

**ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ И ЕЛЕКТРОННИ
УДОСТОВЕРИТЕЛНИ УСЛУГИ****проф. д-р Георги Георгиев Димитров
Свилена Ракшиева***Университет по библиотекознание и информационни технологии***ELECTRONIC IDENTIFICATION AND ELECTRONIC TRUST
SERVICES****Prof. George Dimitrov, PhD
Svilena Rakshieva**

Abstract: *With the adoption of Regulation (EU) No. 910/2014 the electronic identification and the electronic trust services become particularly important to the digital document turnover at both national and European level by receiving a key role in the built-up of trust in the electronic environment and in the opportunities it offers. The new European legal framework, directly applicable to the national legislation, is expected to significantly boost the electronic identification and the electronic trust services, as a result of which these tools will substantially contribute to the increase of the transparency, the neutrality and thus of the effectiveness of electronic transactions.*

Key words: *Electronic identification, electronic trust services, Regulation No. 910/2014, electronic transactions*

Регламент № 910/2014 [1], целящ повишаване на доверието и удобството в трансграничните електронни трансакции в държавите-членки на ЕС, представлява забележителен елемент в законодателния арсенал на ЕС по отношение на цифровия единен пазар, доколкото изграждането на доверие в онлайн средата в днешно време играе изключително важна роля в икономическото и социално развитие. Регламентът е забележителна крачка напред към създаването на обща рамка за сигурни електронни взаимоотношения между гражданите, бизнеса и държавните органи.

Приемането на Регламент № 910/2014 е резултат от острата нужда от укрепване на развитието на цифровия пазар на ЕС чрез въвеждане на съгласувана и всеобхватна правна рамка, която да подсили най-новите постижения в областта, като в същото време отстрани установените недостатъци.

I. НЕДОСТАТЪЦИ И НЕОБХОДИМОСТ ОТ РЕФОРМА

Редица проблеми, предизвикващи свиване на европейската цифрова икономика и спиращи нейния растеж, бяха широко дискутирани и потвърдени няколкократно от органите на ЕС. В съобщението на Комисията от 26 август 2010 г., озаглавено „Програма в областта на цифровите технологии за Европа” [2] беше отбелязано, че разпокъсаността на цифровия пазар, липсата на оперативна съвместимост и растящата киберпрестъпност представляват основни пречки за растежа на цифровата икономика и следователно е нужно да бъдат преодолени. В друг свой документ от 2010 г. -

Доклада за гражданството на ЕС, озаглавен „Премахване на пречките за упражняване на правата на гражданите на ЕС” [3], Комисията изтъква необходимостта да се преодолеят основните трудности, които възпрепятстват гражданите на Съюза да се възползват от предимствата на цифровия единен пазар и предлаганите на него трансгранични цифрови услуги. В допълнение, в свое съобщение за медиите, озаглавено „Списък със задачи в областта на цифровите технологии: нови приоритети за периода 2013-2014 г.” [4], публикувано на 18 декември 2012 г., Комисията подчертава факта, че „цифровата икономика се разраства седем пъти по-бързо в сравнение с останалите икономически отрасли, но понастоящем потенциалът ѝ не може да се разгърне поради нехомогенната общоевропейска рамка на политиките”. Друг установен проблем е обстоятелството, че Директивата за електронните подписи [5] обхваща електронните подписи, „но не предоставя цялостна трансгранична и междусекторна рамка за сигурни, надеждни и лесни за използване електронни трансакции” [6]. Както заглавието подсказва, Директивата за електронните подписи покрива единствено областта на електронните подписи и не съдържа допълнителни правила относно други удостоверителни услуги, които днес се считат за важни за създаването на доверие и сигурност на Европейския цифров единен пазар.

II. ПРЕДИЗВИКАТЕЛСТВОТО

Всички тези недостатъци представляват сериозно предизвикателство пред Европейската комисия, която през 2011 г. беше приканена от Съвета [7] да допринесе към цифровия единен пазар чрез създаване на подходящи условия за взаимно трансгранично признаване на ключови фактори като електронната идентификация, електронните документи, електронните подписи и услугите по електронно доставяне.

По средата между влизането на в сила на Регламента (което се случи на 17 септември 2014 г.) и деня, когато повечето от разпоредбите на Регламента ще започнат да се прилагат (1 юли 2016 г.) може да се каже, че предизвикателството е било прието с радост и скоро ще бъде преодоляно.

Регламент № 910/2014 представлява ясен и изчерпателен инструментариум за създаване на механизми и правила за надеждни и сигурни електронни трансакции. Регламентът се изправя пред предизвикателствата към международните трансакции и тяхната правна рамка, породени от развитието на новите технологии. Така Регламентът с готовност обхваща въпроси, които никога преди не са били регулирани на ниво ЕС.

