата, в обхвата ѝ може да попаднат и живущите и посетителите в имота на жалбоподателите, но поради ниското качество на картината, тяхното идентифициране би било силно затруднено.

Установено е, че така изградената система за видеонаблюдение позволява идентификация на физически лица, но няма възможност за тяхното лицево разпознаване (посредством ползване на база с биометрични данни). На проверяващия екип не са предоставени доказателства за предприети технически и организационни мерки за защита на данните. Не са представени документи (правила, процедури, инструкции или други), регламентиращи обработването на лични данни чрез изградената система за видеонаблюдение. Системата за видеонаблюдение не осъществява предаване и запис на моментни снимки и видеокадри от образа на отдалечено устройство – FTP/Cloud сървър или на друго място за съхранение на данни.

Проверяващият екип констатира, че има поставени информационен стикери, предупреждаващ за осъществяването на видеонаблюдение, поставен на входната врата на жилищната сграда – етажна собственост, който не съдържа информация относно администратора на лични данни, както и данни за контакт с него.

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

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

Жалба ППН-01-778/04.11.2020 г. съдържа задължително изискуемите реквизити, а именно: налице са данни за жалбоподателите, естеството на искането, дата и подписи, приложено е пълномощно за представителна власт, посочени са лицата срещу които е подадена, с оглед което същата е редовна. Жалбата има за предмет неправомерно обработване на личните данни на жалбоподателите от С.П.С., Ж.С., П.С. и Л.С. в хипотезата на осъществявано видеонаблюдение посредством камера монтирана на адрес ***, в обхвата на която се твърди, че попадат имота на жалбоподателите, които е в съседство - дворното място, входа на сградата която обитават и прозорци на фасадата на сградата.

Жалбата е подадена в срока по чл. 38 от ЗЗЛД от физически лица с правен интерес срещу пасивно легитимира страни - физически лица, за които се твърди, че са администратори на лични данни по смисъл чл. 4, ал. 7 Регламент ЕС 2016/679, доколкото се твърди, че сами определят целите и средствата за обработване на лични данни чрез видеонаблюдение. Сезиран е компетентен да се произнесе орган – КЗЛД, която съгласно правомощията си по чл. 10, ал. 1 от ЗЗЛД във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679, разглежда жалби срещу актове и действия на администраторите на лични данни, с които се нарушават правата на субекти на данни свързани с обработване на личните данни, като не са налице изключенията по чл. 2, § 2, буква „в“ и чл. 55, § 3 от Регламент (ЕС) 2016/679 предвид обстоятелството, че случая не касае дейности по обработване извършвани от физическо лице в хода на чисто лични или домашни занимания и/или дейности извършвани от съдилищата при изпълнение на съдебните им функции.

По изложените съображения и предвид липсата на отрицателните предпоставки на чл. 27, ал. 2 от АПК, на проведено на 08.09.2021 г. заседание на комисията жалбата е приета за допустима и като страни в производство са конституирани: жалбоподатели – М.Ч., Т.Ч. и Ст.С. и ответни, пасивно легитимирани страни – С.П.С., Ж.С., П.С. и Л.С. Насрочено е открито заседание за разглеждане на жалбата по същество на 03.11.2021 г., за което страните са редовно уведомени. Информирани са за осъществена по предмета на жалбата проверка, констативен акт от която, ведно с приложения, им е предоставен за запознаване.

На проведено на 03.11.2021 г. открито заседание на КЗЛД, жалбата е разгледана по същество.

Жалбоподателите М.Ч., Т.Ч. и Ст.С. се представляват от адв. М.А. с пълномощно по преписката.

Ответните страни С.П.С., Ж.С., П.С. и Л.С. – редовно уведомени, не се явяват и не се представляват в заседанието пред комисията.

