

Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 4 (91), юли 2021 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода май и юни 2021 г.)

СЪБИТИЯ И ИНИЦИАТИВИ	3
Отбелязваме три години от началото на прилагане на Общия регламент относно защитата на данните	3
КЗЛД предостави на Народното събрание и на Европейската комисия информация в съответствие с изискванията на ЗЕС	4
КЗЛД публикува съвети към администраторите и обработващите лични данни за защита на данните в киберпространството	5
Заседания на Европейския комитет по защита на данните	7
Европейският комитет по защита на данните представи годишен доклад за дейността си през 2020 година	9
Европейската комисия предлага надеждна и сигурна цифрова самоличност за всички европейци	10
Европейската комисия представи нова стратегия за Шенгенското пространство	14
КОНТРОЛНА ДЕЙНОСТ НА КЗЛД	17
РЕШЕНИЯ НА КЗЛД	18
СТАНОВИЩА НА КЗЛД	23

СЪБИТИЯ И ИНИЦИАТИВИ

ОТБЕЛЯЗВАМЕ ТРИ ГОДИНИ ОТ НАЧАЛОТО НА ПРИЛАГАНЕ НА ОБЩИЯ РЕГЛАМЕНТ ОТНОСНО ЗАЩИТАТА НА ДАННИТЕ



На 25 май 2021 г. се навършиха три години от започване прилагането на Общия регламент относно защитата на данните (GDPR). За това време регламентът се утвърди като „златен стандарт“ на глобално ниво в областта на поверителността. В условията на глобализация, дигитално общество и цифрова трансформация на все повече сфери от живота, Европейският съюз се стреми да утвърди своята челна позиция в сферата на защитата на личните данни и пълното зачитане на правата на хората. От съществено значение е да се създадат условия за реализиране на технологичната революция при пълно зачитане на правата на хората. Данните са ценен елемент на цифровата икономика

и играят все по-важна роля за разработването на иновативни системи. Регламентът създава среда за разработване на заслужаващи доверие иновации, като гарантира, че гражданите имат по-голям контрол върху личните си данни и са все по-добре осведомени за своите права.

На предприятията Регламентът предоставя възможности да извлекат максимална полза от цифровите трансформации, като същевременно гарантира доверието на гражданите. Спазването на Регламента помага на предприятията да повишат сигурността на своите данни и да използват неприкосновеността на личния живот като конкурентно предимство.

Общият регламент относно защитата на данните гарантира свободния поток на лични данни между държавите-членки на ЕС. Извън Съюза той създава възможности за насърчаване на потоци от данни въз основа на високи стандарти между държави, споделящи ценностите на ЕС. Все повече държави по цял свят приемат правила за защита на данните, като използват стандарта на ЕС в тази област като отправна точка. Това сближаване открива нови възможности за безопасни потоци от данни между Европейския съюз и трети държави.

Регламентът предоставя на националните органи за защита на данните повече правомощия и възможности да координират своите действия чрез новите механизми за сътрудничество в рамките на Европейския комитет по защита на данните, с цел постигане на съгласувано прилагане на общата европейска правна рамка.

Две години след започването на прилагане на Регламента, на 24 юни 2020 г. бе публикуван първият **доклад за преглед и оценка на резултатите от изпълнението му**, чиито основни констатации бяха:

- Гражданите разполагат с повече възможности и са по-осведомени за правата си;
- Правилата за защита на данните са адаптирани за цифровата ера;
- Органите за защита на данните използват своите по-големи корективни правомощия;
- Органите за защита на данните работят заедно в рамките на Европейския комитет по защита на данните (ЕКЗД), но има възможност за подобрение;
- Използване на пълния потенциал на международното предаване на данни;
- Насърчаване на международното сътрудничество.

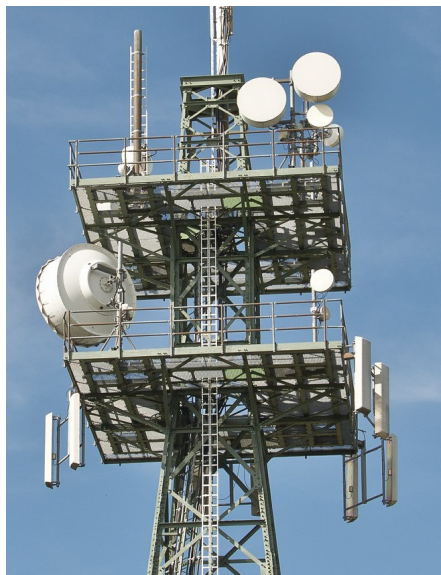
В Регламента се предвижда първият такъв доклад да се извърши **2 години след началото на прилагането му, както и на всеки четири години след това.**

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

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

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

По данни от Публичния регистър на предприятията, уведомили Комисията за регулиране на съобщенията за намеренията си да осъществяват обществени електронни съобщения (чл.33, ал.1, т.1 от ЗЕС), броят на предприятията към 21.04.2021 г. е **1133**. През 2020 г. **114 предприятия са подали в КЗЛД** ежегодна статистическа информация, което е около 10% от общия брой задължени субекти. Това е трайна тенденция, която би могла да се обясни с погрешното разбиране на задължените предприятия, че законовото им задължение възниква единствено при наличие на конкретни искания за достъп до информация през отчетната година.



От подадите информация 114 предприятия, 25 информират за поискана от тях информация за трафични данни. Въз основа на предоставената информация, КЗЛД прави следното обобщение на данните за 2020 година:

– **общият брой на исканията** за достъп до трафични данни е **с 26% по-малко** от този за 2019 г. Забелязва се трайна тенденция през последните години за намаляване на броя на поискана информация;

– случаите, при които **са били предоставени данни** на компетентните органи по чл. 251в, ал. 1 и ал. 2 и чл. 251г, ал. 7 са **над 99%** от всички искания, с което се запазва досегашната тенденция;

– в **61% от случаите** времето, изтекло от началната дата на съхранение до датата искане за предоставяне на данните, е **до 3 (три) месеца**

– случаите, при които **не е могло да се отговори** на искането за предоставяне на трафични данни, са **с 13% повече** в сравнение с 2019 г.

КЗЛД отчита бъдещите предизвикателства и тенденции за развитие в рамките на ЕС като посочва, че настоящите тенденции в развитието на сектора са свързани с постигането на по-висока степен на предвидимост на регулаторната рамка и правни разпоредби, отчитащи съвременните технически достижения. Към момента на общоевропейско ниво се обсъжда Предложението за Регламент на Европейския парламент и на Съвета относно зачитането на личния живот и защитата на личните данни в електронните съобщения и за отмяна на Директива 2002/58/ЕО (Регламент за неприкосновеността на личния живот и електронните съобщения), чиято основна цел е осигуряването на високо ниво на защита на неприкосновеността на личния живот на ползвателите на електронни

съобщителни услуги и еднакви условия на конкуренция за всички участници на пазара. Прегледът на сега действащото законодателство включва постигането на целите на Стратегията за цифров единен пазар на Европейския съюз (ЕС) и гарантира съгласуваност на предложените разпоредби с Общия регламент относно защитата на данните (Регламент (ЕС) 2016/679).

На общоевропейско ниво продължава работата по разпоредбите на Предложението за Регламент на Европейския парламент и на Съвета относно европейска рамка за управление на данните (Акт за управление на данните). Инструментът има за цел да насърчи наличността на данните с цел тяхното използване чрез повишаване на доверието в посредниците за данни и чрез укрепване на механизмите за споделяне на данни на територията на ЕС.

КЗЛД ПУБЛИКУВА СЪВЕТИ КЪМ АДМИНИСТРАТОРИТЕ И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ ЗА ЗАЩИТА НА ДАННИТЕ В КИБЕРПРОСТРАНСТВОТО

В изпълнение на чл. 33 от Регламент (ЕС) 2016/679, администраторите и обработващите лични данни имат задължението да уведомят на надзорния орган за настъпило нарушение на сигурността на личните данни. Комисията за защита на личните данни, която е надзорен орган в Република България, обработва получените уведомления, разглежда и оценява конкретните факти и обстоятелства, и осъществява цялостно наблюдение и анализ на процесите, свързани с вида и характеристиките на информацията от уведомленията.

Основно задължение на администраторите и обработващите лични данни е прилагането на подходящи технически и организационни мерки за осигуряване на сигурност на данните.

През последните месеци КЗЛД отчита увеличение на подадените уведомления за нарушения на сигурността на данните, свързани с пробиви в киберсигурността. Във връзка с това, както и с цел насърчаване на осведомеността на администраторите и обработващите лични данни за задълженията им, произтичащи от приложимото законодателство в областта на защитата на личните данни, КЗЛД публикува кратък материал със съвети относно подобряване на информационната сигурност.