III. МЕТОДОЛОГИЧЕН ПОДХОД И ПОДОБРЕНИЯ

Една от основните цели на Регламент № 910/2014 е да се премахнат съществуващите бариери пред трансграничната употреба на широко използваните в отделните държави-членки средства за електронна идентификация, доколкото тези бариери пречат на гражданите на ЕС да използват своите средства за удостоверяване на идентичността си в друга държава-членка и не позволяват на доставчиците на услуги да се възползват в пълна степен от преимуществата на вътрешния пазар. Регламентът разглежда-да и липсата на взаимно признаване между държавите членки в ЕС на схемите за електронна идентификация, използвани на национално равнище, чрез прилагане на рационален и добре премерен подход.

1. ПРИЛОЖНО ПОЛЕ НА РЕГЛАМЕНТА

На първо място, приложното поле на Регламента е внимателно ограничено. За целите на трансграничната употреба на средствата за електронна идентификация

Регламентът обхваща само обществени услуги. На частния сектор е предоставена пълна автономия. Независимо от това, частният сектор бива активно насърчаван да ползва, на доброволна основа, средствата за електронна идентификация в рамките на схема за идентификация, за която е извършено уведомяване, когато възникне такава нужда за онлайн услуги или електронни трансакции.

2. НЕЗАВИСИМОСТ ЗА ДЪРЖАВИТЕ-ЧЛЕНКИ

На второ място, на държавите членки е дадена голяма степен на независимост. Те запазват правото си да използват или въвеждат средства за електронната идентификация за целите на достъпа до онлайн услуги. Държавите членки също така могат да решават дали да уведомяват Европейската комисия за всички или за някои от използваните на национално равнище схеми за електронна идентификация за достъп до обществени онлайн услуги. С Регламента не се цели намеса по отношение на системите за управление на електронната самоличност и свързаните с тях инфраструктури, установени в държавите-членки. Целта на Регламента е да се гарантира, че е възможно да се осъществява сигурна електронна идентификация и сигурно електронно удостоверяване на автентичност.

3. ДОКУМЕНТ, БАЗИРАН НА ПРИНЦИПИ

На последно, но най-важно място, Регламентът се основава не на строги нормативни правила, а на набор от принципи. Подобна гъвкавост придава допълнителна стойност на механизмите, въведени с Регламента. Той е обвързан с принципа на технологична неутралност, което означава, че Регламентът не въвежда изисквания, които могат да бъдат изпълнени единствено от определена привилегирана технология. Тъкмо обратното – правната сила на Регламента може да бъде постигната чрез каквито и да е технически средства, които удовлетворяват изискванията, въведени от него. Регламент № 910/2014 възприема подход, който е открит към иновациите и предвижда актуална нормативна рамка, съответстваща на непрекъснато растящите темпове на развитие на технологиите. Друг принцип, залегнал в Регламента е, че методите за сертифициране на сигурността на информационните технологии са базирани на международни стандарти. Внимателно е предвидена и евентуална бъдеща поява на иновативни решения и услуги, за които все още може да не са налице стандарти за сигурност. В подобни случаи документът предвижда използване на алтернативни процеси, съпоставими със съществуващите стандарти.

Независимо от гореспоменатите уточнения, Регламент № 910/2014 по същество прокарва два правни механизма – въвежда принципа за взаимно признаване на средствата за електронна идентификация на държавите-членки и създава обща правна рамка за използването на удостоверителните услуги.

IV. ВЗАИМНО ПРИЗНАВАНЕ НА СРЕДСТВАТА ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ

1. НОВОВЪВЕДЕНИЯ НА РЕГЛАМЕНТ № 910/2014

Взаимното признаване на средствата за електронна идентификация, въведено с Регламента, се откроява като принцип от първостепенно значение. Той обосновава основната цел на Регламент № 910/2014, а именно идеята за въвеждане на механизъм, гарантиращ, че гражданите и предприятията могат да използват своите средства за електронна идентификация за достъп до, най-малко, обществените услуги в целия ЕС. Съгласно този принцип държавите-членки следва взаимно да признават средствата за електронна идентификация [8] издадени в рамките на схема за идентификация [9], за която е извършено уведомяване. Механизмът ще се прилага в случаите, когато

националното право или административната практика изискват електронна идентификация чрез средства за електронна идентификация и удостоверяване на автентичност за достъп до дадена услуга, предоставяна онлайн от орган от публичния сектор. Веднага щом е извършено доброволно уведомяване относно схема за електронна идентификация, взаимното признаване става задължително при условие, че са изпълнени условията, определени в Регламент № 910/2014.

Принципът на взаимното признаване е изграден на основата на няколко елемента, целящи създаване на доверие между държавите членки и гарантиране на успешното прилагане на неговите механизми.

А. Необходимост от уведомяване на Европейската комисия

На първо място, за да може едно средство за електронна идентификация на дадена държава-членка да бъде признато от другите държави-членки, то трябва да бъде издаден в рамките на схема за идентификация, за която е извършено уведомяване до Европейската комисия и което е било публикувано в Официалния вестник на ЕС.