Адвокат М.А. поддържа жалбата, декларира, че се е запознала със събраните по преписката материали. Информира, че между страните в административното производство е висящо и гражданско дело ***, което е образувано по искове на ищците, жалбоподатели в настоящето производство, - обективно и субективно, срещу ответниците с правно основание чл. 45 от ЗЗД. Допълва, че по делото е приобщена съдебно-техническа експертиза, която подробно пояснява какви са характеристиките на монтираната камера, като в съдебно заседание вещото лице е заявило, че в обхвата на тази камера попада входната врата на доверителите ѝ, както и част от дворното място. Допълва, че от събрани в хода на гражданското дело гласни доказателства се установяват по безспорен начин, че камерата функционира от 2020 г., а микробусът се паркира на мястото едва в началото на 2021 г. във връзка с получен препис от исковата молба по гражданското дело и организираната защита от страна на ответниците срещу предявените срещу тях обективно и субективно съединени искове. Твърди, че в хода на гражданското дело са събрани гласни доказателства, че до края на 2020 г. камерата се е движела не само вертикално във вида, който представители на КЗЛД са констатирани при проверката, но се е движела във всички посоки съобразно нейните технически параметри и по начина, който е описан в констативния акт на нотариус К.М. За доказване на последното моли Комисията да допусне събирането на гласни доказателства.

Комисията оставя без уважение искането за събиране на гласни доказателства относно насочеността и обхвата на процесната камера, предвид наличието на безспорни писмени доказателства

в тази насока, а именно Констативен протокол от 29.07.2020 г. по чл. 593 от ГПК с рег. № *** по описа на нотариус К.М.

По същество адв. М.А. поддържа становище за основателност на жалбата и моли КЗЛД да издадете разпореждане за преустановяване на заснемането на входа на сградата на доверителите ѝ, както и на дворното им място.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в административното производство, съгласно чл. 7 от Административно-процесуалния кодекс, изискващ наличието на установени действителни факти, имайки предвид събраните доказателства и наведените от страните твърдения, комисията с мнозинство от три гласа приема, че разгледана по същество жалба № ППН-01-778/04.11.2020 г. е частично основателна. Несъгласен с аргументите за основателност на жалбата, господин Веселин Целков гласува с особено мнение, като намира жалбата за неоснователна.

Жалбата има за предмет неправомерно обработване на личните данни на жалбоподателите от С.П.С., Ж.С., П.С. и Л.С. в хипотезата на осъществявано видеонаблюдение посредством камера монтирана на адрес в гр. Б., в обхвата на която се твърди, че попадат имота на жалбоподателите, които е в съседство - дворното място, входа на сградата която обитават и прозорци на фасадата на сградата.

От събраните по преписката доказателства се установи, а и между страните в производството не е спорно, че страните са съседи. Ответниците обитават жилище на първия етаж в сградата в режим на етажна собственост, находящо се в гр. Б., а жалбоподателите имот - намиращ се в съседство, като двата имота са разделени от ограда – телена мрежа. Между жилищната сграда, в която живеят С. и имота на жалбоподателите, в прилежащото към жилищната сграда дворно място, се намира алея, използвана от живущите в жилищната сграда за достъп до гаражите им. Алеята се намира точно под прозорците на жилището на С. и по данни на ответниците често е използвана от С.П.С. за паркиране на личния му микробус.

Страните в производството не спорят, а и от осъществена от екип на КЗЛД проверка е установено, че в имота на ответниците е изградена и функционира система за видеонаблюдение състояща се от 1 броя стационарна камера IP Automat, модел V380-522, 2MPix – Full Hd 1080p, Обектив 3.6мм. Камерата е монтирана на фасадата на остъклена тераса на жилището на С. и има възможност за 360° панорамна гледка, като може да се върти на 320° хоризонтално и 90° вертикално. Към момента на проверката е установено, че хоризонталното въртене не функционира и камерата може да се върти само на 90° вертикално. Достъпът до изходящия образ в реално време се осъществява единствено от П.С. – отдалечено посредством софтуерно приложение, инсталирано на мобилния му телефон, като не е установено наличие на записващи устройства и други технически съоръжения, позволяващи осъществяването на видеозапис, въпреки че видеокамерата има възможност за запис на видеокадри на ONVIF TF – карта памет, каквато към момента на проверката липсва.

