КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

С Т А Н О В И Щ Е

НА

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

рег. № ПНМД-01-78/2022 г.

гр. София, 14.09.2022 г.

ОТНОСНО: *Достъп и предоставяне на данни, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи" и Единен регистър на чужденците*

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 07.09.2022 г. , разгледа искане с рег. № ПНМД-01-78/29.07.2022 г. от г-н Божидар Божанов – министър на електронното управление, който се обръща към КЗЛД с искане за изразяване на становище относно възможността Министерството на електронното управление (МЕУ) да получи достъп до данни, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи" и Единен регистър за чужденци, поддържани от Министерството на вътрешните работи, на основание чл. 70, ал. 1, т. 1 от Закона за българските лични документи (ЗБЛД) и чл. 6, пар. 1, б. „д", предложение второ от Регламент (ЕС) 2016/679 - упражняване на официални правомощия, които са предоставени на администратора по силата на чл. 7в, ал. 2 от Закона за електронното управление (ЗЕУ).

В искането е изложена следната фактическа обстановка:

С Решение № 133 от 10 март 2022 г. Министерският съвет е възложил на министъра на електронното управление да предприеме действия за изграждане на технологична възможност за електронна идентификация чрез мобилно устройство при предоставянето на електронни административни услуги, както и да предложи промени в свързаното законодателство в рамките на 2022 г.

В изпълнение на т. 1 от визираното решение МЕУ е изготвило техническа спецификация и на 21.04.2022 г. е сключило договор по реда на чл. 7с от ЗЕУ със системния интегратор - „Информационно обслужване” АД, който има за предмет изграждане на мобилно приложение за електронна идентификация и електронно подписване - BGID.

В техническата спецификация - приложение към договора и системния проект, изготвен от „Информационно обслужване” АД, е предвидено, като част от процеса на първоначална идентификация, потребителят да направи снимка на личния си документ. От тази снимка, чрез визуално изчитане на MRZ зоната (машинно четимата зона с данни в документите за самоличност), се извлича информация за документа - тип, номер, дата на валидност, имена на притежателя. В допълнение потребителят извършва статично заснемане на лицето си с фронталната камера на мобилното устройство (автопортрет или selfie), след което записва кратко видео с движения по инструкции с фронталната камера на мобилното устройство. С така направеното видео се удостоверява наличието на жив човек по време на първоначалната идентификация (liveness detection).

Дейностите по извличане на елементи от графична и видео информация се извършват в модула за визуална биометрична идентичност. В него ще бъде разработена следната функционалност:

• Декомпресиране на подаденото съдържание във вид, подходящ за последваща обработка;

• Извличане на информация от MRZ зоната на документа - за валидиране на данните на ниво мобилното устройство на потребителя;

• Биометрично сравнение на лицата от две статични изображения - автопортрет и снимка, извлечена от автоматизираната информационна система “Български документи за самоличност” (АИС „БДС”), както и софтуерно избран кадър от liveness detection видеото и снимка от АИС “БДС”.

В системния проект е предвидено още, че за реализацията на тази функционалност ще се използва предварително обучена невронна мрежа, която дава високо ниво на точността на разпознаване. За да се подобри обучението на невронната мрежа, е необходимо технологично да се извърши допълнително обучение/самообучение с наличните снимки в АИС “БДС” - локално в МВР, без тази информация да напуска мрежата на МВР, за което Изпълнителят ще предостави и необходимия високопроизводителен хардуер. Резултатите от самообучението и

тестовите сценарии, които ще бъдат разработени съвместно с МВР, ще останат изцяло в средата на МВР. В резултат, обучената невронна мрежа ще повиши процента на разпознаваемост, с което няма да се допускат опити за фалшифициране. Така създаденият модел, може да бъде използван и за други нужди в рамките на МВР.

В искането се посочва, че за целта е нужно предоставяне на достъп на експерти от МЕУ и „Информационно обслужване" АД до данни от базата данни от АИС „БДС", където МВР е първичен администратор на данните от българските лични документи по силата на чл. 2, ал. 2 от ЗЕУ във връзка със Закона за българските лични документи и като такъв за него възниква задължение да осигури достъп до тези данни автоматизирано и по електронен път като вътрешна електронна административна услуга (чл. 4, ал. 1 ЗЕУ във връзка с чл. 70, ал. 1, т. 1 от ЗБЛД).

