

ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ, КЕП И ЗАЩИТА НА ЛИЧНИ ДАННИ – ВЪЗМОЖНОСТИ ЗА ОПТИМИЗАЦИЯ

Доц. д-р Радан Мирянов
Икономически университет – Варна

ELECTRONIC IDENTIFICATION, QES AND GDPR – SOME OPPORTUNITIES FOR OPTIMIZATION

Assoc. Prof. Radan Miryanov, PhD
University of Economics – Varna

Резюме: Настоящият доклад има за цел да покаже, че в съвременния технологичен свят на свързани мрежи и процеси, на единна в повечето направления за целия Европейски съюз правна уредба включването и визуализацията на определени лични данни в КЕП на физическите лица в България е в противоречие с някои принципи за защита на личните данни и би могло да се оптимизира. В дигиталния свят, в който живеем, правата на гражданите за защита на личните им данни трябва да са с адекватни протекции, като ограничаването на правото за защитата им трябва да бъде надлежно предвидено в закон, да бъде пропорционално, съобразено с целите на ограничаването, но и със защитата на правата и свободите като цяло.

Ключови думи: *идентификация, електронен подпис, лични данни*

Abstract: This paper aims to show that in the modern technological world of interconnected networks and processes, of uniform legislation in most areas for the whole EU, the inclusion and visualization of certain personal data in QES of Bulgarian citizens is contrary to some principles of GDPR and could be optimized. In our digital world, civil rights concerning protection of our personal data must be adequately protected and any restrictions of this protection must be duly provided by law, be proportionate, consistent with the purposes of the restriction but with the protection of rights and freedom in general.

Key words: *identification, electronic signature, personal data*

Doi: <https://doi.org/10.36997/LBCS2021.341>

Въведение

Облачните услуги и идентификацията чрез биометрични данни набират все по-голяма скорост като решения за достъп до онлайн ус-

луги и сигурност на информацията. Биометричната идентификация чрез сензори, които идентифицират потребителите на мобилни устройства по техните пръстови отпечатащи или чрез лицево разпознаване, вече е утвърдена на пазара и може лесно да се превърне в нашата „лична карта“, с която да се идентифицираме във виртуалното пространство.

В същото време в България продължава да се изгражда национална схема за електронна идентификация, която трябва да даде на гражданите възможност за достъп до електронни услуги, но засега средствата, чрез които българските граждани и организации ще се идентифицират чрез нея, са неизвестни, а бизнесът буксува и не е в състояние да използва пълноценно трансграничните онлайн услуги.

Изложение

Трансграничният достъп до публични услуги е част от политиката на Европейския съюз. Затова Европейският парламент приема 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 (Регламент 910/14). Той урежда взаимното признаване на равнище ЕС на схемите за електронна идентификация, за които е извършено уведомяване и на свързаните с тях електронни удостоверителни услуги. Една от многото цели на приемането на Регламент 910/14 е например гражданин на една държава – членка на ЕС, да може да се запише по електронен път за студент в друга държава членка без електронният му подпис да бъде блокиран. Регламентът е задължителен в своята цялост и се прилага пряко във всички държави членки.

От 21.11.2016 г. е в сила Закон за електронната идентификация (ЗЕИ). ЗЕИ въвежда мерките по прилагане на Регламент (ЕС) №910/2014 и електронната идентификация получава своята национална уредба.

Чл. 3, параграф 1 от Регламент 910/14 определя електронната идентификация като процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице. ЗЕИ предвижда на физиче-

ските лица да се издава удостоверение за електронна идентичност.

До въвеждането на националната схема за електронна идентификация ДАЕУ (Държавна агенция „Електронно управление“) предвижда да се използват следните средства за идентификация – квалифициран електронен подпис, различни персонални кодове (ПИК на НАП и НОИ, УКД на НЗОК), потребителско име и парола.