Доколкото не е констатиран запис и съхранение на кадри от видеонаблюдението се налага извода за осъществен от ответника „мониторен контрол“ - ограничена форма на видеонаблюдение - наблюдение с технически средства, без възможност за запис на получените данни, по смисъла на § 1, т. 6 от ДР на ЗЧОХ.

Доказателствата по преписката свидетелстват, че достъп до личните данни събирани посредством техническото устройство има само П.С., предвид което същият има качеството на администратор на лични данни по смисъла на чл. 4, ал. 7 от ОРЗД. Липсват доказателства останалите ответници, пасивно легитимирани страни в производството, да имат отношение към наблюдението, респективно достъп до събраните чрез него лични данни, предвид което по отношение на тях - Ж.С., С.П.С. и Л.С., жалбата следва да бъде оставена без уважение като неоснователна.

В производството не е спорно, че целта на наблюдение е охрана на движима собственост – бус на ответниците. Констатирано е обаче, че в обхвата на наблюдение попада и част от имота на

жалбоподателите – входната врата на двора и входната врата на жилищната сграда, обстоятелство за което свидетелства констативен протокол по чл. 593 от ГПК от 29.07.2020 г. с рег. № *** по описа на нотариус К.М. За последното свидетелства и осъществена от екип на КЗЛД проверка която е констатирала, че „когато камерата е в крайната си позиция нагоре по вертикала, тя заснема отново прозорците на терасата и алеята, но обхваща и входа на имота за автомобили, малка част от оградата, разделяща имота от този на жалбоподателите, както и много малка част от имота на жалбоподателите, в т. ч. част от къщата им и подстъпа към вход ѝ. Предвид горното твърдения на ответниците, че в „Обхватът на камерата е изцяло в имота на ответниците“ не кореспондира със събраните по преписката доказателства.

Предвид целта на осъществявано наблюдение чрез техническо средство и неговия обхват, същото е незаконосъобразно, а и в нарушение на принципа на свеждане на данните до минимум – чл. 5, § 1, буква „а“ и „в“ от ОРЗД. Противно на наблюдението чрез техническо средство осъществявано в рамките на собствения имот или на собствена вещ, не може да се приеме, че наблюдението чрез техническо средство на част от съседни чужди имоти представлява легитимен интерес на администратора предвид липсата на преимуществен интерес на последния пред интереса на физическите лица обект на наблюдението. Не е спорно, че наблюдението на имота на жалбоподателите чрез техническо средство се осъществява без тяхно съгласие (чл. 6, § 1. буква „а“ от ОРЗД), както и че за осъществяването му не са налице предпоставките на чл. 6, § 1, букви „б“, „в“, „г“ и „д“ от ОРЗД. В конкретния случай обработването на лични данни посредством наблюдение чрез техническо средство на съседни имоти е в противоречие и с принципа „свеждане на данните до минимум“ по чл. 5, § 1, б. „в“ от ОРЗД, предвид обстоятелството, че същото не е ограничено до необходимото във връзка с целите за неговото осъществяване – охрана на движима собственост на ответниците. Нещо повече комисията намира, че наблюдението на мястото на което е паркирано превозното средство също е в нарушение на принципа на законосъобразност, доколкото липсва условие за неговата законосъобразност - наблюдаваната посредством камерата движима вещ е паркиран на терен, който не е собственост на администратора и по скоро следва да се третира като прилежаща площ към етажната собственост. В тази връзка не може да се приеме, че П.С. има надделяващ легитимен интерес над интереса на останалите съсобственици в етажната собственост, като факта, че преимуществено на това място се паркира МПС на лицето не променя това обстоятелство, доколкото не е спорно, че МПС-то е в движение и не пребивава постоянно на мястото което под наблюдение, още повече че за видеонаблюдението на този терен няма решение на Общото събрание на етажната собственост, доколкото бусът е паркиран в двора на кооперацията зад дворната врата. Не може да се подкрепи разбирането на ответната страна, че охраната на движимо имущество може да има приоритет пред защита на личната свобода и неприкосновеност на жалбоподателите чрез наблюдение на тяхното дворно място и подход към жилищната сграда, която обитават или чрез наблюдение на терен който не е собственост на администратора. В случай че лицето иска да охранява това имущество, той следва да постави камера с подходящи технически параметри, като в случай че се вземе решение на етажната собственост за наблюдение на този периметър около етажната собственост, то администраторът следва да предприеме подходящи организационни и технически мерки, така че да ограничи наблюдението на публични места и чужди имоти или части от такива.