СЪВЕТИ КЪМ АДМИНИСТРАТОРИТЕ И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ ЗА ЗАЩИТА НА ДАННИТЕ В КИБЕРПРОСТРАНСТВОТО

Дигиталната среда за обработване и съхраняване на данни поражда множество предизвикателства пред сигурността на информацията и в частност – на личните данни. Уязвимостите в компютърните системи и мрежи са обект на различни интереси, нерядко със злонамерен характер. Своевременното им откриване и отстраняване им е отговорност на съответните администратори. Практиката на КЗЛД при обработване на подадени уведомления за нарушения на сигурността на данните по чл. 33 от Регламент (ЕС) 2016/679, свързани с пробиви в киберсигурността, показва многообразие от случаи на нарушения, които биха могли да бъдат предотвратени с навременни мерки.

Ето и някои примери:

- Банка е станала жертва на кибератака срещу един от своите сайтове за онлайн банкиране. За да се стигне до пробива в сигурността са използвани всички възможни идентификатори за вход, като е използвана фиксирана тривиална парола (напр. *Password1*).
- Базите данни на сайт за онлайн пазаруване са били достъпни и изтеглени, след като кибернападателят е научил и използвал потребителското име и паролата на администраторския профил на сайта.

- Сървърите на фирма, предлагаща приложение, използвано от застрахователи за сключване на застраховки, са били хакнати. За да получи достъп до сървърите хакерът е използвал потребителските имена на служители на фирмата и приложение, което генерира и прилага милиони пароли за кратък период от време.

- Базите данни на фирма за събиране на задължения са били блокирани, след като неин служител е отворил фишинг имейл, който е заразил служебният му компютър с вирус.

Много често представители на малкия и среден бизнес разчитат на факта, че данните, които обработват, не са чувствителни или пък не се отнасят до голям брой лица и затова киберпрестъпниците не биха имали интерес да проникнат в тяхната компютърна инфраструктура. Напротив, много от киберпрестъпниците имат за цел точно малкия и среден бизнес, тъй като предполагат, че или не са заделени достатъчно средства за киберсигурност, или тя е била подценена. Често големите бизнеси са доста по-трудни за пробиване, защото те заделят сериозни средства за ИТ сигурност и постоянно подобряване на тяхната киберзащита. Затова силно препоръчваме на малкия и среден бизнес да въведе поне някои от предоставените съвети, които не изискват заделянето на допълнителни средства.

Според Регламент (ЕС) 2016/679, прилагането на подходящи технически и организационни мерки за осигуряване на сигурност на данните е основно задължение на администраторите и обработващите лични данни. В регламента са посочени и конкретни технически и организационни мерки за сигурност, като:

- Псевдонимизация;
- Криптиране;
- Гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- Своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- Редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки.

В тази връзка и с цел акцентиране върху сигурността на обработване на личните данни в информационните системи, КЗЛД насочва вниманието на администраторите и обработващите към следните практически съвети:

№	Съвет	Пояснения
1.	Въвеждане на високи изисквания за пароли	Изискване за дължина и ползване на големи и малки букви, цифри и символи. Изискване за периодична смяна на паролата (през 60-90 дни).
2.	Въвеждане на двуфакторна (мултифакторна) идентификация	Изисква се въвеждането на допълнителна информация от потребителя, например ПИН код, отговор на „таен въпрос“, еднократна парола (автоматично генерирана парола след всеки опит за влизане в потребителския профил, получавана обикновено чрез имейл или СМС), и т.н.
3.	Въвеждане на ограничение за грешно въведени пароли	При този метод се ограничава броя на грешно въведени пароли, за да се намали значително риска от “brute force” атака (между 3 и 5 грешни опита за влизане).

4.	Редовни актуализации на софтуера и фърмуера	Редовните актуализации на софтуера и фърмуера премахват критичните уязвимости, които хакерите използват за достъп до устройствата и системите.
5.	Използване на антивирусни програми	Антивирусните програми блокират достъпа на злонамерени софтуери и вируси до вашите устройства и компрометирането на съхраняваните данни.
6.	Използване на защитни стени	Защитните стени откриват хакери, вируси и друга злонамерена дейност в интернет и определя какъв входящ трафик е разрешен до вашите устройства.
7.	Редовно архивиране на данните	Архивирането помага за възстановяване на данните в случай на хакерска атака и загуба на тяхната наличност.
8.	Криптиране на данните	Криптирането на данните ограничава риска от нарушаване на поверителността на данните.
9.	Редовно обучение на персонала във връзка с правилата за киберсигурност	
10.	Въвеждане на План за реакция при инцидент с киберсигурността	

Съветите имат препоръчителен характер и не претендират за изчерпателност.

За да отговори на необходимостта от повече яснота относно предварителните и последващи действия на администраторите във връзка както с предотвратяването, така и с реакцията на нарушенията на сигурността на личните данни, в началото на 2021 г. Европейският комитет по защита на данните подготви и публикува за обществена консултация **Насоки 01/2021 с конкретни примери**. От множеството предложения и мнения за допълнение към документа е видна изключителната заинтересуваност и ангажираност към темата на широк кръг заинтересувани лица - надзорни органи, бизнес организации, неправителствени организации, физически лица.

ЗАСЕДАНИЯ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ

На заседанията, проведени през месеците май и юни 2021 г. Европейският комитет по защита на данните (ЕКЗД) прие редица документи.

ЕКЗД прие **две становища по първите проекти на решения относно транснационални кодекси за поведение**, представени от белгийския и френския надзорни органи. Проектът на решение на белгийския орган се отнася до кодекса за поведение на EU CLOUD, който е предназначен за доставчиците на компютърни услуги „в облак“. Проектът за решение на френския орган се отнася до кодекса за поведение на CISPE, който ще се прилага от доставчиците на инфраструктура за предоставяне на компютърни услуги „в облак“. Тези кодекси имат за цел да предоставят практически насоки и да определят специфични изисквания за за обработващите лични данни в ЕС, за които се прилагат тези кодекси. Не се предвижда те да се използват в случаи на международното предаване

на лични данни. ЕКЗД е на мнение, че и двата проекта на кодекси са в съответствие с Регламента и отговарят на изискванията, посочени в членове 40 и 41 от ОРЗД. Придържането към одобрените кодекси за поведение може да се използва като елемент за доказване на правно съответствие.

ЕКЗД прие **Изявление относно Акта за управление на данните с оглед на развитието на законодателния процес**. Изявлението е последващо действие във връзка със съвместното становище на ЕКЗД и ЕНОЗД относно Акта за управление на данните и подсилва основните забележки, направени в него. ЕКЗД отново подчертава, че без солидни гаранции за защита на данните съществува риск доверието в цифровата икономика да не бъде устойчиво. Освен това в изявлението се акцентира върху необходимостта да се осигури съгласуваност на Акта за управление на данните с достиженията на правото на ЕС в областта на защитата на данните, а съзаконодателите се призовават да разгледат внимателно някои аспекти, като например взаимодействието между Акта за управление на данните и ОРЗД, както и значението на това да се гарантира, че новите определения и понятия не са несъвместими с ОРЗД.

Комитетът прие **Препоръки относно правното основание за съхранението на данни за кредитна карта единствено с цел улесняване на по-нататъшни онлайн трансакции**. Целта на препоръките е да се насърчи хармонизирано прилагане на правилата за защита на данните по отношение на обработването на данни за кредитни карти в рамките на Европейското икономическо пространство (ЕИП) и да се гарантира еднородна защита на правата на физическите лица при пълно зачитане на основните принципи за защита на данните. ЕКЗД подчертава, че доверието в цифровата среда е критично условие за развитието на цифровата икономика и електронната търговия, които отбелязаха огромен скок в условията на пандемия от COVID-19. В препоръките се прави преглед на основанията за съхранение на данни за кредитна карта единствено с цел улесняване на по-нататъшни онлайн трансакции и се посочва, че съгласието в съответствие с чл. 6 (1) (а) от ОРЗД следва да се счита за единственото подходящо правно основание за съхраняване на данни на кредитни карти след покупката.

След проведена обществена консултация ЕКЗД прие окончателна версия на **Препоръки относно мерките, които допълват инструментите за трансфер, за да се гарантира спазването на нивото на защита на личните данни в ЕС**. Препоръките бяха приети за първи път през ноември 2020 г. след решението на Съда на ЕС по Schrems II. Тяхната цел е да подпомогнат администраторите и обработващите лични данни, действащи като износители на данни, със задължението им да идентифицират и прилагат подходящи допълнителни мерки, когато е необходимо, за да осигурят по същество равностойно ниво на защита на данните, които предават на трети държави. Окончателната версия на препоръките включва няколко промени, с които са отразени коментари и обратна връзка, получени по време на обществената консултация, и поставя специален акцент върху практиките на публичните органи на трета държава.