За осъществяване на процеса по идентифициране на гражданите, които създават профил в BGID, *е необходимо МЕУ да достъпва данните, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи" и Единен регистър за чужденци.*

В искането са изложени мотиви, подкрепящи необходимостта от предоставяне на достъп, както следва:

Разглежданият в настоящото искане въпрос е свързан с предоставянето на данни, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи" и Единен регистър за чужденци при създаването на профил в мобилното приложение за електронна идентификация и електронно подписване - BGID.

Правомощията на министъра на електронното управление, в качеството му на административен орган, са уредени в ЗЕУ. В чл. 7в, ал. 1 от ЗЕУ е посочено, че министърът провежда държавната политика в областта на електронното управление и в областта на информационното общество и информационните технологии във взаимодействие с другите органи на изпълнителната власт. В допълнение, ал. 2 на цитираната разпоредба изрично предвижда, че *министърът на електронното управление провежда държавната политика и в областта на електронната идентификация.*

При реализиране на правомощията си в областта на електронната идентификация и в изпълнение на чл. 5, ал. 3 от ЗЕУ министърът на електронното управление е изградил и поддържа хоризонтална система за електронна автентикация, която служи за идентификация на всички участващи в електронното управление

субекти, обекти и информационни системи. Със системата следва да се интегрират средствата за електронна идентификация, посочени в чл. 5, ал. 2 от ЗЕУ, в т.ч. и цитираното мобилно приложение за електронна идентификация и електронно подписване - BGID, което към настоящия момент е в процес на разработване.

Както бе посочено по-горе, с решение на Министерския съвет № 133 от 22 март 2022 г. на министъра на електронното управление освен, че се възлага да създаде технологична възможност за електронна идентификация чрез мобилно устройство при предоставяне на публични услуги, му се вменява и да измени релевантното законодателство в рамките на 2022 г. - т. 2 от РМС. Основното законодателство в областта е Законът за електронната идентификация (ЗЕИ) и Правилника за прилагането му. В ЗЕИ ще бъдат подробно разписани правомощията на министъра на електронното управление в областта на електронната идентификация, както и основанието за достъп до регистри на МВР. Изменението и приемането на закона и правилника предполагат извършването на поредица от действия, регламентирани в Закона за нормативните актове, което във времеви аспект ще отнеме минимум 5 месеца и би имало за последица неизпълнение на т. 2 от РМС. Към настоящия момент се подготвя предварителна пълна оценка на въздействието на законопроекта.

Поради изложеното и с оглед своевременното изпълнение на РМС е изготвен проект на ЗИД на ЗЕУ. В чл. 5 от законопроекта е предвидено изрично, че министърът на електронното управление създава схема за електронна идентификация, която отговаря на ниво на осигуреност „високо" съгласно Регламент № 910/2014 г. Проектът е публикуван на 15.06.2022 г. за обществено обсъждане на Портала за обществени консултации.

Разгледаните по-горе правомощия на министъра на електронното управление в областта на електронната идентификация по своята същност са властнически правомощия, които са свързани с неговата компетентност в съответна сфера на обществени отношения. ЗЕУ няма за цел да урежда правила и да създава допълнителни основания за обработване на лични данни, тъй като същите са изчерпателно изредени в чл. 6, пар. 1 и чл. 9, пар. 2 от Регламент (ЕС) 2016/679.

От своя страна, ЗБЛД урежда условията и реда за издаване, ползване и съхраняване на българските лични документи. Той предвижда (чл. 70, ал.1, т. 1) данните от информационните фондове за българските лични документи с изключение на пръстовите отпечатъци, снети по реда на този закон, да се предоставят на държавни органи и организации съобразно законоустановените им правомощия. Такъв е и

разглежданият въпрос, състоящ се в предоставяне на данни от АИС „БДС” за целите на упражняването на властнически правомощия, възложени на министъра на електронното управление по силата на чл. 5 и чл. 7в, ал. 1 и 2 от ЗЕУ.

Осъществяването на действия по предоставяне на лични данни (вкл. чрез достъп), съставлява обработване на лични данни по смисъла на Регламент (ЕС) 2016/679 и същото следва да се извършва при спазване на условията за законосъобразност и принципите на обработване, уредени в чл. 5 от Регламента, така че обемът на данни да бъде изчерпателно определен, достатъчен и ненадхвърлящ целта, за която е необходим.