В случая не е спорно, че наблюдението на мястото на което е паркирано превозното средство се осъществява без съгласие на останалите съсобственици на имота (чл. 6, § 1. буква „а“ от ОРЗД), както и че за осъществяването му не са налице предпоставките на чл. 6, § 1, букви „б“, „в“, „г“ и „д“ от ОРЗД, като преимуществен легитимен интерес на администратора не може да бъде обоснован по съображения изложени по-горе, предвид което наблюдението е в нарушение на принципа на законосъобразност. Последното важи с още по-голяма сила и по отношение на наблюдението на обществени места, в случая част от прилежаща към имота улица.

Предвид характерът и видът на констатираното нарушение и обстоятелството, че същото не е преустановено, а също и че засегнатите лични данни не са чувствителни по смисъла на закона и няма

данни за настъпили вреди от обработването, комисията счита за целесъобразно, пропорционално и ефективно налагането на корективна мярка по чл. 58, § 2, буква „г“ от Регламент ЕС 2016/679, като намира, че същата ще постигне целта на закона - ще преустанови нарушението и ще възстанови установения правов ред по отношение на обработването на личните данни. Останалите мерки за по чл. 58, § 1, буква „а“, „б“, „в“, „д“, „е“, „ж“, „з“ и „й“ от ОРЗД са неприложими и нецелесъобразни поради естеството на нарушението и обстоятелството, че към момента на произнасяне същото не е преустановено. Комисията намира, че доколкото нарушението е първо налагането на глоба на администратора би било прекомерно и в нарушение на принципа на съразмерност по чл. 6 от АПК съгласно който „когато с административния акт се засягат права или се създават задължения за граждани, се прилагат онези мерки, които са по-благоприятни за тях, ако и по този начин се постигне целта на закона.“ Следва обаче да се отбележи, че неизпълнението на даденото от комисията разпореждане, в указания срок, е скрепено със санкция за неизпълнение с оглед неговата ефективност и възможността за допълнителен санкционен механизъм по проверка и контрол на изпълнението. Целта е постигане на генерална превенция и пропорционално и законосъобразно обработване на лични данни. Така разпореждания са ефективни, тъй като са скрепени със съответните санкции при неизпълнение, като законодателя предвижда при неспазване на влязло в сила разпореждане на надзорния орган да бъде наложено административно наказание „глоба“ или „имуществена санкция“ по чл. 83, параграф 6 от Регламент 2016/679 в размери до 20 000 000 EUR.

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

РЕШИ:

1. Обявява жалба ППН-01-778/04.11.2020 г. за неоснователна и недоказана по отношение на Ж.С., С.П.С. и Л.С.

2. Обявява жалбата за основателна по отношение П.С.

3. На основание чл. 58, § 2, буква „г“ за нарушение на чл. 5, § 1, букви „а“ и „в“ от Регламент (ЕС) 2016/679 издава разпореждане на администратора П.С. да преустанови заснемането на чужди имоти и обществени територии, като демонтира камерата.

4. Срок за изпълнение на разпореждането – едномесечен от влизането на решението в сила, след което да уведоми комисията за изпълнението като представи съответните доказателства.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

(О.М. по т. 2, 3 и 4)

РЕШЕНИЕ
№ ППН-01-654/2020 г.
София, 03.02.2022 г.

Комисията за защита на личните данни (КЗЛД) в състав: Председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков на заседание, проведено на 15.12.2021 г., на основание на основание чл. 10, ал. 1 от Закона за защита на личните данни, респективно чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламента, ОРЗД), разгледа по същество жалба № ППН-01-654/14.09.2020 г.

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

Комисията за защита на личните данни е сезирана с жалба, подадена от М.Б., с изложени твърдения за неправомерно обработване на личните му данни от служител на Министерство на вътрешните работи (МВР). Жалбата е адресирана и до Директора на ОДМВР - гр. Варна и до Окръжна прокуратура – Бургас.

