Dimitrov, Petrov & Co.
BULGARIAN LAW FIRM

Partners:
George Dimitrov
Bogdan Petrov
Alexander Todorov
Metodi Baykushev
Zoya Todorova
Hristo Nihrizov
Plamena Georgieva
Boyana Milcheva

Associates:
Desislava Krusteva
Dimitar Karabelov
Sylvina Beleva
Encho Simeonov
Donka Stoyanova
Emil Tumbev
Boyan Ivanov
Nikoleta Stoyanova
Pavlina Ivanova
Bilyana Stefanova
Tsvetelina Georgieva
Albena Angelova
Gergana Georgieva
Pencho Stanchev

Sofia 1303, Bulgaria
28 Todor Alexandrov Blvd, fl. 7
tel.: +359 2 421 42 01
fax: +359 2 421 42 02
e-mail: mail@dpc.bg

Varna 9000, Bulgaria
7 Krastyu Mirski Str, fl. 3, office 9
tel.:+359 52 912 986
fax:+359 52 912 987
e-mail: varna@dpc.bg

website: http://www.dpc.bg

MERITAS
LAW FIRMS WORLDWIDE

THE UPCOMING REGULATION OF CERTIFICATION SERVICES IN THE EU

In a world where services increasingly become digital and cross-border and cross-sector electronic transactions become irreplaceable, the EU Digital Single Market is on the verge of receiving a major boost with the newly adopted Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter "Regulation No 910/2014" or "the Regulation").

The Regulation, adopted by the European Parliament and the Council on 23 July 2014, repeals Directive No 1999/93/EC on a Community framework for electronic signatures (the E-Signatures Directive) and seeks to overcome current security and interoperability deficiencies. It aims to increase the transparency, the neutrality and thus the effectiveness of the electronic interaction between citizens, businesses and public authorities by creating a predictable, clear and workable legal environment for secure and trustworthy electronic transactions.

The Regulation brings innovation to the regulatory frameworks of both electronic identification and electronic trust services. With respect to the electronic identification, the Regulation introduces the principles of interoperability and of mutual recognition of national identification schemes, notified to the European Commission. As a result, EU citizens will be able to use their own national identification means to access public services across EU member states where other identification schemes are available. With respect to trust services, the Regulation builds up an innovative legal framework in order to make them legally recognized and applicable across borders within the EU. More precisely, it ensures that electronic signatures and electronic seals have the same legal value as signatures, seals or stamps physically applied to a document, that electronic time stamps and electronic registered delivery services are legally recognized, that electronic documents are legally admissible, and that the authenticity of a website may be verified.

The countdown for completion of the reform brought by Regulation No 910/2014 has already started. Notwithstanding the Regulation's entry into force on 17 September 2014, it will apply as of 1st July of 2016, with few exceptions - a number of implementing acts are expected to be adopted by mid-2015 which will allow for Member states to start voluntarily recognizing other Member states' notified e-identification schemes. The rest of the Regulation's provisions will then gradually start applying. Provisions regarding electronic trust services will apply as of 1st July 2016, whilst those regarding the mandatory mutual recognition of e-identification schemes are previewed for mid-2018.

It seems that in terms of e-identification and trust services the best is yet to come. Meanwhile, in the digital era we are living in, acquaintance with Regulation No 910/2014 is a must.

*

* *

Regulation No 910/2014[1], designed to boost the trust and convenience in cross-border electronic transactions across EU Member States, represents a noteworthy centerpiece in the EU legislative arsenal with regard to the digital single market, insofar as building trust in the online environment is today privileged as the cornerstone of economic and social development. The Regulation is a remarkable step forward towards the creation of a common framework for secure electronic interactions between citizens, businesses and public authorities.

The adoption of Regulation No 910/2014 came as a result of the crucial necessity to bolster the development of the EU digital market by introducing a coherent and comprehensive legal framework which would strengthen the up-to-date achievements in the field and, in the same time, remedy the identified shortcomings.

I. INSUFFICIENCIES AND NEED FOR A REFORM

A number of issues causing shrinkage of the European digital economy and preventing it from growing were widely discussed and confirmed on multiple occasions by the EU authorities. In its Communication of 26 August 2010 "A Digital Agenda for Europe"[2] the European Commission pointed out that the fragmentation of the digital market, the lack of interoperability and the rise of cybercrime represented major obstacles to the growth of the digital economy and needed to be overcome. In another 2010 document - the EU Citizenship Report, entitled "Dismantling the obstacles to the EU citizens' rights"[3]- the Commission further emphasized the need to eliminate the difficulties which prevented the EU citizens from enjoying the benefits of the digital single market and the cross-border digital services offered thereon. Furthermore, in a press release, entitled "Digital "to-do" list: new digital priorities for 2013-2014"[4], published on 18 December 2012, the Commission pointed out the fact that "[t]he digital economy [was] growing at seven times the rate of the rest of the economy, but this potential [was] held back by a patchy pan-European policy framework". Another issue identified was the circumstance that the E-Signatures Directive[5] dealt with electronic signatures "without [in fact]