Б. Ниво на осигуреност

Друг важен елемент е нивото на осигуреност на средствата за електронна идентификация. Както е посочено в съображенията на Регламент № 910/2014, нивата на осигуреност следва да характеризират степента на надеждност на средството за електронна идентификация при установяване на самоличността на дадено лице. Нивото на осигуреност зависи от степента на надеждност, което средството за електронна идентификация предоставя по отношение на самоличността на дадено лице, и се основава на процеси, управленски дейности и извършвани технически проверки. Според тези критерии, нивото на осигуреност би могло да се категоризира като „ниско“, „значително“ и „високо“. За целите на взаимното признаване, средството за електронна идентификация, издадено от една държава-членка, трябва да съответства на ниво на осигуреност, равно или по-високо от нивото на осигуреност, изисквано от съответния орган от публичния сектор за онлайн достъп до услуга в друга държава-членка, при условие че нивото на осигуреност на тези средства за електронна идентификация съответства на ниво на осигуреност „значително“ [10] или „високо“ [11]. Взаимното признаване на схеми за електронна идентификация, чието ниво на осигуреност е „ниско“ [12], е доброволно. В допълнение, съответният орган от публичния сектор трябва да прилага ниво на осигуреност „значително“ или „високо“ по отношение на достъпа до тази онлайн услуга.

В. Техническо сътрудничество и оперативна съвместимост

Техническото сътрудничество и оперативната съвместимост са друг важен елемент, въз основа на който е изграден принципът за взаимно признаване. Държавите-членки си сътрудничат по отношение на сигурността на схемите за електронна идентификация и гарантират, че електронните схеми за идентификация, за които е извършено уведомяване на Комисията, са оперативно съвместими. За целите на оперативната съвместимост, Регламентът установява рамка за оперативна съвместимост, състояща се от задаване на минимални технически изисквания във връзка с нивата на осигуреност, категоризиране на националните нива на осигуреност, задаване на минимални технически изисквания за оперативна съвместимост, както и минимален набор от данни за идентификация, механизми за уреждане на спорове и общи оперативни стандарти за сигурност. Рамката за оперативна съвместимост следва да се придържа към принципа за технологична неутралност, да спазва европейските и междуна-

родните стандарти, да улеснява спазването на принципа за защита на личния живот и да гарантира, че личните данни се обработват законосъобразно.

Г. Необходимост от предоставяне на възможност за трансгранично онлайн удостоверяване на автентичност

Взаимното признаване на средствата за електронна идентификация означава също, че държавите-членки предоставят възможност за трансгранично онлайн удостоверяване на автентичност. Тази възможност следва да се предоставя безплатно, когато се извършва във връзка с онлайн услуга, предоставяна от орган от публичния сектор. По отношение на субекти, които не са органи от публичния сектор, държавите-членки, могат, по своя преценка, да определят условия за достъп до онлайн автентикация, при условие че тези условия не са непропорционални и дискриминационни към лица, установени в друга държава-членка.

Д. Отговорност

Регламентът въвежда и набор от правила относно отговорността. Включена е отговорността на държавите-членки (за щети, причинени на физическо или юридическо лице поради неспазване на изискванията, свързани с данни за идентификация на лица), на издателя на средството за електронна идентификация (за щети, причинени на физическо или юридическо лице поради неспособност средството за електронна идентификация да се припише на правилното лице), на страната, извършваща процедурата по удостоверяване на автентичността (за щети, причинени на физическо или юридическо лице поради неспособност да се гарантира правилното функциониране на удостоверяването на автентичност).

2. НОВОВЪВЕДЕНИЯ В БЪЛГАРСКАТА ПРАВНАТА РАМКА

В резултат на подема, който се наблюдава в рамките на ЕС, и българското законодателство предприема първи стъпки към по-богата уредба по въпроса за електронната идентификация. Именно в тази насока на второ четене е приет Законопроект за електронната идентификация, който има за основна цел да създаде инструмент за включването на България в един дългосрочен управленски модел за оперативна съвместима платформа за обществените услуги в Европа.

В самия законопроект следва да се обърне внимание на няколко базови момента, които ще поставят основата за развитието на обществените отношения, свързани с електронната идентификация за в бъдеще.

Основна роля при настоящото инкорпориране на новият европейски модел за идентификация играят министърът на вътрешните работи, министърът на транспорта, информационните технологии и съобщенията, както и създаваните от тях контролни и административни органи. За български граждани, които пребивават в чужбина, е предвидено тази дейност да бъде подпомагана от дипломатическите и консулските представителства на Република България.

На българските граждани и на чужденците, притежаващи ЕГН или съответно ЛНЧ и навършили 14 години, се предоставя възможност да притежават уникален идентификатор, на базата на който да бъдат ясно разграничавани от другите лица във виртуалната среда. Електронен идентификатор може да бъде получен едва след издаване на удостоверение за електронна идентичност от компетентните органи. Удостоверението за електронна идентичност от своя страна е дефинирано като формализиран официален електронен документ, издаден за определен срок и съдържащ електронния идентификатор на физическото лице и други негови лични данни. Удостоверенията се издават по писмено поискване на желаещите от министъра на вътрешните

работи, от регистрирани от него администратори на електронна идентичност или чрез дипломатическите или консулските представителства на България в чужбина. След успешното му издаване конкретното удостоверение се публикува в регистъра на удостоверенията за електронна идентичност, поддържан отново от министъра на вътрешните работи.