Жалбоподателят информира, че заедно с четирима свои приятели, присъствал на футболен мач проведен на 12.09.2020 г. между „ЦСКА“ и „Черно Море“. Допълва, че на почивка между двете полувремена заедно с приятелите си напуснал стадиона, за да вземат шалове, шапки и тениски на отбора който подкрепят – ЦСКА, а на връщане към стадиона „точно на ъгъла на бул. „8-ми Приморски полк“ и ул. „Никола Вапцаров“ били нападнати от непознат мъж с обвинения, че са хвърлили бомба на стадиона. Твърди, че при виковете към тях се приближили трима полицаи, а един от полицаите, без да се легитимира им изискал личните карти, които снимал с телефона си, след което върнал документите за самоличност. Счита действията на полицаия за незаконосъобразни и в нарушение на чл. 45, ал. 1 и 2 от ЗЗЛД и моли комисията за проверка по случая. В допълнение твърди, че е осъществен състав на престъпление по чл. 325, ал. 1 от НК, както и нарушение на чл. 6, ал. 2 и чл. 14, ал. 5 от ЗМВР.

Към жалба не са приложени доказателства, посочени са свидетели на нарушенията.

Жалбата е подадена по електронен път, без квалифициран електронен подпис, поради което на жалбоподателя са дадени указания по редовност на искането, същите изпълнени - жалбата е потвърдена – депозирана на 13.01.2021 г., с подпис на жалбоподателя.

Предвид горното и с оглед застъпените в административния процес принципи на равенство на страните и истинност, министъра на вътрешните работи е информиран за образуването по случая административно производство, указана му е възможността да ангажира писмено становище по изложените в жалбата твърдения и да представи относими по случая доказателства.

В отговор е изразено становище за неоснователност на жалбата. Информират за образувана по случая проверка по преписка ***** по описа на ОДМВР-Варна, при която не са установени доказателства полицейски служители да са заснемали с мобилен телефон лични документи, както и същите да са били свидетели на такива действия от други техни колеги. Допълват, че от извършената проверка не са установени данни за извършени дисциплинарни нарушения или престъпления от полицейските служители. Сочат, че след приключване на проверката преписката е изпратена в Районна прокуратура – Варна, където е образувано ДП **** по чл. 131, ал. 1 т. 12 от НК, за което нямат данни дали е приключило. Молят комисията да остави жалбата без уважение, като неоснователна и недоказана.

На проведено на 20.10.2021 г. заседание на КЗЛД жалбата е приета за редовна и допустима - съдържа задължително изискуеми реквизити, подадена е в срока по чл. 38, ал. 1 от ЗЗЛД от физическо

лице с правен интерес срещу надлежна страна - администратор на лични данни по смисъла на чл. 4, § 7 от ОРЗД, каквото качество притежава министъра на вътрешните работи по смисъла на чл. 4, ал. 7 от Общия регламент ЕС 2016/679 и специалната норма и чл. 29, ал. 1 от Закона за Министерство на вътрешните работи.

Предмет на жалбата са твърдения за неправомерно обработване – събиране и съхранение на личните данни на жалбоподателя, съдържащи се в документ за самоличност, от служител на МВР, посредством снимане на личната карта с мобилен телефон и съхранение в устройството на направената снимка. Комисията е сезирана на 14.09.2020 г., само два дни след извършване на твърдяното нарушение, предвид което се налага извода, че жалбата е подадена срока по чл. 38, ал. 1 от ЗЗЛД.