ЕКЗД и ЕНОЗД приеха **Съвместно становище относно предложението на Европейската комисия за регламент за определяне на хармонизирани правила относно изкуствения интелект**. Двата органа приветстват целта да се обърне внимание на използването на системи за изкуствен интелект в Европейския съюз, включително използването им от институции, органи или агенции на ЕС. В становището си те призовават за забрана на използването на изкуствен интелект за автоматизирано разпознаване на човешки характеристики в публично достъпни пространства, както и някои други употреби на изкуствения интелект, които могат да доведат до дискриминация. ЕКЗД и ЕНОЗД подчертават необходимостта да се изясни изрично, че съществуващото законодателство на ЕС за защита на данните се прилага за всяка обработка на лични данни, попадаща в обхвата на проекта за регламент за изкуствения интелект. Въпреки че приветстват подхода, основан на риска, залегнал в предложението, те считат, че понятието „риск за основните права“ следва да бъде приведено в съответствие с рамката на ЕС за защита на данните.

Като се вземат предвид изключително високите рискове, породени от дистанционната биометрична идентификация на лица в публично достъпни пространства, ЕКЗД и ЕНОЗД призовават

за обща забрана за всякаква употреба на изкуствен интелект за автоматизирано разпознаване на човешки черти в публично достъпни пространства, като разпознаване на лица, походка, пръстови отпечатыци, ДНК, глас, натискане на клавиши и други биометрични или поведенчески сигнали, във всеки контекст. Също така препоръчват забрана на системите за изкуствен интелект, използващи биометрични данни, за категоризиране на индивиди в групи (кълъстери) въз основа на етническа принадлежност, пол, политическа или сексуална ориентация или други основания, на които е забранена дискриминацията съгласно член 21 от Хартата на основните права. ЕКЗД и ЕНОЗД обръщат внимание на факта, че органите по защита на данните вече прилагат ОРЗД и Директивата за защита на данните в правоприлагането в системи за изкуствен интелект, включващи лични данни, за да гарантират защитата на основните права и по-конкретно правото на защита на данните. В резултат определянето на органите по защита на данните за национални надзорни органи би осигурило по-хармонизиран регулаторен подход и би допринесло за еднаквото тълкуване на разпоредбите за обработка на данни в целия ЕС.

ЕВРОПЕЙСКИЯТ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ ПРЕДСТАВИ ГОДИШЕН ДОКЛАД ЗА ДЕЙНОСТТА СИ ПРЕЗ 2020 ГОДИНА



European Data Protection Board

На 2 юни 2021 г. Европейският комитет по защита на данните (ЕКЗД) представи своя Годишен доклад за 2020 г., озаглавен „Гарантиране на правата за защита на данните в променящия се свят“.

Европейският комитет за защита на данните е независим европейски орган, създаден с Общия регламент относно защитата на данните (ОРЗД), който има за цел да осигури съгласувано прилагане на правилата за защита на данните в Европейското икономическо пространство (ЕИП). Тази цел се постига чрез насърчаване на сътрудничеството между националните надзорни органи и издаване на общи насоки за цялото ЕИП относно тълкуването и прилагането на правилата за защита на данните. ЕКЗД е съставен от представители на националните органи за защита на данните и Европейския надзорен орган по защита на данните. Без право на глас в него участват представители на Европейската комисия и на надзорните органи на Исландия, Лихтенщайн и Норвегия (които са страни от ЕИП, но не и на ЕС), които също са членове на ЕКЗД.

В Годишния доклад ЕКЗД отчита работата си по всички направления в своята дейност – издаване на насоки, препоръки, становища, решения; провеждане на консултации; насърчаване на сътрудничеството между органите по защита на данните и т.н.

Докладът на ЕКЗД за 2020 г. предоставя подробен преглед на работата, извършена от Комитета през годината, белязана от световната пандемия от КОВИД-19, която промени значително живота на хората в целия свят. По думите на председателя на ЕКЗД, Андреа Йелинек, „локдауните през 2020 г. във всички наши държави не означават спад в дейността на ЕКЗД“. Комитетът отчита, че 2020 година е белязана от много важни развития в правната сфера на ЕС за защита на данните, изискващи неговия експертен опит и насоки. Във връзка с предприетите в държавите-членки на ЕИП мерки за наблюдение, ограничаване и смекчаване на разпространението на вируса, Комитетът е издал насоки относно приложенията за местоположение и проследяване на контакти; обработка на здравни данни за научни изследвания; ограничения на правата на субекта на данните при извънредно положение и обработка на данни в контекста на повторно отваряне на граници.

Отчетени са дейностите на ЕКЗД, последващи Решението на Съда на Европейския съюз по случая Schrems II, което има значителни последици за базираните в ЕИП субекти, които прехвърлят данни в САЩ и други трети държави.

През 2020 г. Комитетът приема **10 насоки** по теми като концепциите за администратор и обработващ; таргетиране на потребители на социални медии, както и три насоки в окончателните им версии след проведени консултации (относно видео устройствата, правото да бъдеш забравен и защита на данните по дизайн и по подразбиране). Издадени са **32 становища по чл. 64** от Регламента. Прието е **първото решение за разрешаване на спорове на основание чл. 65** от Регламента. През 2020 г. има 628 трансгранични случая, от които 461 произтичат от подадена жалба, докато 167 имат друг произход (като разследвания, правни задължения и/или съобщения в медиите).

През 2020 г. ЕКЗД определя своята стратегия за 2021-2023 г., която обхваща четири основни стълба със стратегически цели:

1. Подобряване на хармонизацията и улесняване на съгласуваността;
2. Подпомагане на ефективното прилагане и ефективно сътрудничество между националните надзорни органи;
3. Подход към новите технологии, базиран на основните права
4. Глобално измерение.

За всеки от стълбовете е определен набор от ключови действия, които да спомогнат за постигането на тези цели.

Годишният отчет на ЕКЗД за 2020 г. е публикуван [ТУК](#).

ЕВРОПЕЙСКАТА КОМИСИЯ ПРЕДЛАГА НАДЕЖДНА И СИГУРНА ЦИФРОВА САМОЛИЧНОСТ ЗА ВСИЧКИ ЕВРОПЕЙЦИ



На 03 юни 2021 г. Европейската комисия предложи рамка за **европейска цифрова самоличност**, която ще бъде достъпна за всички граждани на ЕС, пребиваващи в ЕС лица и предприятия в ЕС.

Тази инициатива Комисията надгражда върху съществуващата трансгранична правна рамка за надеждни цифрови самоличности (Регламент относно електронната идентификация и удостоверителните услуги). Приета през 2014 г., тя предоставя основата за трансгранична електронна идентификация, удостоверяване на автентичност и сертифициране на уебсайтове в рамките на ЕС. Няма обаче изискване към държавите членки да разработят национална цифрова самоличност и да я направят оперативно съвместима с разработените от други държави членки решения, което води до големи различия между държавите.

С настоящото предложение се премахват тези недостатъци, като се подобрява ефективността на рамката и се разширяват ползите от нея върху частния сектор и мобилната употреба. Гражданите ще могат да доказват самоличността си и да споделят електронни документи от своите европейски портфейли за цифрова самоличност, както и да имат достъп до онлайн услуги чрез своята национална цифрова идентификация, която ще се признава в цяла Европа. Най-големите платформи ще бъдат задължени да приемат европейските портфейли за цифрова самоличност по искане на ползвателя. Използването на европейския портфейл за цифрова самоличност винаги ще бе по избор на потребителя.

Съгласно новия регламент държавите членки ще предлагат на гражданите и предприятията цифрови портфейли, които ще могат да свържат техните национални цифрови самоличности с данни

за други лични характеристики (напр. свидетелство за управление на МПС, дипломи, банкова сметка). Тези портфейли могат да бъдат предоставяни от публични органи или от частни субекти, които се признават от съответната държава членка.

Комисията приканва държавите членки да създадат общ инструментариум до септември 2022 г., като започнат необходимата подготвителна работа незабавно. Този инструментариум следва да включва техническата архитектура, стандарти и насоки за най-добри практики. Комисията ще подкрепи прилагането на европейската рамка за цифрова самоличност чрез програмата „Цифрова Европа“, а много държави членки са предвидили проекти за прилагането на решения за електронно управление, включително на европейската цифрова самоличност в своите национални планове в рамките на [Механизма за възстановяване и устойчивост](#).

Под формата на въпроси и отговори Европейската комисия е предоставила следният документ **с разяснения относно европейската цифрова самоличност**:

Какво представлява цифровата самоличност?

Идентификацията ни позволява да докажем кои сме. Ето защо в ежедневието си ползваме паспорти и лични карти. Цифровата самоличност ни помага да пестим време и опростява взаимодействията. В момента множество частни и публични доставчици предлагат средства за цифрова самоличност, които позволяват например достъп на потребителите до различни обществени услуги онлайн или онлайн банкиране. Тези средства предлагат различна степен на надеждност и сигурност. Големите платформи позволяват на своите потребители да влизат в профила си и да ползват различни услуги онлайн — от пазаруване до четене на новини — но не им предоставят пълен контрол върху данните, които те споделят при идентификацията си, за да ползват онлайн услуги.