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal L 257, 28.8.2014, p. 73 - 114

[2] COM(2010) 245 final/2

[3] COM(2010) 603 final

[4] Available on http://europa.eu/rapid/press-release_IP-12-1389_en.htm

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19.01.2000, p. 0012 - 0020

delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transitions"[6]. As it title suggests, the E-Signatures Directive merely covered the area of electronic signatures and did not contain further rules on other trust services which today are considered as important to the establishment of trust and confidence on the European digital single market.

II. THE CHALLENGE

All these shortcomings represented a major challenge to the European Commission which, in 2011, was invited by the Council[7] to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders such as electronic identification, electronic documents, electronic signatures and electronic delivery services.
Past halfway between the Regulation's entry into force (which took place on 17 September 2014) and the day most of the provisions of the Regulation will become applicable (1st July of 2016) it seems safe to say that the challenge was gladly accepted and will soon be completed.
Regulation No 910/2014 represents a clear and comprehensive toolkit setting up mechanisms and rules for the establishment of trustworthy and confidence-enhanced electronic transactions. It faces the challenges brought by the development of new technologies to international transactions and to their legal framework. It thus eagerly covers matters which have never been regulated on EU level before.

III. METHODOLOGICAL APPROACH AND REFINEMENTS

One of the most important objectives of Regulation No 910/2014 is to remove the existing barriers to the cross-border use of electronic identification means commonly used in the Member States to authenticate, insofar as these barriers prevent EU citizens from operating with their electronic identification to authenticate themselves in another Member State, and service providers from enjoying the full benefits of the internal market. The Regulation addresses the lack of recognition amongst EU Member States of national authentication schemes by employing a rational and well-measured approach.
Firstly, the Regulation's scope of application is attentively limited. For the purposes of cross-border use of electronic identification means, it only covers public services. The private sector is granted full autonomy. Notwithstanding, the latter is strongly encouraged to voluntarily use electronic identification means under a notified, thus recognized, scheme for identification purposes when such are needed for the purposes of online services or electronic transactions.

[6] Regulation No 910/2014, Recital (3)
[7] Council conclusions of 27 May 2011

Secondly, a great level of independence is left to the Member States. They remain free to introduce or maintain the use electronic identification means for the purposes of accessing online services. It is also up to Member States to decide whether to notify to the European Commission all, some or none of their electronic identification schemes used at national level to access public online services. The Regulation does not seek to intervene with electronic identity management systems and infrastructures established in Member States. It merely aims to ensure that secure electronic identification and authentication is possible.

Lastly but most importantly, Regulation No 910/2014 is not built upon rigid regulatory rules but on a set of principles. Such flexibility adds a particular value to the mechanisms introduced by it. The document is bound by the principle of technological neutrality, which is to mean that the Regulation does not introduce requirements which could be met solely by a certain privileged technology. On the contrary - the legal effect of the Regulation should be achieved by any technical means which satisfies the requirements introduced by it. Regulation No 910/2014 also follows an open-to-innovation principle which allows for an up-to-date regulatory framework corresponding to the ever accelerating pace of technological evolution. Basing security and certification methods on international standards is another principle adopted by the Regulation. Furthermore, it considerately takes into account the prospective emergence of innovative solutions and services for which security standards may not yet be available. In such cases the document foresees using alternative processes comparable to existing standards.

Notwithstanding the above methodological refinements, in essence Regulation No 910/2014 institutes two legal mechanisms - it introduces the principle of mutual recognition of electronic identification (eID) means amongst Member States and establishes a general legal framework for the use of trust services.

IV. THE MUTUAL RECOGNITION OF EID MEANS

The mutual recognition of electronic identification means, introduced by the Regulation, stands out as a principle of utmost importance. It substantiates the main objective of Regulation No 910/2014, namely the idea of introducing a mechanism aimed at ensuring that people and businesses could use their electronic identification means to access at least public online services across the EU. Pursuant to this principle, Member States mutually recognize each other's electronic identification means[8] issued under a notified identification scheme[9]. The mechanism would apply in cases where electronic identification

[8] According to Art. 3, pt.2 of the Regulation "electronic identification means" is a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.

[9] Pursuant to Art. 3, pt.4 of the Regulation "electronic identification scheme" is a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.

via eID means and authentication is required under one Member State's national law or administrative practice to access a service provided by a public sector body online. As soon as an electronic identification scheme has been voluntarily notified, the mutual recognition becomes mandatory, provided that the conditions set up in Regulation No 910/2014 are fulfilled.