От тук нататък процесът по удостоверяване на електронната идентичност се извършва чрез автоматизирана проверка на валидността на така издаденото удостоверение при хипотези на предоставяне на електронни услуги или при заявка на заинтересовано лице. Предвидено е осигуряването на свободно и безплатно стандартизирано приложение за проверка на валидността на удостоверението за електронна идентичност, което да бъде достъпно по електронен път.

С оглед зачитане на конкретните нужди на гражданите е предвидено едно лице да има правото да поиска издаване на повече от едно удостоверение за електронна идентичност. Спазвайки принципа на технологична неутралност, законопроекът е уредил механизми електронната идентичност да се съхранява и активира чрез различни носители, включително документи за самоличност с чип, банкови карти с чип, други смарт карти и мобилни устройства. В дискрецията на титулярите на електронна идентичност е поставено пълното право да поискат спиране действието на издаденото удостоверение. Същото правомощие има и министърът на вътрешните работи в изчерпателно изброените от закона случаи (напр. смърт на титуляря или при инциденти, свързани с компрометиране на сигурността на удостоверението).

С оглед на конфиденциалността и нуждата от абсолютна неприкосновеност на данните, които следва да бъдат събирани от физическите лица, министърът на вътрешните работи създава и поддържа публичен електронен регистър на администраторите на електронна идентичност и на центрове за електронна идентификация. Според законопроекта те ще бъдат длъжни да създадат и поддържат вътрешни процедури за сигурност, при които да осъществяват дейността си, съгласно изисквания, определени с наредба, издадена от МС в срок до 6 месеца от обнародването на закона в Държавен вестник. Процедурите за сигурност не са публични и отразяват съответствието на администратора на електронна идентичност с изискванията на закона, както и надеждността и сигурността на осъществяваната от него дейност.

Въвеждат се определени изисквания и по отношение на техническото оборудване и технологиите, според които администраторите на електронна идентичност и на центрове за електронна идентификация трябва да осигурят и да използват процедури и методи за администриране и управление на сигурността на използваната инфраструктура в съответствие с общоприети в международната практика стандарти за управление на информационната сигурност, определени в наредбата.

Във връзка с взаимното признаване на национални схеми за електронна идентификация в рамките на Европейския съюз (ЕС) и за целите на трансграничната автентикация съгласно Регламент № 910/2014 задължението за уведомяване на Европейската комисия е възложено на министъра на вътрешните работи. На министъра на вътрешните работи е възложено и да следи за интегритета на схемата за електронна идентификация, за потенциалните заплахи и за пробив в сигурността на схемата.

Със законопроекта се възлагат функции и на министъра на транспорта, информационните технологии и съобщенията да осъществява сътрудничеството с другите държави членки в няколко основни насоки: обмяната на информация, опит и добри практики във връзка с оперативната съвместимост и сигурност на схемите за електронна идентификация, обхвата и подготовката на партньорски проверки, участието в

мрежа за сътрудничество, която публикува и разпространява препоръки и становища, свързани с националните схеми за електронна идентификация.

Изпълнението на изброените дейности от страна на посочените държавни органи обуславя взаимното признаване с други държави-членки на ЕС, на средства за електронна идентификация с оглед улесняване на трансграничното използване на онлайн услуги и възползване на гражданите от предимствата на единния европейски цифров пазар.

Законопроектът отчита и особеностите на секторните политики, стратегии, цели и дейности на ниво министерства, агенции и общински администрации в областта на развитието на електронното управление. Във връзка с това е предвидена допълнителна възможност за физическите лица да се идентифицират чрез секторни електронни идентификатори в сектори, в които държавните органи предоставят на гражданите възможност да упражняват права по електронен път или да извършват електронни услуги, при което не се събират данни за гражданите от други органи и лица извън конкретния сектор. Правомощието да определя секторите, в които електронната идентификация на лицата да се осъществява чрез секторни електронни идентификатори, е предоставено на Министерския съвет.

Не на последно място е регламентирана и отговорността при неправомерни действия, както и санкциите, които ще бъдат налагани във връзка с нарушенията. Такава отговорност носят както администраторите на електронна идентичност и централните за електронна идентификация, така и действията и бездействията на физически лица, които възпрепятстват дейността на контролните органи или такива, които не подават заявление при промяна в обстоятелствата, подлежащи на вписване в регистър. Провинилите се носят административнонаказателна отговорност, отговорност за неизпълнение на принудителна административна мярка, като е уреден и квалифициран състав при повторно нарушение.

Производство за налагане на административни наказания се извършва от длъжностни лица, определени от министъра на вътрешните работи, а наказателните постановления се издават от министъра. Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на Закона за административните нарушения и наказания.