Сезиран е компетентен да се произнесе орган – КЗЛД, която съгласно правомощията си по чл. 10, ал. 1 от ЗЗЛД във връзка с чл. 57, § 1, буква „е“ от Регламент (ЕС) 2016/679, разглежда жалби подадени от субект на данни срещу актове и действия на администраторите на лични данни, с които се нарушават правата на физическите лица свързани с обработване на личните данни, като не е налице изключенията по чл. 2, § 2, буква „в“ и чл. 55, § 3 от Регламент (ЕС) 2016/679 предвид обстоятелството, че случая не касае дейности по обработване извършвани от физическо лице в хода на чисто лични или домашни занимания и/или дейности извършвани от съдилищата при изпълнение на съдебните им функции. В тази връзка и за пълнота следва да се отбележи, че горното се отнася за изложените в жалбата твърдения относно нарушения на ЗЗЛД, като твърденията за извършени престъпления и дисциплинарни нарушения не са от компетентността на КЗЛД, а на останалите сезирани със случая органи МВР и прокуратура.

По изложените съображения и предвид липсата на отрицателните предпоставки посочени в чл. 27, ал. 2 от АПК, като страни в производството са конституирани: жалбоподател – М.Б. и ответна страна – министъра на вътрешните работи. Насрочено е открито заседание за разглеждане на жалбата по същество на 15.12.2021 г. от 13.00 часа, за което страните са редовно уведомени и им е указано разпределянето на доказателствената тежест в процеса. На жалбоподателя е предоставено за запознаване заверено копие на изразено от ответната страна писмено становище за неоснователност на жалбата с указания, че следва не по-късно от дата на откритото заседание да представи доказателства относно изложените в жалбата твърдения за неправомерно събиране и съхранение на личните му данни. Въпреки дадените указания, такива не са депозирани в КЗЛД.

За изясняване на случая от фактическа страна е изискана информация от ОДМВР-Варна и РП-Варна.

В отговор и с писмо ППН-01-654#11/29.11.2021 г. от ОДМВР – Варна информират, че при извършената по случая проверка „не са установени доказателства, че полицейски служители са извършили справки на посочените в жалбата на М.Б. лица, да са заснемали с мобилен телефон лични документи, както и същите да са станали свидетели на такива действия от страна а други техни колеги. От извършената проверка не са установени данни за извършени дисциплинарни нарушения или извършени престъпления от полицейски служители“. Допълват, че след приключване на проверката преписката е изпратена в Районна прокуратура – Варна по компетентност и е образувано досъдебно производство № *** по чл. 131, ал. 1, т. 12 от НК – причиняване на телесна повреда на М.Б. по хулигански подбуди. Последното се потвърждава и от отговор на РП – Варна, постъпил в КЗЛД с писмо ППН-01-654#11/29.11.2021 г., в което като допълнение е посочено, че досъдебното производство е спряно с постановление от 14.06.2021 г. поради неустановен извършител на деянието.

На проведено на 15.12.2021 г. заседание на комисията, жалбата е разгледана по същество.

Жалбоподателят М.Б. – редовно уведомен, не се явява и не се представлява в заседанието пред комисията.

Министърът на вътрешните работи се представлява от юрисконсулт с пълномощно по административната преписка. Оспорва жалбата. Не сочи нови доказателства, искания по

доказателствата няма. Счита жалбата за неоснователна и недоказана и моли комисията да я остави без уважение, като заявява, че описаната в жалбата до КЗЛД практика на служители на МВР за заснемане на документ за самоличност с мобилно устройство не е разписана като процедура в нито един вътрешен документ и не е практика на служителите на ведомството.

В качеството си на административен орган и във връзка с необходимостта от установяване истинността по случая, като основен принцип в административното производство, съгласно чл. 7 от АПК, изискващ наличието на установени действителни факти и предвид събраните доказателства и наведените твърдения, комисията приема, че разгледана по същество жалба № ППН-01-654/14.09.2020 г. е неоснователна.

Предмет на жалбата са твърдения за неправомерно обработване – събиране и съхранение на личните данни на жалбоподателя, съдържащи се в документ за самоличност, от служител на МВР, посредством снимане на личната карта с мобилен телефон и съхранение в устройството на направената снимка на 12.09.2020 г., около 19: 40 часа в гр. Варна „на ъгъла на ул. „8-ми Приморски полк“ и ул. „Никола Вапцаров“, при проверка от органите на реда за нарушение на обществения ред.