Какво представлява европейският портфейл за цифрова самоличност?

Много граждани вече използват цифрови портфейли на своите смартфони, за да съхраняват бордните си карти, когато пътуват, или виртуалните си банкови карти с цел удобство при плащане. Съгласно новите правила европейските портфейли за цифрова самоличност ще бъдат на разположение на всички. Това са лични цифрови портфейли, които позволяват на гражданите да се идентифицират по цифров път и да съхраняват и управляват данни за самоличност и официални документи в електронен формат. Тези документи може да включват свидетелство за управление на МПС, медицински рецепти или дипломи. С помощта на портфейла гражданите ще могат да доказват самоличността си, когато това е необходимо, за да получат достъп до услуги онлайн, да споделят цифрови документи или просто да докажат конкретна лична характеристика, например възраст, без да разкриват своята самоличност или други лични данни. Във всеки един момент гражданите ще имат пълен контрол върху данните, които споделят.

Какво ще се промени за европейците?

Основният нов елемент, предлаган от новите правила, е, че всеки ще има право на европейски портфейл за цифрова самоличност, който се приема във всички държави членки. Той обаче няма да е задължителен. Потребителите ще могат да контролират какви лични данни искат да споделят във връзка с онлайн услуги. Макар че доставчиците на обществените услуги, както и на някои частни услуги, ще бъдат задължени да признават европейската цифрова самоличност, благодарение на нейните защитни елементи всички частни доставчици на услуги признават използването ѝ за услуги, изискващи задълбочено удостоверяване на самоличността на клиента, като по този начин се създават нови възможности за бизнес.

Какво мога да правя с новия европейски портфейл за цифрова самоличност?

Ще можете да използвате портфейла за достъп както до публични, така и до частни услуги онлайн в ЕС, по-специално за такива, които изискват задълбочено удостоверяване на самоличността на клиента. Примери за такива услуги са: достъп до банкова сметка или кандидатстване за заем, подаване на данъчни декларации, записване в университет във вашата държава или в чужбина, както и много други дейности, при които използвате обичайните си средства за идентификация.

За каква цел мога да използвам моя европейски портфейл за цифрова самоличност?

Ето няколко примера за това как европейският портфейл за цифрова самоличност би могъл да се използва, щом бъде на разположение:

Използване на европейския портфейл за цифрова самоличност: Петър е инсталирал личен цифров портфейл на мобилния си телефон. Той е предоставен от неговата държава, като се гарантира, че портфейлът е издаден лично на него. Цифровият портфейл на Петър му позволява да изтегли, съхранява и използва основните си лични данни, шофьорска книжка, диплома и банкова карта, която преди това е носил като физически карти във физическия си портфейл.

За да докажете възрастта си: Мира чака на опашка, за да влезе в нощен клуб, а охранителят на вратата иска да види документа ѝ за самоличност. Вместо да покаже личната си карта, тя използва своя европейски портфейл за цифрова самоличност. Охранителят може да провери, че Мира е навършила установената от закона минимална възраст, а тя може да предпочете да използва своя портфейл за цифрова самоличност, за да потвърди възрастта си, без да показва никакви други лични данни.

За наемане на автомобил на летище: Сара обикновено чака реда си на опашката на гишето за отдаване под наем на автомобили на летището. Тя изчаква, докато дружеството за отдаване на автомобили под наем направи копие на паспорта или личната ѝ карта, свидетелството за управление на МПС и кредитната ѝ карта и подписва всички документи. С помощта на цифровата самоличност това може да се направи, без да се налага да чакате на опашката, и дори преди да пристигнете в офиса на дружеството. Сега Сара ще може да отиде направо на паркинга, да вземе автомобила и да потегли към хотела си. Дружеството за отдаване на автомобили под наем може да ѝ даде ключа от автомобила на паркинга или да даде възможност автомобилът да бъде стартиран чрез мобилния телефон.

Доказване на вашата самоличност, за да използвате услуга онлайн: Курт заминава на работа в друга държава. Той трябва да се регистрира като пребиваващ в новата държава и за тази цел може да използва своя европейски портфейл за цифрова самоличност. Курт може да използва своя портфейл също така, за да докаже самоличността си за различни онлайн услуги в новата си държава на пребиваване, като например да си открие банкова сметка, да закупи SIM карта за мобилния си телефон или да си направи абонамент за обществен транспорт.

Каква е добавената стойност в сравнение с настоящата система?

Европейските портфейли за цифрова самоличност ще бъдат изградени върху надеждни цифрови самоличности, предоставени от държавите членки, като ще бъде подобрена тяхната ефективност, ще бъдат разширени ползите от тях за частния сектор и ще бъдат предложени лични цифрови портфейли, които са сигурни, безплатни, удобни за използване и защитават личните данни.

За тази инициатива Комисията доразвива съществуващата трансгранична правна уредба за надеждни цифрови самоличности — европейската инициатива за електронна идентификация и удостоверителни услуги (Регламент относно електронната идентификация и удостоверителните услуги).

Регламентът беше приет през 2014 г. и осигурява основата за трансграничната електронна идентификация, удостоверяването на автентичност и сертифицирането на уебсайтове в рамките на ЕС. В регламента обаче не е предвидено задължение държавите членки да предоставят на своите граждани и предприятия система за цифрова самоличност, даваща възможност за сигурен достъп до обществени услуги, нито да гарантират нейното използване отвъд границите на ЕС. В него не съдържат и разпоредби относно използването на такава идентификация за частни услуги или с мобилни устройства. Това води до различия между отделните държави.

Някои държави предлагат система за идентификация на своите граждани, други — не, а дори когато такива системи са налице, не всички от тях могат да се използват трансгранично. В момента в 14 държави членки се използват 19 схеми за електронна идентификация, за които е подадено уведомление и които обхващат 60 % от населението на ЕС-27, но възприемането им е слабо, използването им — тромаво, а въвеждането им от бизнеса е ограничено.

Пандемията от коронавирус и преминаването към цифрови услуги показаха, че тази ситуация има ограничения, които трябва спешно да бъдат преодоляни.

Какво се случва със съществуващата ми електронна идентификация? Трябва ли да наново да се регистрирам?

Не. Европейските портфейли за цифрова самоличност ще се основават на националните системи, които вече съществуват в някои държави членки. В момента не всяко лице, живеещо в ЕС, има достъп до средство за цифрова самоличност.

Как мога да получа европейски портфейл за цифрова самоличност?

Държавите членки ще предлагат портфейла на национално равнище на своите граждани и пребиваващите в държавата лица. Всеки ще може да изтегли, инсталира и използва европейския портфейл за цифрова самоличност на своя личен смартфон или друго устройство.

Как ще бъдат гарантирани сигурността, неприкосновеността на личния живот и защитата на личните данни?

В предложението се предвижда високо ниво на сигурност. Комисията ще предложи и съгласува с държавите членки стандартите, техническите спецификации и оперативните аспекти, за да се гарантира, че европейските портфейли за цифрова самоличност на държавите членки предлагат най-високи нива на сигурност. Държавите членки ще сертифицират портфейлите си, за да се уверят, че те отговарят на тези изисквания. Всички лични данни ще бъдат споделяни онлайн само ако гражданинът желае да направи това.

Комисията предвижда ли единната европейска цифрова самоличност да замени националните цифрови самоличности?

Не. Целта на регламента не е такава. Държавите членки ще продължат да предоставят цифрови самоличности. Европейската рамка за цифрова самоличност изгражда на тази основа и разширява функционалността и използваемостта на националните документи за електронна идентификация посредством личен цифров портфейл.

Как ще гарантирате, че системите са оперативно съвместими и че работят между различните държави членки?

Комисията ще предложи и съгласува с държавите членки стандартите, техническите спецификации и оперативните аспекти чрез акт за изпълнение.

Кога мога да използвам този личен цифров портфейл?

Държавите членки следва да започнат да издават новите европейски портфейли за цифрова самоличност една година след влизането в сила на настоящия нов регламент.

Каква е целта на общия инструментариум, предложен заедно с европейската рамка за цифрова самоличност?

Пандемията от коронавирус изостри необходимостта от ефективни и лесни за ползване цифрови услуги в целия ЕС. Няма време за губене. От съществено значение е държавите членки незабавно да започнат работа с Комисията и частния сектор, за да подготвят въвеждането на европейската рамка за цифрова самоличност. Веднага щом Комисията приеме предложението, ще се организира тясно сътрудничество за обсъждане на техническото изпълнение и определяне на общи стандарти.

Какъв е графикът за разработване, приемане и прилагане на инструментариума?

Незабавно ще започне работата за постигане на договореност с държавите членки относно бъдещите действия. Целта е до септември 2022 г. държавите членки, в тясно сътрудничество с Комисията, да постигнат съгласие по инструментариума за прилагане на европейската рамка за цифрова самоличност, а Комисията да публикува този инструментариум през октомври 2022 г. След като бъде договорена техническата рамка, той може да бъде тестван в пилотни проекти.