V. ЕЛЕКТРОННИ УДОСТОВЕРИТЕЛНИ УСЛУГИ

1. ОСНОВНИ ПРИНЦИПИ

A. Приложно поле

Освен въвеждането на принципа за взаимно признаване в европейската законодателна рамка, във втората си част Регламент № 910/2014 установява и обща правна рамка за използването на редица удостоверителни услуги, а именно електронни подписи, електронни печати, електронни времеви печати, електронна препоръчана поща и удостоверяване на автентичността на уебсайт. И в тази област приложното поле на Регламента е внимателно ограничено. Документът не създава общо задължение за използването на удостоверителни услуги, нито пък обхваща предоставянето на удостоверителни услуги, използвани единствено в рамките на затворени системи, произтичащи от националното право или от споразумения между определен кръг от участници. Регламент № 910/2014 не е свързан със сключването и действителността на договори или други правни задължения, нито засяга националните изисквания, които се отнасят до публичните търговски или други регистри.

Б. Общи хоризонтални принципи, приложими по отношение на доставчиците на удостоверителни услуги

Независимо от горните ограничения, Регламент № 910/2014 предвижда ясна и точна правна рамка за удостоверителните услуги, състояща се от няколко хоризонтални принципи, които се прилагат по отношение на доставчиците на удостоверителни услуги и тяхната дейност, както и от специфични правила, свързани с използването на удостоверителни услуги. На основание чл. 3, т. 16 от Регламента удостоверителна е електронна услуга, осигурявана обикновено срещу заплащане, която се състои от: (а) създаване, проверка и валидиране на електронни подписи, електронни печати или електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения, свързани с тези услуги; или (б) създаване, проверка и валидиране на удостоверения за автентичност на уебсайт или (в) съхраняване на електронни подписи, печати или удостоверения, свързани с тези услуги.

Трябва да се отбележи, че съгласно Регламента, доставчиците на удостоверителни услуги могат да бъдат „квалифицирани” и „неквалифицирани”. Квалифицирани доставчици на услуги са тези, които предоставят една или повече квалифицирани удостоверителни услуги и им е предоставен квалифициран статут от надзорен орган на държава-членка. От друга страна, доставчици на неквалифицирани услуги са тези, които не предоставят квалифицирани удостоверителни услуги по смисъла на Регламента.

Както квалифицираните, така и неквалифицираните доставчици на удостоверителни услуги носят отговорност за щети, нанесени умишлено или поради небрежност, на клиенти – физически или юридически лица, поради неизпълнение на задълженията съгласно Регламента, освен в случаите, когато клиентите са надлежно информирани относно ограниченията на съответните удостоверителни услуги. Независимо от общата приложимост на принципа на отговорността, тежестта на доказване по отношение на отговорността, се различава, когато става дума за квалифицирани и неквалифицирани доставчици на удостоверителни услуги [13].

Освен това, доставчиците на квалифицирани и неквалифицирани удостоверителни услуги са длъжни да предприемат подходящи технически и организационни мерки за управление на рисковете, свързани с предоставянето на удостоверителни услуги. Те са длъжни да уведомяват надзорния орган без излишно забавяне, но при всички случаи в срок от 24 часа, за всеки случай на пробив в сигурността или нарушаване на целостта, които имат въздействие върху предоставяната удостоверителна услуга. Ако пробивът в сигурността или нарушаването на целостта окажат негативно въздействие върху физическо или юридическо лице, доставчикът е длъжен да уведоми въпросното физическо или юридическо лице.

Регламентът също така предвижда определянето на надзорен орган във всяка държава-членка, който да извършва надзорните дейности върху доставчиците на квалифицирани удостоверителни услуги и да предприема действия, когато това е необходимо, спрямо доставчиците на неквалифицирани удостоверителни, действащи на територията. За да се гарантира ефективното функциониране на надзорните органи в държавите-членки, на същите се предоставят необходимите правомощия и достатъчни ресурси. Освен това, надзорните органи следва да работят в съответствие с принципа на взаимопомощ и сътрудничество с оглед ефективен обмен на добри практики.

В. Допълнителни хоризонтални принципи, приложими по отношение на доставчиците на квалифицирани удостоверителни услуги

В допълнение към гореспоменатите общи принципи, приложими както за доставчиците на квалифицирани удостоверителни услуги, така и за доставчиците на неквалифицирани удостоверителни услуги, първите трябва да отговарят и на някои до-

пълнителни изисквания. За да станат доставчици на квалифицирани удостоверителни услуги, т.е. за да започнат да предоставят квалифицирани удостоверителни услуги, заинтересованите лица изпращат на надзорния орган уведомление за намерението си заедно с доклад за оценяване на съответствието, съставен от органа за оценяване на съответствието. Ако надзорният орган потвърди, след проверка, че изискванията, определени от Регламент № 910/2014 са изпълнени от страна на доставчика на удостоверителни услуги, последният може да получи квалифициран статут. Освен това, квалифицираните доставчици на удостоверителни услуги трябва да фигурират в специални доверителни списъци, създадени, поддържани и публикувани от държавите-членки. Тези списъци указват статута на даден доставчик на услуги и имат решаваща роли при изграждане на доверие между пазарните субекти. Доверието се укрепва и от годишните одити, на които са подложени доставчиците на удостоверителни услуги. Съгласно правилата, разписани в Регламента, доставчиците биват одитирани на всеки 24 месеца от орган за оценяване на съответствието, за да бъде доказано, че те напълно отговарят на изискванията на Регламента.