Тъй като в конкретния случай се касае за предоставяне на данни, събрани във връзка с издаването на български лични документи, предоставянето им следва да става и при отчитане изискванията на чл. 70 от ЗБЛД. чл. 70, ал. 1, т. 1 от цитирания закон предвижда, че данни се предоставят на държавни органи и организации съобразно законоустановените им правомощия.

В тази връзка е необходимо да се изясни как би следвало да се тълкува разпоредбата на чл. 70, ал. 1, т. 1 от ЗБЛД и по-специално терминът „законоустановено правомощие” на държавен орган.

Съгласно трайно установената практика на КЗЛД публичните органи притежават властнически правомощия, които са свързани с тяхната компетентност. В съществена част от случаите, упражняването на правомощия, респективно реализирането на компетентност, е свързано с достъп и обработване на лични данни, които се администрират от друг административен орган - първичен администратор на данни. Нещо повече, достъпът и обработването на лични данни в определени случаи е необходимо за упражняването на официални правомощия. Това означава, че реализирането на правомощията е пряко свързано с необходимостта за обработване на определен обем от лични данни - в противен случай може да се възпрепятства или да се стигне до невъзможност да се упражнят възложените от закон правомощия (арг. чл. 6, пар. 3 от Регламент (ЕС) 2016/679). В този смисъл, достъпът и обработването на лични данни не може само по себе си и самоцелно да е правомощие. То е необходим и съществен елемент от сложния фактически състав на упражняването на властническите правомощия.

В конкретния случай, за да се реализира и да функционира електронната идентификация чрез мобилното приложение, разработвано от МЕУ и по този начин министърът на електронното управление да осъществи властническите си правомощия,

предвидени в ЗЕУ, следва да се предостави достъп до данни, съдържащи се Национален автоматизиран информационен фонд „Национален регистър на българските лични документи” и Единен регистър за чужденци. Не би следвало да се изисква наличието на изрично разписано в нормативен акт задължение/право на достъп до данните от посочения регистър, тъй като подобен подход би разширил както основанията за обработване на лични данни по Регламент (ЕС) 2016/679, така и би бил в противоречие със специалния статут на публичните органи, предвиден чрез ясното разграничение на правните субекти по смисъла на чл. 70, ал.1, т. 1 от ЗБЛД. Въпреки това, МЕУ ще предложи в ЗЕИ изрично правно основание за достъп до Национален автоматизиран информационен фонд „Национален регистър на българските лични документи” и Единен регистър за чужденци.

Наред с посоченото, необходимо е да се има предвид и чл. 2, ал. 1 от ЗЕУ, съгласно който административните органи не могат да изискват от гражданите и организациите представянето или доказването на вече събрани или създадени данни, а са длъжни да ги съберат служебно от първичния администратор на данните. По силата на чл. 2, ал. 2 от ЗЕУ първичният администратор на данни е административен орган, който по силата на закон събира или създава данни за гражданин или организация за първи път и изменя или заличава тези данни (в случая това е МВР). Нещо повече, чл. 3 от ЗЕУ вменява на първичния администратор задължение да изпраща служебно и безплатно данните на всички административни органи, които въз основа на закон също обработват тези данни и са заявили желание да ги получават. Това задължение съответства и на функциите на информационните фондове, регламентирани с чл. 70 от ЗБЛД.

Въз основа на гореизложеното и с оглед спецификата на личните данни и особената закрила, която законодателството урежда по отношение на тях, от МЕУ молят КЗЛД да се произнесе със становище по следните въпроси:

- необходимо ли е в законодателството, и по-специално в ЗЕУ, да се съдържа изрична правна норма, уреждаща възможността да се предостави на МЕУ достъп до данни, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи” и Единен регистър за чужденци, поддържани от МВР, с цел идентифициране на гражданите, които създават профил в мобилното приложение за електронна идентификация и електронно подписване - BGID, администрирано от МЕУ;

- следва ли да се извърши от МЕУ и оценка на въздействието;
- необходимо ли е, ведно с посочените по-горе изисквания, да има и разрешение от КЗЛД, за да получи МЕУ достъп до данни, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи” и Единен регистър за чужденци.