Към м. октомври на настоящата 2021 г. национална схема за електронна идентификация все още не е изградена и въведена, а признатите средства за идентификация са „прекалено национални“, за да могат гражданите на ЕС да заявяват по електронен път административни услуги в България като използват средствата за електронна идентификация, издадени в собствената им държава, при условие че още на входа на Системата за сигурно електронно връчване (ССЕВ) ни посреща следната помощна информация: „При електронна автентикация с квалифициран електронен подпис е необходимо *същият да съдържа информация за ЕГН* на автора на подписа в полето *serial number = ЕГН*. В съответствие с §1, т. 22 от допълнителните разпоредби на Закона за електронното управление при условията на §5 от Наредбата за общите изисквания към инф. системи, регистрите и електронните адм. услуги“.

Параграф 1, т. 22 от ДР на ЗЕУ гласи, че по смисъла на ЗЕУ „уникален идентификатор“ е единният граждански номер на българските граждани, личният номер на чужденците, единният идентификационен код за търговците и клоновете на чуждестранните търговци и кодът по БУЛСТАТ за лицата, подлежащи на вписване в регистър БУЛСТАТ. Т.е. законодателят е поставил знак за равенство между понятията „уникален идентификатор“ по смисъла на ЗЕУ и ЕГН, а личен номер имат само чужденците, пребиваващи по-дълготрайно на територията на България. Следователно по силата на §1, т. 22 от ДР на ЗЕУ само дълготрайно пребиваващи на територията на държавата чужденци могат да се ползват от услугите, предоставяни от ДАЕУ. Буди недоумение и фактът, че словосъчетанието „уникален идентификатор“ е използвано единствено в чл.13, ал.1, т.6 от ЗЕУ, като то касае информацията, която доставчиците на електронни административни услуги предоставят на получателите на услуги.

Параграф 1, т. 22 от ДР на ЗЕУ дефинира понятие, използвано в чл.13, ал.1, т.6 от ЗЕУ, което касае уникалния идентификатор на доставчиците на електронни административни услуги и не може да

бъде годно правно основание за вписване на ЕГН в КЕП и задължително условие за достъп до национална система за административни услуги.

Изискването за вход в ССЕС с КЕП, съдържащ ЕГН на автора на подписа, е при условията на §5 от Наредбата за общите изисквания към инф. системи, регистрите и електронните адм. услуги.

Параграф 5, ал.1 от наредбата определя, че „В срок от една година след въвеждането в продукционен режим на националната схема за електронна идентификация по Закона за електронната идентификация за идентификация на физически лица, освен по реда на Закона за електронната идентификация и чрез други методи, определени със закон, може да се прилага и прочитане на уникален идентификатор от квалифициран електронен подпис“.

Текстът на §5, ал.1 от наредбата според мен е неприложим, защото той се отнася за период след въвеждането в продукционен режим на националната схема за електронна идентификация по ЗЕИ.

Затова смятам, че условието за достъп на лицата до електронни административни услуги с КЕП не се опира на валидни и/или относими правни норми.

Доколкото Регламент 910/14 приравнява КЕП на саморъчния подпис, а саморъчният подпис не е средство за идентификация и когато подписваме документ на хартиен носител не полагаме до подписа си данни за ЕГН и други лични данни, буди недоумение на какво правно основание доставчици на електронни удостоверителни услуги издават квалифицирани удостоверения за електронен подпис с вписани данни за ЕГН, при условие че нито вече коментираните §1, т. 22 от ДР на ЗЕУ и §5 от наредбата, нито липсата на национална схема за електронна идентификация към момента биха могли да бъдат законово основание. Считам, че правно основание за тези действия липсва в цялата национална уредба (Стаматова 2018).

С ПРИЛОЖЕНИЕ I на регламент 910/14 е определено, че КУ за КЕП съдържат най-малко името на титуляря или псевдоним и ако се използва псевдоним, той се посочва ясно, а в буква „е“ на приложението е регламентирано изискването за идентификационен код на удостоверението, който е уникален за доставчика на квалифицирани удостоверителни услуги.