Квалифицираните доставчици на удостоверителни услуги имат право да използват марката за доверие на ЕС [14], за да могат да обозначават по ясен и разпознаваем начин услугите, които предоставят. Това предимство е важно, тъй като спомага за повишаване на доверието на потребителите в предоставяната електронна услуга. Прозрачността на пазара се подсилва и от някои допълнителни изисквания, на които трябва да отговарят доставчиците на квалифицирани удостоверителни услуги. Тези допълнителни изисквания се отнасят до използването на средства за проверка с цел издаване на квалифицирани удостоверения за удостоверителни услуги на физически или юридически лица, до задължението да информират за промени в предоставянето на удостоверителните услуги, до персонала, до отговорността за вреди, до техническата сигурност и надеждност, както и до надеждността на системите за съхранение на данни.

2. ПРАВИЛА, СВЪРЗАНИ С ЕЛЕКТРОННИТЕ УДОСТОВЕРИТЕЛНИ УСЛУГИ

След като очертава общата рамка за доставчиците на квалифицирани и неквалифицирани удостоверителни услуги и след като структурира техните дейности, Регламент № 910/2014 доразвива правилата, касаещи всяка от въведените удостоверителни услуги, а именно електронни подписи, електронни печати, електронни времеви печати, услуги за електронна препоръчана поща, както и удостоверения за автентичност на уебсайт и въвежда принципа, според който правната сила и допустимостта на електронните документи като доказателство при съдебни производства са същите като на хартиените документи.

А. Електронни подписи

Регламент № 910/2014 въвежда забраната, че правната сила и допустимостта на електронния подпис като доказателство при съдебни производства могат да бъдат оспорени единствено на основанието, че той е в електронна форма или че не отговора на изискванията за квалифицирани електронни подписи. В Регламента са залегнали някои правила, касаещи усъвършенстваните електронни подписи, но централно място в правната рамка в областта на електронните подписи заема квалифицирания електронен подпис.

Регламентът приема, че електронният подпис има същата правна сила като саморъчния подпис. В допълнение към това, за да гарантира трансграничното използване на квалифицирани електронни подписи в държавите-членки, Регламентът призовава към взаимно признаване на квалифицираните електронни удостоверения. За тази цел, Приложение 1 на Регламента описва подробно изискванията към квалифицира-

ните удостоверения за електронни подписи. Регламентът дава възможност за допълнителни незадължителни изисквания, които да бъдат въведени по преценка на всяка държава-членка, стига те да не възпрепятстват трансграничната оперативна съвместимост и признаване на удостоверенията. Независимо от това, с цел постигане на ефективност и успешно утвърждаване на изискванията към квалифицираните електронни подписи, не следва да се прилагат допълнителни задължителни изисквания по отношение на квалифицираните удостоверения извън тези, съдържащи се в Приложение 1.

За изграждане и поддържане на доверието в европейския цифров пазар, Регламент № 910/2014 взема под внимание необходимостта от установяване на ясни правила и процедури, касаещи случаите, в които квалифицирано удостоверение за електронни подписи бъде отменено. В такива случаи, то следва да изгуби валидността си от момента на отмяната и неговият статут не може да бъде възстановен отново. Въвеждането на допълнителни правила относно временното спиране на валидността е предвидено в Регламента, тъй като временното спиране е практика сред доставчиците на удостоверителни услуги. Временното спиране се различава от отмяната на удостоверението, доколкото то води до временно, а не постоянна загуба на валидност на удостоверението. Регламентът дава възможност на държавите-членки да въвеждат и поддържат правила за временното спиране на валидността на квалифицираните удостоверения на електронните подписи, но призовава към ясно и публично указване на периода на спиране.

Предвидени са и редица разпоредби по отношение на изискванията към устройствата за създаване на квалифициран електронен подпис, както и по отношение на услугите по квалифицирано валидиране и квалифицирано съхраняване на квалифицирани електронни подписи. Във връзка с услугата по квалифицирано валидиране на квалифицирани електронни подписи Регламентът предвижда, че тя може да се предоставя единствено от доставчик на квалифицирани удостоверителни услуги, който прилага всички изисквания към валидирането на квалифицирани електронни подписи и който дава възможност наверяващите се страни да получат резултата от процеса на валидиране по автоматизиран начин, който е надежден и ефикасен и носи усъвършенстван електронен подпис или усъвършенстван електронен печат на доставчика на услугата по квалифицирано валидиране. По отношение на услугата по съхраняване на квалифицирани електронни подписи Регламентът предвижда, че тя може да се предоставя единствено от доставчици, използващи процедури и технологии, позволяващи гарантиране на надеждността на квалифицирания електронен подпис и в допълнение въвежда редица стандарти за предоставянето на тази услуга.