Заснемането на документ за самоличност – лична карта и съхранението на направеното изображение е форма на обработване на лични данни по смисъла на чл. 4, т. 2 от ОРЗД доколкото същото е извършено с автоматично средство, а съдържащата се в документа за самоличност информация има характера на лични данни за лицето, чрез която последното може да бъде безспорно индивидуализирано.

Твърденията на жалбоподателя, че при проверка от служители на МВР документа му за самоличност е заснет с мобилно устройство – телефон на единия от полицаите, а снимката е съхранена в паметта на устройството, са оспорени от ответната страна. Извършена по случая проверка от ОДМВР – Варна не е установила доказателства полицейски служители „да са заснемали с мобилен телефон лични документи, както и същите да са станали свидетели на такива действия от страна на други техни колеги.“ В тази връзка и доколкото жалбоподателя не ангажира доказателства в подкрепа на изложените в жалбата твърдения за обработване на лични данни, същата следва да бъде оставена без уважение, като неоснователна и недоказана, предвид разпределяне на доказателствената тежест в процеса.

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

РЕШИ:

Остава без уважение жалба № ППН-01-654/14.09.2020 г., подадена от М.Б., като неоснователна и недоказана.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № ПНМД-17-37/2022 г. гр. София, 24.02.2022 г.

ОТНОСНО: *Законосъобразно обработване на данни за трудови доходи на лицата за целите на определяне размера на удръжката по запор, наложен върху вземане на длъжник от пенсия*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов и Мария Матева, на свое редовно заседание, проведено на 23.02.2022 г., разгледа искане за становище с вх. № ПНМД-17-37/04.02.2022 г. от управителя на Националния осигурителен институт (НОИ), с което се поставя въпрос относно определянето размера на удръжката по запор, наложен върху вземане на длъжника от пенсия.

В писмото от НОИ се посочва, че е отправено запитване до Камарата на частните съдебни изпълнители (КЧСИ) за това как следва да се процедира в случаите, когато се налага запор върху пенсия, но в запорното съобщение е посочено, че лицето получава и трудово възнаграждение, без да е определен размерът на удръжката. В полученото становище от КЧСИ, което прилагат към искането, се казва, че „*НОИ се явява много по-информиран от съдебния изпълнител и много по-компетентен от работодателя на длъжника, да определи секвестрируемата част от дохода на лицето, доколкото начинът за това е ясно определен в разпоредбата на чл. 446, ал. 1, т. 1, т. 2 и т. 3 от ГПК, а информацията за размера на всички доходи на длъжника постъпва в НОИ всеки календарен месец*“. КЧСИ прави извод, че при наличие на указание от съдебния изпълнител, че длъжникът получава и доходи за положен труд от друг източник, НОИ следва да определи и преведе секвестрируемата част, а при съмнение за правилното прилагане на чл. 446 от ГПК – да поиска указание от съдебния изпълнител, като това указание ще бъде дадено при конкретни параметри на получаваните от лицето доходи и ще бъде валидно до тяхната промяна, за което НОИ следва да индикира.

От НОИ изразяват притеснения относно процедирането по описания начин, тъй като осигурителният институт е първичен администратор на данните за пенсия, но получава данните за осигурителен доход на лицата от Националната агенция за приходите (НАП), на законово основание – чл. 5, ал. 4 във вр. ал. 6, изр. посл., във вр. чл. 33, ал. 8 от Кодекса за социално осигуряване (КСО), във връзка с изпълнение на функциите, възложени на института по силата на чл. 33 от КСО.

От НОИ твърдят, че на съдебните изпълнители се предоставя достъп до регистрите в средата за междурегистров обмен RegiX, в т.ч. до Регистър на задължените лица на НАП/ Справка с данни за осигурените лица от подадени декларации по Наредба № Н-13 към КСО и съдържащите се в същата данни за осигурителен доход, както и до Регистър на пенсионерите на НОИ/ Справка за доход от пенсия и добавка. Въз основа на тези данни и в съответствие с правомощията си по ГПК, съдебните изпълнители могат да определят секвестрируемия доход на длъжника при налагане на запор върху пенсия, в случаите когато длъжникът получава пенсия и трудово възнаграждение. От НОИ считат, че възлагането да определя размера на секвестрируемия доход в тези случаи е свързано с това един администратор на лични данни да обработва данни, предоставени му от друг администратор, за цели, различни от тези на обработването.