ЕВРОПЕЙСКАТА КОМИСИЯ ПРЕДСТАВИ НОВА СТРАТЕГИЯ ЗА ШЕНГЕНСКОТО ПРОСТРАНСТВО

На 2 юни 2021 г. Европейската комисия представи нова **стратегия за Шенгенското пространство**, чиято цел е най-голямата зона за свободно пътуване в света да стане по-силна и по-устойчива. Тази стратегия се основава на обширни консултации с членовете на Европейския парламент и министрите на вътрешните работи, заседавали в рамките на Шенгенския форум през ноември 2020 г. и май 2021 г. При представянето на новата стратегия, Европейската комисия публикува прессъобщение, в което заявява:

„Шенгенското пространство обхваща 26 държави, в които живеят над 420 милиона души. Премахването на контрола по вътрешните граници между шенгенските държави е неразделна част от европейския начин на живот: почти 1,7 милиона души живеят в една държава от Шенгенското пространство и работят в друга. Хората са изградили живота си около свободите, предлагани от Шенгенското пространство, като всеки ден 3,5 милиона души пресичат границите между шенгенските държави.

Свободното движение на хора, стоки и услуги е в основата на Европейския съюз и е от ключово значение за възстановяването на Европа след кризата с коронавируса. С днешната стратегия

Комисията прави оценка на предизвикателствата, пред които е изправено Шенгенското пространство през последните години, и очертава път напред, който запазва ползите от Шенген. Необходими са общи действия на равнището на Съюза, за да могат държавите членки да се справят с днешните предизвикателства.

Доброто функциониране на Шенгенското пространство се основава на три стълба: ефективно управление на външните граници на ЕС, укрепване на вътрешните мерки за компенсиране на липсата на контрол по вътрешните граници, по-специално по отношение на полицейското сътрудничество, сигурността и управлението на миграцията, и осигуряване на солидна подготовка и управление, включително завършването на процеса на интегриране в Шенгенското пространство. С цел да се насърчи взаимното доверие в прилагането на шенгенските правила, днес Комисията представя и **предложение за преразглеждане на механизма за оценка и наблюдение по Шенген.**“

Във връзка с представянето на стратегията, председателят и членове на Европейската комисия направиха следните изявления

Урсула фон дер Лайен, председателят на Европейската комисия: „Свободата на движение, живот и работа в различни държави членки е свобода, която европейските граждани високо ценят. Шенгенското пространство е едно от най-големите постижения на ЕС, но различните кризи и предизвикателства ни показаха, че не можем да приемем Шенген за даденост. Днес представяме начин за постигане на напредък, който да гарантира, че Шенген може да понесе изпитанието на времето — начин, който ще гарантира свободното движение на хора, стоки и услуги, независимо от обстоятелствата — така че да възстановим нашите икономики и заедно да излезем по-силни от кризата.“

Маргаритис Схинас, заместник-председател на Европейската комисия, който отговаря за утвърждаването на европейския начин на живот: „Безпрепятственото движение в рамките на Шенгенското пространство е от съществено значение за нашия европейски начин на живот. Шенгенското пространство е добре смазана машина, но подобно на всяка машина, неговите основи трябва постоянно да се поддържат и укрепват. Днес определяме нов път напред, който гарантира сигурността и мобилността на гражданите на ЕС, като същевременно повишава устойчивостта на Шенген към предизвикателства. Естествено, Шенген не е завършен без всички наши държави членки. По-приобщаващото Шенгенско пространство ще бъде едно по-силно и по-сигурно пространство.“

Илва Йохансон, комисар по въпросите на вътрешните работи: „Днешната стратегия за Шенгенското пространство ще ни направи по-силни, за да бъдем по-свободни в рамките на вътрешните си граници. Съвременните информационни системи ще подобрят управлението на външните граници, а засиленото полицейско сътрудничество и общото управление на миграцията ще спомогнат за укрепването на Шенгенското пространство без гранични проверки. Представената днес стратегия ще насърчи доверието и управлението, за да можем по-добре да предвиждаме и реагираме, и да сме по-добре подготвени, и съм решена да настоявам всички държави членки да дадат своя принос.“

Стратегията се стреми към:

- **Гарантиране на ефективно управление на външните граници на ЕС** чрез продължаващото изграждане на Постоянния корпус на европейската гранична и брегова охрана; постигането на оперативна съвместимост на информационните системи за управление на границите и миграцията до 2023 г.; както и предстоящо предложение за цифровизиране на заявленията за издаване на визи и документите за пътуване. Комисията също така призовава съзаконодателите бързо да приемат предложението за Нов пакт за миграцията и убежището във връзка с проверката на лицата, преминаващи границите без разрешение.

- **Укрепване на Шенгенското пространство във вътрешен план** под формата на тясно сътрудничество между държавите членки в областта на предотвратяването и борбата със заплахите

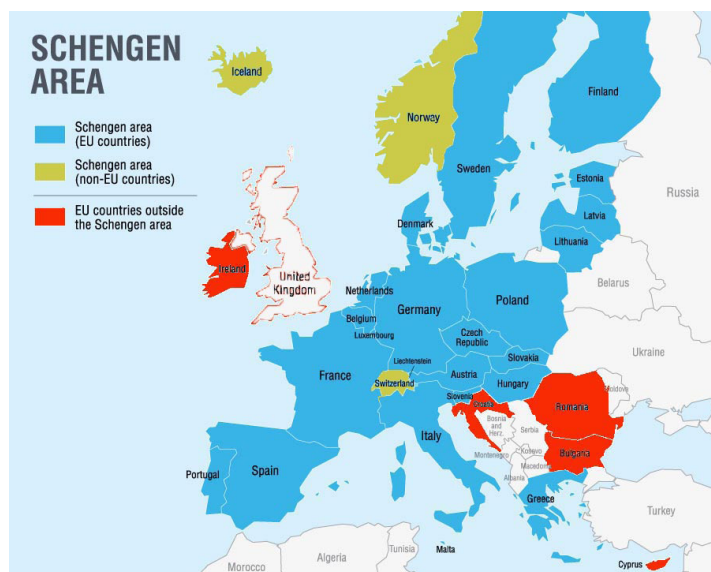
за сигурността е от решаващо значение, за да се поддържа и компенсира липсата на контрол по вътрешните граници. Новите инициативи ще включват кодекс на ЕС за полицейско сътрудничество; актуализиране на рамката от Прюм за обмен на информация относно ДНК, пръстови отпечатъци и регистрацията на превозни средства; и разширяване на използването на предварителна информация за пътниците за полети в рамките на Шенгенското пространство. След като бъде приет, Новият пакт за миграцията и убежището ще установи и общ подход към управлението на миграцията, който е важен елемент за доброто функциониране на Шенгенското пространство.

• **Повишаване на подготовката и подобряване на управлението:** Комисията предлага да се преразгледа механизмът за оценка и наблюдение по Шенген. Тя ще свиква и редовни Шенгенски форуми за насърчаване на политическия диалог за справяне с общите предизвикателства въз основа на годишни доклади за състоянието на Шенгенското пространство. По-късно тази година Комисията ще предложи да се преразгледа Кодексът на шенгенските граници, за да се повиши устойчивостта на Шенген на сериозни заплахи, като се гарантира тясно сътрудничество и се въведат необходимите предпазни мерки, така че повторното въвеждане на проверки по вътрешните граници да остане крайна мярка. Комисията ще представи също така план за действие при извънредни ситуации, който позволява повторното активиране на успешната система за „зелени ленти“ за непрекъснат превоз на товари в случай на бъдещи кризи. И накрая, Комисията ще започне диалог с държавите членки за справяне с дългосрочното повторно въвеждане на граничен контрол по вътрешните граници.

• **Разширяване на Шенгенското пространство:** Бъдещето на Шенген трябва да включва разширяването към държавите — членки на ЕС, които все още не са част от Шенгенското пространство. За държавите, които са оценени като готови за това, присъединяването към Шенгенското пространство е както оправдано правно очакване, така и правно задължение.

Относно преразглеждането на механизма за оценка и наблюдение по Шенген, промените включват ускоряване на процеса на оценка, както и ускорена процедура в случай на съществени пропуски, които като цяло биха могли да изложат Шенген на риск. Ще бъде поставен по-силен политически акцент върху оценките по Шенген, тъй като резултатите от тях ще бъдат включени в годишния доклад за състоянието на Шенгенското пространство и обсъдени с Европейския парламент и Съвета. Механизмът включва засилен мониторинг на зачитането на основните права.