Правен анализ:

Съгласно чл. 70 от Закона за българските лични документи (ЗБЛД) данните от информационните фондове за българските лични документи, с изключение на пръстовите отпечатъци, снети по реда на този закон се предоставят на:

1. държавни органи и организации съобразно законоустановените им правомощия, както и на лица, на които е възложено със закон да изпълняват държавни функции;

2. граждани, притежаващи български лични документи, само ако данните не засягат трети лица;

3. юридически лица на основата на закон или с акт на съдебната власт.

Данните се предоставят в срок до 14 дни от регистриране на искането или подаване на писменото заявление по ред, определен с акт на Министерския съвет.

Предоставянето на данни от информационните фондове за българските лични документи, с изключение на пръстовите отпечатъци, е уредено по аналогичен начин както предоставянето на данни от ЕСГРАОН по смисъла на чл. 106 от Закона за гражданската регистрация (ЗГР). И в двата случая данни се предоставят на държавни органи и организации съобразно законоустановените им правомощия. В този смисъл, мотивите за законосъобразното предоставяне на данните следва да са аналогични.

КЗЛД неведнъж се е произнасяла със становища по конкретни казуси[1], свързани с предоставянето на данни на държавни органи и организации съобразно законоустановените им правомощия.

Като централен едноличен орган на изпълнителната власт със специална компетентност, министърът на електронното управление попада в хипотезата на чл. 106, ал. 1, т. 2 от ЗГР, според която той има право да получи от ЕСГРАОН категориите и обема от данни, необходими за реализиране на неговите правомощия, свързани с провеждане на държавната политика в областта на електронната

[1] Становище на КЗЛД с рег. № ПНМД-01-64/2021 г. ; Становище на КЗЛД с рег. № ПНМД-01-87/2020 г. (публикувани на www.cpdp.bg в секция „Практика”)

идентификация. В допълнение, с Решение № 133/10.03.2022 г. Министерският съвет е възложил на министъра на електронното управление конкретна задача – да предприеме действия за изграждане на технологичната възможност за електронна идентификация чрез мобилно устройство при предоставяне на административни услуги. За тази цел възниква необходимост от достъп до данните, съдържащи се в Национален автоматизиран информационен фонд „Национален регистър на българските лични документи" и Единен регистър за чужденци, поддържани от МВР, с цел идентифициране на гражданите, които създават профил в мобилното приложение за електронна идентификация и електронно подписване – BGID, администрирано от МЕУ.

За предоставянето на данни в хипотезата на чл. 70, ал. 1, т. 1 от ЗБЛД могат да се подкрепят същите съображения, като тези за предоставянето на данни по чл. 106, ал. 1, т. 2 от ЗГР. Трябва да се има предвид, че и в двата случая постановяването на разрешение от КЗЛД е недопустимо.

При предоставянето на данните следва да се спазват принципите, прогласени в чл. 5 от Регламент (ЕС) 2016/679, като се отчита необходимостта и пропорционалността от обработването на определени категории данни при упражняването на правомощията и изпълнението на възложените конкретни задачи в рамките на тези правомощия.

В настоящия правен анализ заслужава да се акцентира и върху приложното поле на Закона за електронното управление (ЗЕУ), който урежда обществените отношения между административните органи, свързани с работата с електронни документи и предоставянето на административни услуги по електронен път, както и обмена на електронни документи между административните органи. Съгласно разпоредбите на ЗЕУ, административните органи не могат да изискват от гражданите и организациите представянето или доказването на вече събрани или създадени данни, а са длъжни да ги съберат служебно от първичния администратор на данните.

Съгласно чл. 35 от Регламент (ЕС) 2016/679 когато съществува вероятност определен вид обработване, по-специално **при което се използват нови технологии**, и **предвид естеството, обхвата, контекста и целите на обработването**, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да

бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

Основание за извършването на оценка на въздействието върху защитата на личните данни може да се търси и в *Списъка на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните съгласно чл. 35, пар. 4 от Регламент (ЕС) 2016/679*, публикуван на сайта на КЗЛД[2].