The principle of mutual recognition is built upon several elements aimed at establishing trust amongst Member States and at guaranteeing the successful application of its mechanisms.

First of all, in order for one Member States' electronic means to be recognized in other Member States, it needs to be issued under an electronic identification scheme which was notified to the European Commission and was published in the Official Journal of the EU.

Another important element is the assurance level of the electronic identification means. As indicated in the recitals of Regulation No 910/2014, the assurance level characterizes the degree of confidence in electronic identification means when it comes to establishing the identity of a person. The assurance level depends on the strength of confidence that a given electronic identification means provides with regard to the identity of a person, and is based on processes, management activities and implemented technical controls. According to these criteria assurance levels may be categorized as "low", "substantial" and "high". For the purpose of the mandatory mutual recognition, the assurance level of the electronic identification means issued by one Member State should correspond to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in another Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level "substantial"[10] or "high"[11]. Mutual recognition of electronic identification schemes the assurance level of which is "law"[12] is voluntary. In addition, it is also necessary that the relevant public sector body uses the assurance level "substantial" or "high" in relation to accessing that service online.

The technical cooperation and interoperability is another important element on which the principle of mutual recognition is constructed. Member States will cooperate with regard to the security of the electronic identification schemes and will ensure that electronic identification schemes notified to the Commission are interoperable. For the purposes of ensuring interoperability, the Regulation provides for the establishment of an interoperability framework, which will consists of a reference to minimal technical requirements related to

[10] According to Art. 8, pt.2, (b) of Regulation No 910/2014 assurance level "substantial" refers to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person.

[11] Pursuant to Art. 8, pt.2, (c) of Regulation No 910/2014 assurance level "high" refers to an electronic identification means, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial.

[12] According to Art. 8, pt.2, (a) of Regulation No 910/2014 assurance level "low" refers to an electronic identification means, which provides a limited degree of confidence in the claimed or asserted identity of a person.

assurance levels, a mapping of national assurance levels, a reference to minimal technical requirements for interoperability, as well as to a minimum set of person identification data, arrangements for dispute resolution and common operational security standard. The interoperability framework is deemed to abide by the principle of technological neutrality, to follow European and international standards, to facilitate the privacy-by-design and to ensure that personal data is lawfully processed.

The mutual recognition of eID means also implies that Member States provide cross-border online authentication capabilities. These cross-border capabilities should be provided free of charge when it is carried out in relation to an online service provided by a public sector body. With regard to entities which are not public bodies, Member States may, at their discretion, define terms of access to the online authentication, provided these terms are not disproportionate or discriminatory to parties established in another Member State.

A set of rules on the liability is also introduced by the Regulation. It covers the liability of Member States (for damages caused to natural or legal persons due to a failure to comply with the requirements relating to person identification data), of the issuer of the electronic identification means (for damages caused to natural or legal persons due to a failure to attribute the electronic identification means to the correct person), and of the party operating the authentication procedure (for damages caused to natural or legal persons due to a failure to ensure the correct operation of the authentication).

V. THE ETRUST SERVICES FRAMEWORK

1. GENERAL PRINCIPLES

Further to the introduction of the principal of mutual recognition in the European legal framework, the second part of Regulation No 910/2014 establishes a general legal framework for the use of a number of trust services, namely electronic signatures, electronic seals, time stamping, electronic registered delivery service and website authentication. In this domain again the Regulation's scope is attentively limited. The document does not create a general obligation to use trust services nor does it cover the provision of services used exclusively within closed systems between a defined set of participants. Regulation No 910/2014 does not cover the conclusion and the validity of contracts or other legal obligations either and does not affect national requirements with regard to pubic commercial or other registers.

Notwithstanding the above limitations, Regulation No 910/2014 provides for a concise legal framework for trust services, composed of a number of horizontal principles which apply with regard to trust service providers and their activity, as well as of specific rules related to the use of trust services. Pursuant to Art. 3, pt. 16 of the Regulation trust service is an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic

registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services.

It is noteworthy that pursuant to the Regulation, trust service providers may be "qualified" and "non-qualified". Qualified service providers are those who provide one or more qualified trust services and are granted the qualified status by a Member State's supervisory body. On the contrary, non-qualified service providers are those who do not provide qualified trust services under the meaning of the Regulation.

Both qualified and non-qualified trust service providers may be held liable for damages caused intentionally of negligently to customers – natural or legal person, due to a failure to comply with the obligations under the Regulation, unless customers have been duly informed on the limitations of the respective trust service. Notwithstanding the general applicability of the liability principle, the burden of proof with regard to the liability differs when it comes to qualified and non-qualified trust service providers[13].