Предвид гореизложеното, от НОИ молят КЗЛД за становище по въпроса за законосъобразното обработване на данни за трудови доходи на лицата за целите на определяне размера на удръжката по запор, наложен върху вземане на длъжника от пенсия.

Към искането е приложено и становището на КЧСИ по същия въпрос.

Правен анализ:

С Част пета на Гражданския процесуален кодекс (ГПК) – „Изпълнително производство“ се уреждат процесуалните правила, по които се развива производството по принудително изпълнение на частни вземания. За инициране на изпълнителното производство следва да е налице установено по съответния ред неизпълнение на изискуемо задължение на длъжника, като по своята същност то се явява правна възможност за принудително удовлетворяване на притезателното право на кредитора да получи своето вземане. В частност, определянето на т.нар. несеквестируем доход по смисъла на чл. 446 и чл. 446а от ГПК е елемент от сложния фактически състав на производството по изпълнение на парични вземания.

С оглед принудителния характер на този вид гражданско производство се налага и високата степен на неговата правна регламентация, като на всеки етап от процедурата следва да са изяснени детайлно правомощията, правата и задълженията на участниците в нея, което от своя страна е израз на принципа на правовата държава, прогласен в чл. 4 от Конституцията на Република България. В тази връзка, е от съществено значение да се подчертае, че обработването на лични данни настъпва вследствие на изпълнението на процесуалните правила, въведени с ГПК, които следва да го дефинират изчерпателно и точно с оглед гарантирането на правна сигурност и стабилност на изпълнителния процес.

Недопустимо е правилата за обработване на лични данни да са предпоставка за определяне и прилагане на процесуалните правила в изпълнителното производство. Тъкмо обратното, за да е допустимо обработването на лични данни (което по правило не е самоцелен процес), то следва да се извършва с определена легитимна цел. Видно от дефиницията в чл. 4, т. 7) от Регламент (ЕС) 2016/679 „администратор на лични данни“ 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.** В конкретния случай администраторите – и ЧСИ, и НОИ, имат конкретни задължения с оглед изпълнителното производство, като целите и средствата за обработването на лични данни, извършвано от тях, произтичат от ГПК.

Поставеният от НОИ въпрос не е свързан със законосъобразността на обработването на конкретни категории лични данни, а с това какви са процедурните правила и кой е натоварен от процесуалния закон да извърши определянето на несеквестируемия доход с оглед целите на изпълнителния процес. Разрешаването на този въпрос обаче не е от компетентността на надзорния орган по защита на данните. Нещо повече, едва след неговото разрешаване ще е възможно да се разсъждава върху приложимите правила и изисквания относно защитата на данните.

КЗЛД е постоянно действащ независим надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент (ЕС) 2016/679 и на ЗЗЛД (арг. чл. 6, ал. 1 от ЗЗЛД).

Разглеждането и разрешаването на спорове между отделни администратори на лични данни или допълването със становище на евентуални празноти в действащото законодателство, включително по процесуални въпроси, не попада в материалната компетентност на КЗЛД (арг. чл. 51 и чл. 55 във вр. с чл. 57 и 58 от Регламент (ЕС) 2016/679).

По тези съображения и на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Поставеният от НОИ въпрос относно юридическото действие по определяне на размера на удържката по заповед, наложен върху вземане на длъжника от пенсия, касае приложението на процесуалните правила, регламентиращи изпълнителния процес по Гражданския процесуален кодекс (ГПК).

2. Компетентен да разреши възникналия между НОИ и Камарата на частните съдебни изпълнители спор по прилагането на тези правила в случая е единствено съдът.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/



Комисия за защита на личните данни

Председател: Венцислав Караджов

Членове: Цанко Цолов
Мария Матева
Веселин Целков

Информационен бюлетин № 2 (95) 2022 г.

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

Уеб сайт на КЗЛД: www.cpdp.bg

Разпространява се в електронен вид

ISSN 2367-7759