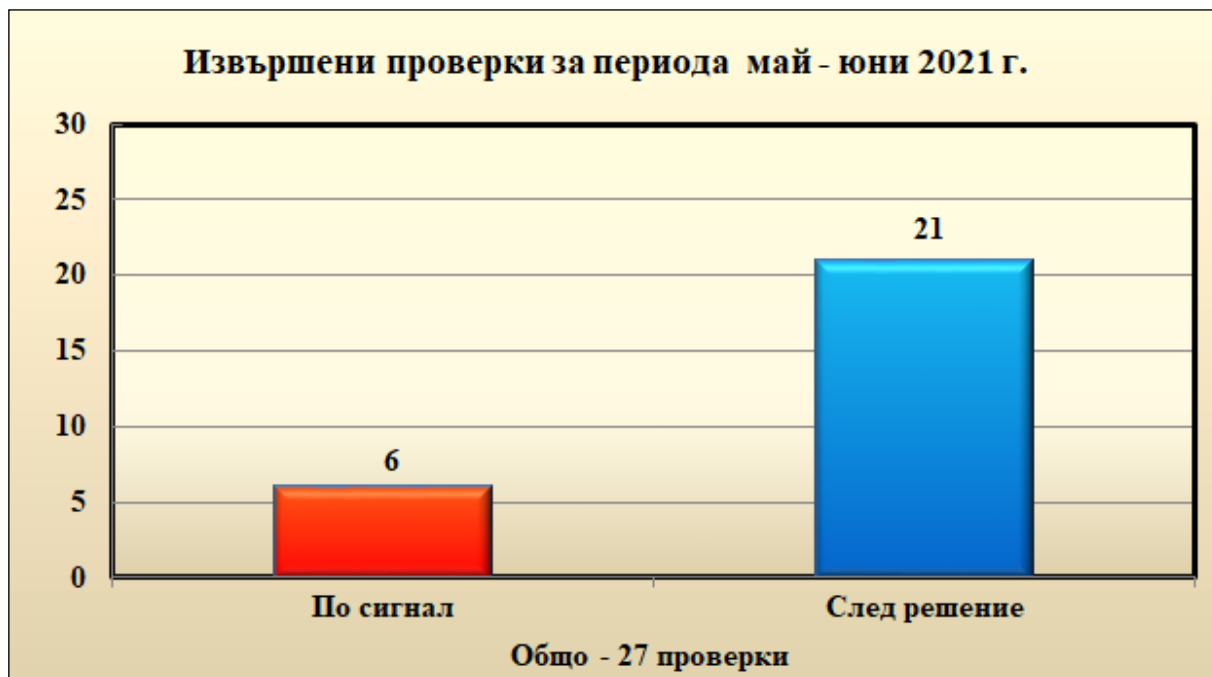
Също на 2 юни 2021 г., Европейската комисия публикува обширен **информационно-разяснителен материал под формата на въпроси и отговори със заглавие „Към по-силно и по-устойчиво Шенгенско пространство“**.



КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА МАЙ - ЮНИ 2021 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. през месеците май и юни 2021 г. са извършени общо 27 проверки – 6 след постъпили в КЗЛД сигнали и 21 след решение на КЗЛД.



Разгледани са 79 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

Във връзка с констатации, че с определени операции по обработване на лични данни са нарушени разпоредби на регламента, за отчетния период КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са издадени 7 Разпореждания и са отправени 2 Официални предупреждения.

РЕШЕНИЯ ПО ЖАЛБИ

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

РЕШЕНИЕ № ППН-01-1238/2019 София, 03.06.2021 г.

Комисията за защита на личните данни („Комисията”/„КЗЛД”) в състав: Председател – Венцислав Караджов и членове – Цанко Цолов и Мария Матева, на редовно заседание, проведено на 16.12.2020 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни във връзка с чл. 57, параграф 1, буква „е” от Регламент 2016/679 разгледа по основателност постъпила по компетентност от Апелативна прокуратура – София жалба № ППН-01-1238/12.08.2019 г., подадена от И.П. и С.П.

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

В приложената към постановлението на прокуратурата жалба се твърди, че незаконосъобразното обработване на лични данни в случая се изразява в извършване на справка в регистрите на МВР от служител на МВР чрез използване на служебно положение, с цел изясняване собствеността на лек автомобил, който се е намирал „паркиран повече от 2 години“ на улица в с. Б. без съгласието на лицата субекти на лични данни – жалбоподателките.

Твърди се, че след като е извършена справка от служителя на МВР, същият не просто е установил чия е собствеността на лекия автомобил, но е предприел и действия по свързване по телефон със собствениците на лекия автомобил (или е уведомил трето лице), с цел същият да бъде преместен от съответната улица, като в тези телефонни обаждания е било съобщено, че се разполага с информация за лични данни на жалбоподателките, а именно – телефонни номера, както и на лицето е било известно обстоятелството кога е починал бащата на жалбоподателките.

Жалбоподателките считат, че посоченото обработване на техни лични данни е в нарушение на Регламент 2016/679 и ЗЗЛД.

В условията на залегалото в административния процес служебно начало и в изпълнение на чл. 26 АПК, за започване на производството е уведомен министърът на вътрешните работи в качеството му на администратор на лични данни по смисъла на чл. 29, ал. 1 от Закона за МВР. Предоставена е възможността по чл. 34, ал. 3 АПК за изразяване на становище с относими доказателства по предявените в жалбата твърдения.

Пълномощникът на министъра на вътрешните работи заявява следното:

В справка, извършена по преписка № ****/19 г. на ГДНП, пр. пр. № *****/2018 г по описа на СРП, е посочено, че са снети обяснения от Р.А. – служител в 06 РУ-СДВР. По случая г-жа Р.А. е посочила, че от 2017 г. автомобилът „Хюндай“ е оставен пред къщата ѝ в с. Б. от лице със собствено име С., който е приятел на сина ѝ. През времето, в което въпросният автомобил е бил паркиран пред

къщата ѝ, никой не го е потърсил, нито въпросният С., нито други лица, в това число и собствениците на автомобила. Предвид дългия период от време, служителката се притеснила същият да не е предмет или средство на престъпление. Предвид това ѝ притеснение, г-жа Р.А. решила да провери кой е собственикът на автомобила и дали същият не е починал, след като никой не го е потърсил толкова дълго време, като е проверила дали автомобилът не се издирва. Р.А. сочи, че след като е установила, че автомобилът не се издирва, е помолила сина си да се уточни с неговия приятел и автомобилът да бъде преместен.

Снети са обяснения и от жалбоподателките. В писмени обяснения жалбоподателката И.П. заявила, че е предоставила наследствения си автомобил с марка „Хюндай“, на С. от с. Б., когото познавала от 9 години. Предоставила му също документи на колата и шофьорската си книжка.

Видно от справката, снети са обяснения и от В.П., който заявил, че след разговор с негов познат със собствено име С. се съгласил въпросният автомобил да бъде паркиран пред къщата на баба му и дядо му в с. Б.. Соочи, че С. му казал, че автомобилът му е оставен от една от жалбоподателките – И.П.. С. му споделил, че колата е наследствена собственост на две сестри. В справката е посочено, че в писмените си обяснения В.П. посочва, че е получил телефонния номер на сестрите от С., за да им каже да дойдат да си го приберат.

Представителят на министъра счита, че жалбата е неоснователна и недоказана по отношение на администратора на лични данни.

От снетите по случая обяснения става ясно, че служителката е направила справка относно автомобила, стоящ пред дома ѝ с оглед притеснението ѝ същият да не е обект на престъпление кражба или да не е послужил за извършване на престъпление. От нейните обяснения и тези на В.П. не може по никакъв начин да се направи предположение, че тя му е предоставила личните данни на трети лица, а именно на жалбоподателките. В.П. посочва, че е получил телефонен номер от своя приятел С., на когото едната жалбоподателка е предоставила сама автомобила си, ведно с личен документ за самоличност – свидетелство за управление на моторно превозно средство. В този документ, който жалбоподателката сама е предоставила на своя познат, фигурират нейни лични данни – имена, дата на раждане и ЕГН. Видно от нейните обяснения и от тези на В.П., въпросният С. е разполагал и с телефонния ѝ номер, както и с информация за това, че автомобилът е придобит от нея по наследство.

От извършената проверка по преписка ****/19 по описа на ГДНП, пр.пр. *****/2018 г. по описа СРП по никакъв начин не може да бъде направено обосновано предположение, че служителката на 06 РУ-СДВР е предоставила лични данни на двете жалбоподателки на сина си. Твърденията на жалбоподателките не се потвърждават от взетите сведения от Р.А. и от В.П..

В случая личните данни на жалбоподателките са обработени от физическо лице В.П. в хода на негови лични занимания. Този вид обработване е изключено от приложното поле на действие на Регламент (ЕС) 2016/679 (чл. 2 от Регламента).

Във връзка с твърдението, че материалите от извършената проверка са изпратени в СРП, от районната прокуратура са изискани документи от пр.пр. № *****/2018 г. по описа на СРП. В КЗЛД постъпили изисканите документи без справка от Дирекция „Компютърни информационни системи“ при МВР, поради факта, че е класифицирана информация по ЗЗКИ.