Б. Електронни печати

Подобно на електронните подписи, електронните печати имат същата правна сила като обикновените печати. Съгласно условията на Регламента, електронните печати представляват данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произхода и целостта на последните. Фактът, че са данни, създадени и функциониращи в електронна среда, не следва да ги лишава от тяхното предназначение и сила. Напротив, Регламентът въвежда презумпция за цялост и точност на произхода на данните, за които се отнася квалифицираният електронен печат. Освен това, квалифицираният електронен печат се прилага като печат с най-висока степен на сигурност, изисквана при трансгранично използване при онлайн услуга, предлагана от орган от публичния сектор. Удостоверенията за квалифицирани електронни печати и в този случай са от първостепенна важност. Те са обект на задължителни изисквания, които не могат, по усмотрение на държавите-членки, да надхвърлят изискванията, предвидени в

Приложение 3 към Регламента. Въпреки това, държавите-членки имат възможност да въвеждат допълнителни, но задължителни, специфични изисквания, стига те да не възпрепятстват трансграничната оперативна съвместимост и признаване на електронните печати. Правилата, касаещи отмяната и временното спиране на валидността на удостоверенията за електронни печати са много сходни с приложимите за електронните подписи правила.

В. Електронни времеви печати

Съгласно Регламента електронните времеви печати означават данни в електронна форма, които свързват други данни в електронна форма с конкретен момент във времето и представляват доказателство, че последните данни са съществували в съответния момент. Електронните времеви печати имат правна сила, която не може да бъде оспорена единствено на основание, че са в електронна форма. Регламентът подчертава важноста на взаимно признаване сред държавите-членки на тези инструменти. Отчитайки необходимостта от изграждане на ясна и ефективна правна рамка по отношение на квалифицираните електронни времеви печати, Регламентът предвижда редица изисквания, които трябва да се спазват за целите на признаването и ефективното използване на тези удостоверителни услуги.

Г. Услуги за електронна препоръчана поща

По своята същност услугите за електронна препоръчана поща позволяват предаването на данни между трети страни по електронен път, предоставят доказателство във връзка с обработката на предаваните данни, включително доказателство за изпращането и получаването на данните, и защитават предаваните данни срещу риск от загуба, кражба, повреда или непозволенни изменения. Услугите за електронна препоръчана поща също имат правна сила, която не може да бъде оспорена единствено на основание, че са предоставяни в електронна форма. Регламентът подчертава колко е важно да се изгради правна рамка за трансграничното признаване на тези удостоверителни услуги, като потвърждава водещата роля на квалифицираните услуги за електронна препоръчана поща. Въвеждат се редица изисквания, приложими за тези квалифицирани удостоверителни услуги, които да спомогнат за правилното им използване и по този начин да се гарантира тяхната валидност.

Д. Удостоверяване автентичността на уебсайтове

Регламентът съдържа допълнителни изисквания по отношение на удостоверяването на автентичността на уебсайтове. Удостоверяването на автентичността на уебсайтове осигурява средство, с което даден посетител на уебсайт може да бъде уверен, че зад уебсайта стои реален и легитимен субект. Тези услуги значително допринасят за изграждането на доверието в онлайн бизнес средата между държавите-членки. Регламентът подчертава, че предоставянето и използването на услугите по удостоверяване на автентичността на уебсайт са изцяло на доброволна основа. Въпреки това, с цел гарантиране подобряването на работата на потребителя с уебсайта, както и с цел увеличаване на доверието в европейския цифров единен пазар, Регламентът установява минимални задължения за сигурност и отговорност за доставчиците, предоставящи удостоверяване автентичността на уебсайтове.

VI. ПРОЦЕДУРЕН ПОДХОД

Важно е да се отбележи, че приносът на Регламента по отношение на развитието на европейския цифров единен пазар се изразява не само в правните нововъведения, които Регламентът принципно въвежда в правната рамка на ЕС, но също и в неговия методологичен и процедурен подход по отношение на приемането, изпълнението и прилагането на правилата, залегнали в него.

1. ВЪЗМОЖНОСТ ЗА ПРИЕМАНЕ ОТ ЕВРОПЕЙСКАТА КОМИСИЯ НА ПОДЗАКОНОВИ НОРМАТИВНИ АКТОВЕ

С цел изпълнение на някои технически задачи по подходящ и бърз начин, европейският законодател е делегирал на Европейската комисия правомощието да приема подзаконовни нормативни актове. Подзаконовите нормативни актове могат да бъдат делегирани актове или актове за изпълнение. В съответствие с чл. 290 от Договора за функционирането на Европейския съюз (ДФЕС), Регламент № 910/2014 предвижда приемането от Комисията на един делегиран акт. Тази власт, предоставена на Комисията, се отнася изключително до установяване на критерии, които да бъдат изпълнени от назначените от държавите-членки частни или публични органи, отговарящи за сертифициране на устройства за създаване на квалифициран електронен подпис. Много повече на брой, а именно 28, са актовете за изпълнение, за които на Комисията са дадени правомощия да приема. Както е предвидено, няколко изпълнителни акта вече са приети от Комисията, по отношение на електронната идентификация (по аспекти, свързани с процедурните правила за сътрудничество между държавите-членки при електронната идентификация; относно рамката за оперативна съвместимост; за минималните технически спецификации, стандарти и процедури по отношение на нивата на осигуреност) и по отношение на удостоверителните услуги (по някои аспекти, свързани с електронния подпис и печатните формати, които да бъдат признати от орган от публичния сектор; относно техническите спецификации и формати на доверителните списъци; както и по отношение на марката за доверие на ЕС за квалифицирани удостоверителни услуги). Това делегиране на правомощия към Европейската комисия, в някои ограничени, главно технически области, има за цел да облекчи законодателна тежест и да се гарантира, че по време на работата на Комисията, международните стандарти и технически спецификации ще бъдат взети под внимание.