Регламентът определя изискване за уникален идентификационен код на удостоверението, а не на лицето и допуска само името

или псевдонима да фигурират в съдържанието на квалифицираните удостоверения за електронни подписи, което означава, че със сигурна технология за създаване на КЕП може да се създаде подпис с правна признатост и без да съдържа в удостоверението прекомерно количество лични данни, както е случаят с издаваните удостоверения от доставчиците на квалифицирани електронни услуги у нас (Димитров 2018).

Считам, че доставчикът на квалифицирани удостоверителни услуги, при наличие на правно основание, е отговорен за идентификацията на физическите лица (Кръстева 2018). В противен случай значителен брой разпоредби, свързани със събирането и обработването на лични данни от доставчиците, биха били ненужни и незаконосъобразни.

Съгласно чл. 4, параграф 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (GDPR), „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор, като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социалната идентичност на това физическо лице.

Параграф 2 на чл.4 определя обработването на личните данни, а в параграф 11 е казано, че „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени“.

Чл.8 от Хартата на основните права на Европейския съюз определя, че *личните данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание.*

Личните данни, вписани в удостоверението за КЕП на физическите лица в България, са три имена, ЕГН, имейл адрес. Удостоверението има свой уникален номер, съдържа набор от данни за издателя на удостоверението и данни за валидирането на удостоверението.

В свое СТАНОВИЩЕ с рег. № ПНМД-01-11/2021 г., публикувано на адрес https://www.cpdp.bg/?p=element_view&aid=2282, Комисията за защита на личните данни (КЗЛД) по искане на МОН счита, че 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.*

Съгласието е едно от основанията за събиране и обработване на лични данни. В действителност има ситуации, при които администраторът на лични данни – например в сферата на здравеопазване, образование, не следва да иска съгласие. Съгласие не е необходимо и когато данните се събират във връзка с предоставянето на различни административни услуги от държавни органи или органи на местното самоуправление, когато се събират и обработват за целите на трудовите правоотношения и други случаи (Андреева и др. 2020).

КЕП обаче се използва не само при обмен на документи с държавната администрация. Има случаи, в които се налага и при отношения с трети страни – като например сключване на договор за изработка на мебели за дома или за доставка на обзавеждане и много други.

Според чл. 6, параграф 1 GDPR „Обработването е законосъобразно само ако и доколкото е приложимо“ при изпълнението на договор, по който субектът на данните е страна. Не случайно регламентът казва „само и доколкото е приложимо“. Ако гражданин има сключен онлайн и подписан двустранно с КЕП договор за доставка и монтаж на душ кабина в дома му, то тогава той няма как да не е посочил имената и домашния си адрес – в противен случай доставката и монтажът няма как да бъдат извършени. КЕП съдържа данни за имената му, които съвпадат с посочените в документа, съдържа имейл адреса, от който е изпратил подписания договор, но проблемът е, че съдържа и данни за единния му граждански номер.

Въпросът е: не може ли услугата да бъде извършена и договорът да бъде изпълнен без да се обработват данните за неговото ЕГН и доколко изпълнението или неизпълнението на услугата е зависимо

от обработката на тази категория данни. Как може гражданинът да е сигурен, че обработването на личните му данни е в изпълнение само на договора, при условие че при сключването му изискуемите лични данни, определени от доставчика, не са съдържали изискване за предоставяне на ЕГН и съгласието му за обработка е само върху исканите данни, но не и върху принудително предоставените от самия него данни за ЕГН, съдържащи се в КЕП. Даже планираното обработване на личните му данни да не надхвърля това, което е обективно необходимо за изпълнение на договора и администраторът да е съобщил за операциите с тях при започване на обработването в съответствие със задълженията за справедливост и прозрачност на GDPR, който носи отговорност при незаконосъобразна обработка на данни, предоставени „доброволно“ след даването на съгласие за обработка, които по никакъв начин не подпомагат предоставянето на договорената услуга (Петрова 2018).

Не ми е известно дали доставчиците на електронни удостоверителни услуги са убедени, че действат в съответствие с принципите за защита на данните, посочени в член 5, както и с всички други изисквания на GDPR, но когато интернет потребител въведе свой собствен ЕГН в търсачката на Google, нерядко списъкът с резултатите съдържа линкове към страници, съдържащи информация и за други лични данни, като номер на лична карта или паспорт.