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

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

Жалбата е процесуално допустима – подадена в срока по §44, ал. 2 от ПЗР на ЗЗЛД от субекти на данни с правен интерес. Същата има за предмет твърдение за нарушаване на права по

Регламент 2016/679 или ЗЗЛД. С жалбата е сезиран компетентен да се произнесе орган – Комисията за защита на личните данни, която съгласно правомощията си по чл. 10, ал. 1 ЗЗЛД във връзка с чл. 57, параграф 1, буква „е“ от Регламент 2016/679 разглежда жалби, подадени от субекти на данни. Налице са предпоставките за допустимост и по чл. 27, ал. 2 от АПК.

На проведено на 09.09.2020 г. закрито заседание на Комисията жалбата е обявена за допустима и като страни в производството са конституирани: жалбоподатели И.П. и С.П., ответна страна – министъра на вътрешните работи. Страните са уведомени за насроченото за 28.10.2020 г. открито заседание за разглеждане на спора по същество.

Предвид направените доказателствени искания за разпит на свидетели, разглеждането по същество е отложено за 16.12.2020 г.

На проведеното на 16.12.2020 г. открито заседание страните се представляват от процесуални представители, които поддържат изложените по преписката становища. Като свидетели са разпитани Р.А. (вече С.) и В.П.. Свидетелските показания в съществената си част се припокриват с тези, дадени в хода на предварителната проверка в СРП.

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

От изложеното в жалбата и постановлението на прокуратурата се извеждат две твърдения за нарушаване правата на жалбоподателките. Първото се отнася за достъп до регистрите на МВР, извършен от служител на министерството, който е станал поради извънслужебна необходимост и не по регламентирания в ЗМВР ред. Второто твърдение е за неправомерно предоставяне на трето лице на така получената от регистрите информация.

Предвид факта, че от Софийска районна прокуратура не предоставиха справка от Дирекция „Компютърни информационни системи“ при МВР, поради защитата ѝ по Закона за защита на класифицираната информация, не може да се направи категоричен извод за датата на достъпване в регистрите на МВР. От обясненията на страните в хода на прокурорската проверка, от факта, че справка се отнася за периода 01.12.2017 г. – 30.06.2018 г., както и от дата на първата прокурорска проверка, се достига до извода, че достъпът е осъществен месец март-април 2018 г., т.е. по време на действието на Закона за защита на личните данни (приложима редакция ДВ, бр. 7 от 2018 г.) и преди да започне прилагането на Регламент 2016/679.

Видно от свидетелските показания, дадени в хода на прокурорската проверка, служителят на МВР Р.А. е проверила собствеността на автомобил в регистрите на МВР, което представлява обработване на лични данни.

Законът за защита на личните данни (ЗЗЛД) урежда защитата на правата на физическите лица при обработване на личните им данни. Целта на закона е гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните.

1. Относно първото твърдение за нарушение – неправомерен достъп до регистрите на МВР, следва да се разгледат разпоредбите на ЗМВР. Съгласно чл. 25, ал. 1 от ЗМВР **за изпълнение на дейностите си** органите на МВР могат да обработват лични данни. Следователно, органите на МВР могат да обработват лични данни на основание чл. 4, ал. 1, т. 6 от ЗЗЛД (прил. ред.) – обработването е необходимо за упражняване на официални правомощия, предоставени със закон на администратора.

За да бъде осъществена хипотезата на чл. 4, ал. 1, т. 6 от ЗЗЛД (прил. ред.) обаче, обработването следва да бъде за целите, посочени в чл. 25, ал. 1 от ЗМВР – за изпълнение на дейностите на МВР и по установения ред. Констатацията на Апелативна прокуратура – София, която се основава на снетите в хода на прокурорската преписка сведения от достъпилия регистър служител (потвърдени и пред КЗЛД), както и на представената справка от дирекция „Компютърни информационни системи“ при

МВР, е, че достъпът до системата на МВР е извършен поради извънслужебна необходимост, поради което е извън регламентирания в ЗМВР ред. Тази констатация се споделя и от КЗЛД.

Видно от представената справка за служителя на МВР, достъпил до личните данни, както и от свидетелските ѝ показания, служителят има достъп до регистрите за целите на изпълнение на служебните си задължения.

Предвид горното, макар по принцип органите на МВР да могат да обработват лични данни, в разглеждания случай обработването е извършено в нарушение на организационните мерки, произтичащи от чл. 25, ал. 1 от ЗМВР – обработването да е за изпълнение на дейностите на министерството. Това представлява нарушение на чл. 23, ал. 1 от ЗЗЛД (прил. ред.), съгласно който администраторът на лични данни предприема необходимите технически и организационни мерки, за да защити данните от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

2. Второто твърдение за нарушение е относно предоставяне на трето лице на достъпени от регистрите данни.

Безспорно е, че синът на служителя, достъпил до регистрите на МВР, е позвънил последователно на двете жалбоподателки относно автомобила им. Недоказано обаче остава твърдението, че данните са получени от служителя на МВР. Видно от събраните в хода на прокурорската проверка обяснения, жалбоподателките се познават с лицето С., на което са предоставили автомобила, заедно с документите му и шофьорската книжка на една от жалбоподателките, както и са осъществявали телефонни разговори с него. С. от своя страна се познава със сина на служителя на МВР, достъпил до регистрите, като последният посочва, че именно от С. има информация за имената, телефоните и факта на наследяване на автомобила.

Предвид горното, недоказано остава твърдението, че служител на МВР е разкрил на трето лице лични данни, придобити от регистрите на МВР, поради което в тази част жалбата е неоснователна.

Предвид посоченото в т. 1 и 2, жалбата е частично основателна.

Съгласно действалия към момента на извършване на нарушението чл. 38, ал. 2 от ЗЗЛД (прил. ред.), с решението си КЗЛД може да даде задължително предписание, да даде срок за отстраняване на нарушението или да наложи административно наказание. Административните наказания „имуществената санкция“ са посочени в чл. 42 от ЗЗЛД (прил. ред.).

Комисията действа в условията на оперативна самостоятелност като преценява кое от своите правомощия да реализира. Преценката се основава на съображенията за целенасоченост, целесъобразност и ефективност на решението, като следва да се постанови акт, който в най-пълна степен да защитава обществения интерес, при отчитане и на конкретните смекчаващи и отегчаващи отговорността обстоятелства.

Смекчаващо отговорността обстоятелство е, че достъпът до регистрите на МВР е извършен от служител на министерството, на когото е предоставен достъп за изпълнение на служебните му задължения, а не е осъществен от трето-неоторизирано лице. Не се установи така достъпените данни да са предоставени на трето лице. Предвид посочените смекчаващи обстоятелства, КЗЛД намира, че налагането на административно наказание „имуществена санкция“ на администратора би било непропорционално на извършеното нарушение.

Същевременно, нарушения като констатираното в настоящото производство е възможно да се повторят, предвид множеството регистри с лични данни, които поддържа администраторът и необходимостта за честото извършване на справки в тях. За да се намали възможността за извършване на подобни нарушения, КЗЛД намира, че следва да даде задължително предписание на администратора за извършване на обучения и осъществяване на контрол върху дейността на служителите с достъп до лични данни.

Администраторът на лични данни следва да въведе извършването на контрол чрез периодични случайни проверки (random-check) на логове (log files) дали осъществен оторизиран достъп (т.е. извършен от лица, които имат предоставен достъп до регистрите с лични данни) е нерегламентиран (т.е. не е за изпълнение на дейностите на органите на МВР по смисъла на чл. 25, ал. 1 от ЗМВР). В допълнение към това, администраторът следва да извършва обучение на длъжностните лица с достъп до регистрите на МВР относно правилата и процедурите за обработване на лични данни.

Така мотивирана и на основание чл. 38, ал. 2 от ЗЗЛД (прил. ред.), Комисията за защита на личните данни

РЕШИ:

1. Обявява жалба рег. № ППН-01-1238/12.08.2019 г., подадена от И.П. и С.П. срещу министъра на вътрешните работи, за основателна за нарушение на чл. 23, ал. 1 от ЗЗЛД (ДВ, бр. 81 от 2011 г.).

2. На основание чл. 38, ал. 2 от ЗЗЛД (ДВ, бр. 103 от 2005 г.) дава задължително предписание на администратора на лични данни – министъра на вътрешните работи:

а) Да въведе контрол за спазване на процедурите чрез извършване на периодични случайни проверки на логове, като се извършва анализ и оценка дали осъществения оторизиран достъп до регистрите с лични данни на МВР е регламентиран или е нерегламентиран;

б) Да извършва обучение на длъжностните лица с достъп до регистрите с лични данни на МВР относно правилата и процедурите за обработване на лични данни.

3. Обявява жалбата за неоснователна в останалата ѝ част.

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

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/



СТАНОВИЩА НА КЗЛД

СТАНОВИЩЕ НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ рег. № ПНМД-01-11/2021 г. гр. София, 17.06.2021 г.