2. ПРЕХОДЕН ПЕРИОД

В допълнение към това, Регламентът предвижда преходен период между приемането и влизането в сила на неговите разпоредби. С цел постигане на правна сигурност за операторите на пазара, потребителите и публичните органи разпоредбите, касаещи въпросите, които преди това са били регулирани от Директивата за електронен подпис или касаещи сертификатите и устройствата, издадени съгласно условията на гореспоменатата Директива, ще влязат в сила не по-рано от средата на 2016 г., когато Директивата ще се счита за окончателно отменена и неприложима. До тогава, устройствата за създаване на защитени подписи, чието съответствие е било определено съгласно условията на Директивата, ще се считат за устройства за създаване на квалифицирани подписи съгласно Регламента. По същия начин, квалифицирани удостоверения, издадени на физически лица по силата на Директивата ще се считат за квалифицирани удостоверения за електронен подпис съгласно Регламента.

Прилагането на Регламента ще започне от 1 юли 2016 г. Доброволното признаване на схемите за електронна идентификация може да започне от края на 2015 г., а задължителното трансграничното признаване на тези схеми е планирано за септември 2018 г.

И въпреки, че остават още няколко години, докато видим широкото въздействие на нововъведенията на Регламент № 910/2014 и пълното прилагане на разпоредбите му, неговите механизми са вече задвижени и дават своето отражение в националното ни законодателство.

Литература:

1. 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, публикуван в Официален вестник на Европейския съюз L 257, 28.08.2014 г., стр. 73-114
2. COM(2010) 245 окончателен/2
3. COM(2010) 603 окончателен
4. Достъпно на http://europa.eu/rapid/press-release_IP-12-1389_en.htm
5. Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 относно правната рамка на Общността за електронните подписи, публикуван в Официален вестник на Европейския съюз L 013, 19.01.2000 г., стр. 0012 – 0020
6. Регламент № 910/2014, Цитат (3)
7. Заключение на Съвета от 25 май 2011 г.
8. Съгласно чл. 3, т.2 на Регламента „средство за електронна идентификация“ означава материална и/или нематериална единица, която съдържа данни за идентификация на лица, която се използва за удостоверяване на автентичност за онлайн услуга.
9. Съгласно чл. 3, т.4 на Регламента „схема за електронна идентификация“ означава система за електронна идентификация, при която средства за електронна идентификация се издават на физически или юридически лица, или физически лица, представляващи юридически лица.
10. Съгласно чл. 8, т.2, (б) на Регламент № 910/2014 ниво на осигуреност „значително“ се отнася за средство за електронна идентификация в контекста на схема за електронна идентификация, което предоставя значителна степен на надеждност на претендираната или заявената самоличност на дадено лице.
11. Съгласно чл. 8, т.2, (в) на Регламент № 910/2014 хх ниво на осигуреност „високо“ се отнася за средство за електронна идентификация в контекста на схема за електронна идентификация, което предоставя по-висока степен на надеждност на претендираната или заявената самоличност на дадено лице, отколкото средствата за електронна идентификация с ниво на осигуреност „значително“.
12. Съгласно чл. 8, т.2, (а) на Регламент № 910/2014 ниво на осигуреност „ниско“ се отнася за средство за електронна идентификация в контекста на схема за електронна идентификация, което предоставя ограничена степен на надеждност на претендираната или заявената самоличност на дадено лице.
13. По отношение на доставчици на неквалифицирани удостоверителни услуги тежестта на доказване пада върху физическото или юридическото лице, подало иск. По отношение на доставчици на квалифицирани удостоверителни услуги, обратно, наличието на умисъл или небрежност, довели до щети, се презюмира, освен ако доставчикът докаже друго.
14. Според Цитат (1) от Регламента за изпълнение (ЕС) № 2015/806 на Комисията от 22 май 2015 г. относно определяне на спецификации, отнасящи се до формата на марката за доверие на ЕС за квалифицирани удостоверителни услуги, целта на марката за доверие на ЕС е квалифицираните удостоверителни услуги ясно да се разграничат от другите удостоверителни услуги, като по този начин се допринася за прозрачността на пазара и така се спомага за доверието в онлайн услугите и за удобство при ползването им, които са изключително важни, за да могат потребителите напълно да се възползват от електронните услуги и осъзнато да разчитат на тях.