Извършването на оценката на въздействието върху защитата на личните данни може да се извърши като част от общата оценка на въздействието в контекста на приемането на нормативния акт за въвеждането в експлоатация на мобилното приложение за електронна идентификация и електронно подписване (арг. чл. 35, пар. 10 от Регламент (ЕС) 2016/679).

В допълнение следва да се отбележи, че приемливата оценка на въздействието върху защитата на личните данни по Регламент (ЕС) 2016/679 следва да съдържа:

- систематично описание на обработването (член 35, пар. 7, буква а)): взема се под внимание характерът, обхватът, контекстът и целите на обработката (съображение 90); личните данни, получателите и периодът, за който ще се съхраняват личните данни, се записват; функционално описание на операцията по обработване; идентифициране на активите, на които разчитат личните данни (хардуер, софтуер, мрежи, хора, хартия); отчита се евентуално спазването на одобрените кодекси за поведение (член 35, параграф 8);
- необходимост и пропорционалност на обработването (член 35, параграф 7, буква б)): определени са мерките, предвидени за спазване на регламента (член 35, параграф 7, буква г) и съображение 90, като се вземат предвид: мерките, допринасящи за пропорционалност и необходимост на обработването на базата на: конкретни, изрични и законни цели (член 5, параграф 1, буква б); законосъобразност на обработването (член 6); адекватни, уместни и ограничени до необходимите данни (член 5, параграф 1, буква в); ограничена продължителност на съхранение (член 5, параграф 1, буква д)); мерки, допринасящи за правата на субектите на данни: информация, предоставена на субекта на данни (членове 12, 13 и 14); право на достъп и преносимост (членове 15 и 20); право на поправяне, заличаване, възражение, ограничаване

[2] https://www.cpdp.bg/?p=element&aid=1186

на обработването (членове 16-19 и 21); получатели; обработващ (и) (член 28); гаранции, свързани с международния (те) трансфер (Глава V); предварително консултиране (член 36).

- управление на рисковете за правата и свободите на субектите на данни (член 35, параграф 7, буква в)): произходът, характерът, особеностите и тежестта на рисковете се оценяват (виж съображение 84) или по-конкретно за всеки риск (неправомерен достъп, нежелано изменение и изчезване на данни) от гледна точка на субектите на данни: вземат се предвид източниците на рискове (съображение 90); потенциалните въздействия върху правата и свободите на субектите на данни са идентифицирани в случай на незаконен достъп, нежелано изменение и изчезване на данни; заплахи, които могат да доведат до нелегален достъп, идентифициране на нежелани модификации и изчезване на данни; оценка на вероятността и тежестта (съображение 90); определят се мерките, предвидени за третиране на тези рискове (член 35, параграф 7, буква г) и съображение 90);
- участие на заинтересовани страни: консултация с длъжностното лице по защита на данните (член 35, параграф 2); иска се становището на субектите на данните или на техните представители (член 35, параграф 9).

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. Искането за достъп до информационните фондове на МВР е извън компетентността на КЗЛД. Компетентен да разгледа такова искане е министърът на вътрешните работи, като администратор на лични данни по чл. 29, ал. 1 от Закона за Министерството на вътрешните работи.

2. За осигуряването на достъп до данни в хипотезата на чл. 70, ал. 1, т. 1 от ЗБЛД не е необходимо постановяване на разрешение от КЗЛД, тъй като в този случай не е приложим разрешителен правен режим.

3. Независимо че на основание чл. 70, ал. 1, т. 1 от ЗБЛД във връзка с чл. 7в, ал. 2, т. 1, б. в) от ЗЕУ и Решение на МС № 133/10.03.2022 г. министърът на електронното управление може да иска достъп до данни, няма пречка специалното законодателство, уреждащо тези правоотношения, да включва изрична разпоредба в този смисъл. На основание чл. 51, ал. 1 от Закона за нормативните актове искане за тълкуване на законодателството, в случая е от компетентността на Народното събрание.

4. На основание чл. 35, пар. 10 от Регламент (ЕС) 2016/679 администраторът МЕУ следва да извърши оценка на въздействието върху защитата на личните данни, която е различна от оценката на въздействието на нормативните актове по смисъла на Закона за нормативните актове.

ПРЕДСЕДАТЕЛ:
Венцислав Караджов /п/

ЧЛЕНОВЕ:
Цанко Цолов /п/
Мария Матева /п/
Веселин Целков /п/