ОТНОСНО: *Подписване на документи от администрацията с квалифициран електронен подпис и предоставянето им в електронна среда*

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 09.06.2021 г., разгледа искане за становище с вх. № ПНМД-01-11/2021 г. от Министерство на образованието и науката (МОН), с което се отправя въпрос, свързан с подписване на документи от служители в администрацията с квалифициран електронен подпис (КЕП) и предоставянето им в електронна среда за целите на документооборота.

От МОН информират, че съгласно изискванията на *Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги* (НОИИСРЕАУ) са длъжни да използват система за електронен документооборот и да участват в електронен обмен на документи с други администрации, недопускайки обмен на документи на хартиен носител, освен в случаите, когато това е определено със закон. В изпълнение на чл. 37 от НОИИСРЕАУ електронните документи се подписват с електронен подпис, издаден по реда на *Наредбата за удостоверенията за електронен подпис в администрациите*. Електронното подписване е установено и по отношение на резултата от предоставяните електронни административни услуги (чл. 9 НОИИСРЕАУ). В чл. 101, ал. 3 от *Наредбата за обмена на документи в администрацията* (НОДА) също е регламентирано изготвяните електронни документи да се подписват с електронен подпис.

В тази връзка е изложен и анализ, според който доставчиците на удостоверителни услуги, включват информация за ЕГН в квалифицираните удостоверения за квалифициран електронен подпис (КУКЕП). Изразяват се притеснения, че тази информация обаче е видима, както при квалифицираните удостоверения за квалифициран електронен подпис, които се издават на физическа лица (в лично качество), така и за КУКЕП, които се издават на физически лица, асоциирани с юридически лица (т.е. в служебно качество). Опасенията са свързани с обстоятелството, че при изпращане на подписан документ с електронен подпис, без да бъде променен неговият формат (например, чрез сканиране на документа или преобразуването му в друг формат), всички, които имат достъп до документа могат да получат както данни, необходими за валидиране на електронния подпис, срока на валидност и данни за администрацията (наименование/ЕИК/БУЛСТАТ), така и лични данни за лицето, подписало документа - три имена и ЕГН, както и електронен адрес, съдържащи се в електронния подпис.

Предвид гореизложеното, МОН счита, че за предоставянето на достъп до ЕГН на физически лица, действащи при осъществяване на служебните си задължения, не са налице нормативни основания, респ. липсва и съответствие с нормативните изисквания за защита на личните данни. Във връзка с това от МОН се обръщат към КЗЛД с молба за изразяване на становище по казуса.

По тези съображения и отчитайки надзорните правомощия на Комисията за регулиране на съобщенията (КРС) в областта на законодателството, уреждащо електронните удостоверителни услуги, от страна на КЗЛД е изпратено официално запитване с изх. № ПНМД-01-11#1/22.03.2021 г.

В него е поставен следният въпрос:

„Безспорно е, че ЕГН е необходим за издаването на КЕП (чл. 43 от Закона за електронния документ и електронните удостоверителни услуги), но има ли изрично нормативно изискване ЕГН на титуляря на КЕП да е видим при подписване на електронни документи за неограничен кръг от лица – получатели на въпросните документи?“

В отговор на поставения въпрос, със свое писмо с вх. № ПНМД-01-11#2/28.05.2021 г., КРС предоставя следната информация:

*„... съгласно действащата нормативна уредба в областта на електронните удостоверителни услуги **няма** предвидено такова нормативно изискване.“*

Правен анализ:

В разпоредбата на чл. 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (Обн. Л. ОВ. бр. 257 от 28 август 2014 г.) са посочени легалните дефиниции на понятията, свързани с разглеждания казус, както следва:

Съгласно т. 10) **„електронен подпис“** означава данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, и които титулярят на електронния подпис използва, за да се подписва;

Съгласно т. 11) **„усъвършенстван електронен подпис“** означава електронен подпис, който отговаря на изискванията, посочени в член 26;

Съгласно т. 12) **„квалифициран електронен подпис“** означава усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи;

Съгласно т. 13) **„данни за създаване на електронен подпис“** означава уникални данни, които се използват от титуляря на електронния подпис за създаването на електронен подпис;

Съгласно т. 14) **„удостоверение за електронен подпис“** означава електронен атестат, който свързва данните за валидиране на електронен подпис с физическо лице и потвърждава най-малко името или псевдонима на това лице;

Съгласно т. 15) **„квалифицирано удостоверение за електронен подпис“** означава удостоверение за електронни подписи, което се издава от доставчик на квалифицирани удостоверителни услуги и отговаря на изискванията, предвидени в приложение I;

Съгласно т. 16) **„удостоверителна услуга“** означава електронна услуга, обикновено предоставяна срещу възнаграждение, която се състои във:

а) създаването, проверката и валидирането на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; **или**

б) създаването, проверката и валидирането на удостоверения за автентичност на уебсайт; **или**

в) съхраняването на електронни подписи, печати или удостоверения, свързани с тези услуги.

Съгласно Приложение I на Регламент (ЕС) 910/2014 квалифицираните удостоверения за

електронни подписи следва да съдържат определен набор от данни по отношение на титулярите. Ключово обаче е разграничението между целите, за които се обработват тези данни – издаването и съответно ползването на електронния подпис.

По силата на чл. 24, пар. 1 от Регламент (ЕС) 910/2014 при издаването на квалифицирано удостоверение за удостоверителна услуга доставчикът на квалифицирани удостоверителни услуги проверява чрез подходящи средства и в съответствие с националното право самоличността и, ако е приложимо, всички специфични данни за физическото или юридическото лице, на което се издава квалифицираното удостоверение. Тази информацията се проверява от доставчика на квалифицирани удостоверителни услуги пряко или чрез трета страна в съответствие с националното право:

а) чрез личното присъствие на физическото лице или на упълномощен представител на юридическото лице; **или**

б) дистанционно, чрез средство за електронна идентификация, като за целта преди издаването на квалифицираното удостоверение е било осигурено физическото присъствие на физическото лице или на упълномощен представител на юридическото лице и въпросното средство отговоря на изискванията на член 8 по отношение на нивата на осигуреност „значително“ или „високо“; **или**

в) чрез удостоверение за квалифициран електронен подпис или за квалифициран електронен печат, издадено в съответствие с буква а) или б); **или**

г) чрез използване на други признати на национално равнище методи за идентификация, които дават ниво на осигуреност, равностойно на физическото присъствие по отношение на надеждността. Равностойното ниво на осигуреност се потвърждава от орган за оценяване на съответствието.

Посочената разпоредба задължава доставчика на удостоверителни услуги да идентифицира по безспорен начин титулярите на даден електронен подпис, като за целта се събират и обработват определен обем от лични данни. Несъмнено, един от начините за идентификация на субекта на данни е обработването на неговия ЕГН в съвкупност с други идентификационни данни. Това обаче, не означава, че ЕГН трябва да е видим при подписването на документи. Основната цел при използването на уредените с Регламент (ЕС) 910/2014 услуги е да се гарантира осигуряването на сигурна електронна идентификация и сигурно електронно удостоверяване на автентичност. С тези задължения са изрично натоварени доставчиците на електронни удостоверителни услуги и поради това не е налице нито необходимост, нито правно основание, ЕГН на титуляря да бъде видимо за неограничен кръг от лица – участници в обмена на електронни документи.

Разпоредбата на чл. 11 от Закона за гражданската регистрация (ЗГР) гласи, че ЕГН е административен идентификатор, чрез който физическите лица се определят еднозначно. В тази връзка, ЕГН може да бъде нормативно установен като реквизит, който напр. е част от заявление, което лицето подава по повод искане за инициране на административно производство или за предоставяне на услуга. В такива случаи целта и основанието за обработване на ЕГН са предвидени в нормативен акт и то е част от съдържанието на конкретен документ, а не на електронния подпис.

Нещо повече, съгласно чл. 25, пар. 2 от Регламент (ЕС) 910/2014 правната сила на квалифицирания електронен подпис е равностойна на тази на саморъчния подпис, за чиято валидност не се изисква добавяне на ЕГН.

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

СТАНОВИЩЕ:

1. Съгласно действащата нормативна уредба в областта на електронните удостоверителни услуги, липсва нормативно изискване и съответно правно основание, ЕГН на титуляря на КЕП да е видим при подписване на електронни документи.

2. Отчитайки посоченото в т. 1, Министерство на образованието и науката следва да се обърне към доставчика, предоставил съответните електронни удостоверителни услуги, с цел предприемане на действия по преустановяване на визуализацията на ЕГН на титуляря на КЕП при подписване на електронни документи от служители в неговата администрация.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

**Комисия за защита на личните данни**

Председател: Венцислав Караджов

Членове: Цанко Цолов

Мария Матева

Веселин Целков

Информационен бюлетин № 4 (91) 2021 г.

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

Уеб сайт на КЗЛД: www.cdpd.bg

Разпространява се в електронен вид

ISSN 2367-7759