Пример за предоставянето на прекомерно количество лични данни (и то на неограничен брой лица) е, ако заповед на ректора на ИУ, съставена като електронен документ, подписан с КЕП, бъде публикувана на сайта на университета. Тогава ще се визуализира ЕГН на ректора, като информацията може да бъде достъпена без ограничения от огромен брой потребители. В този и в много други подобни случаи, според мен, бихме могли да говорим за обработка на лични данни, за която няма съгласие, не е свързана с изпълнение на договор, не е законово задължение, не защитава жизненоважни интереси, не е в обществен интерес нито в изпълнение на официални правомощия и не защитава легитимните интереси на администратора.

Заклучение

След всичко казано дотук считам за обективна необходимост доставчиците на електронни удостоверителни услуги да премахнат

възможно най-бързо данните за ЕГН от удостоверенията за КЕП, а ДАЕУ да помисли за създаването на такъв вид достъп до ССЕВ с КЕП, при който например чрез посочения в КЕП имейл да се осъществява обратна връзка с желаещото да достъпи портала лице и при необходимост от него да се иска потвърждение за неговия ЕГН. Като още по-сигурен и безпроблемен начин намирам публичният орган, предоставящ административни услуги, виждайки данните за уникалния номер на удостоверението за КЕП, да отправя по електронен път искане до доставчика на квалифицирани електронни услуги с цел идентификация на лицето, поискала предоставянето на определена услуга.

По данни на електронните медии на 25.08.2021 г. служебното правителство е приело решение за уведомяване на Европейската комисия за частни схеми за електронна идентификация, които дават възможност на гражданите и бизнеса да се ползват от възможността за достъп до електронни услуги на държавите – членки на ЕС. Частните схеми за електронна идентификация са добра възможност за отдалечено установяване на идентичност и проверка на самоличност на физически и юридически лица, въз основа на което те да получат също така отдалечено желаните публични услуги. Изградените схеми за електронна идентификация са свързани с издаването на облачен КЕП, който, от една страна, има правната сила на саморъчно положен подпис, от друга страна, лицето, което иска достъп до определена услуга, се разпознава от разстояние и не на последно място – облачният КЕП не съдържа данни за ЕГН, освен ако притежателят му изрично не поиска визуализация на своето ЕГН в удостоверението за КЕП.

Засега съществува нормативна уредба относно установяването на държавна схема за електронна идентификация, а за възможността за идентифициране на гражданите и организациите с частни средства за идентификация уредба почти липсва.

Считам, че в България следва да се установят и използват частни схеми за сигурна електронна идентификация, като за целта се създаде ясна нормативна база, отчитаща уредбата на Регламент 910/14, на GDPR и другите относими нормативни актове.

Използвана литература

1. Андреева, А. и др. (2020). За свободата и дисциплината в трудовото право – съвременни аспекти в дигиталната ера. // Бизнес и право (Business and Law), №3, с. 55-75.
2. Димитров, П. (2018). Методологични проблеми при използване на квалифициран електронен подпис и универсалната двуфакторна автентикация в уеб приложения. // Известия на Съюза на учените – Варна. Серия Икономически науки, №3, с. 287-293.
3. Кръстева, Д. (2018). Задължения на обработващите лични данни съгласно изискванията на GDPR. // Труд и право: Месечен дайджест за трудови и осигурителни отношения, №4, с. 52-58.
4. Петрова, Д. (2018). Изследване развитието на електронното правителство в Република България и оценка на тенденциите за използване на електронни административни услуги от гражданите. // Eastern Academic Journal, Vol. 2, July, pp. 39-49.
5. Стаматова, В. (2018). Личните данни и защитата им по GDPR. //CIO: Chief Information Officer, №1, pp. 54-61.

За контакти: доц. д-р Радан Мирянов
Икономически университет – Варна
miryanov@ue-varna.bg