Further, both qualified and non-qualified trust service providers are bound by the requirement to take the appropriate technical and organizational measures to manage the risks that the provision of trust services faces. They are obliged to notify to the supervisory body, without undue delay and in any case within 24 hours, any breach of security or loss of integrity which may impact in any way the provided trust service. In case the breach of security or the loss of integrity might negatively affect a natural or a legal person, the service provider is obliged to notify them as well.

The Regulation also provides for the designation of a supervisory body, established in every Member State, which would be responsible for supervising qualified trust service providers and for taking action, when necessary, in relation to non-qualified trust service providers established on its territory. In order to guarantee the effectivity of the functioning of supervisory bodies across Member States, the Regulation requires that they are given the necessary powers and adequate resources. In addition, supervisory bodies shall comply with the principle of mutual assistance and cooperation so as to effectively exchange good practices.

In addition to the above common principles applicable to both qualified and non-qualified trust service providers, the latter are subject to further requirements. In order to become a qualified trust service provider, *i.e.* to start providing qualified trust services, the provider should submit a notification to the relevant supervisory body together with a conformity assessment report, issued by a conformity assessment body. Should the supervisory body confirm, after verification, that the requirements laid down in Regulation No 910/2014

[13] With regard to non-qualified trust service providers the burden of proof lies with the natural or legal person claiming the damage. With regard to qualified trust service providers, on the contrary, the negligence or the intention which has caused the damage is presumed unless proven otherwise by the service provider.

are fulfilled by the trust service provider the latter may be granted a qualified status. Additionally, qualified trust service providers should figure in specific trusted lists, established, maintained and published by Member States. These trusted lists indicate the status of a given service provider and are thus essential to the build-up of trust amongst market operators. Trust is also strengthened by the annual audits qualified trust service providers are subject to. Pursuant to the rules set out in the Regulation, they should be audited every 24 months by a conformity assessment body in order to prove they are fully compliant with the requirements introduced by the Regulation.

Qualified trust service providers are entitled to use the EU trust mark[14] to indicate in a simple and recognizable way the service they provide. This advantage is noteworthy as it helps increasing the users' confidence in the provided electronic service. The transparency on the market is also boosted by the set of additional requirements that qualified trust services are subject to, pertaining to the use of verification means for the purposes of issuing qualified certificates for trust services to natural or legal persons, the information obligation in case of change of the provision of qualified services, the personnel, the liability for damages, the technical security and reliability, and the trustworthiness of the data storage systems.

2. EXPLICIT RULES REGARDING EACH ETRUST SERVICE

Once the general framework on the qualified and non-qualified trust service providers presented and their activities structured, Regulation No 910/2014 further develops rules regarding each of the introduced trust services, namely electronic signatures, electronic seals, electronic time stamping, electronic registered delivery service and web authentication, and established the principle according to which electronic documents are recognized the same legal effect and admissibility as evidence in legal proceedings as regular documents.

Electronic signatures

Regulation No 910/2014 substantiates the prohibition that the electronic signature is denied legal effect and admissibility as evidence in legal proceedings only because it is in electronic form or because it does not meet the requirements for a qualified electronic signature. The document sets forth some rules with regard to advanced electronic signatures, but the centerpiece of the legal apparatus in the field of electronic signatures is the qualified electronic signature.

The Regulation recognizes the equivalence of the qualified electronic signature's legal effect to the one of a handwritten signature. Furthermore, in

[14] According to Recital (1) of Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services, the aim of the EU trust mark is to clearly differentiate qualified trust services from other trust services, which would essentially contribute to transparency in the market by fostering confidence in and convenience of online services which are essential for users to fully benefit and consciously rely on electronic services.

order to guarantee the cross-border use of qualified electronic signatures across EU Member States, the Regulation calls for a mutual recognition of qualified electronic certificates. For this purpose, in its Annex 1, it carefully details the requirements pertaining to the qualified electronic certificates of electronic signatures. The Regulation leaves room for additional non-mandatory attributes for qualified electronic signatures which may be introduced on the discretion of every Member State, provided that they do not hinder cross-border interoperability and recognition of certificates. Notwithstanding, in a pursuit of efficiency and successful consolidation of requirements pertaining to qualified electronic signatures, no additional mandatory requirements exceeding those contained in Annex 1 should be applied with regard to certificates.

In order to build up trust and to sustain the confidence in the EU digital market, Regulation No 910/2014 considerately takes into account the need to establish clear rules and procedures in case the qualified electronic certificates are revoked. In such cases it is required that the certificate loses its validity from the moment of its revocation and it could not obtain it again. The introduction of further rules on temporary suspension is foreseen by the Regulation as the temporary suspension is an established practice of trust service providers across Member States. The temporary suspension differs from the revocation of the certificate insofar as it implies a temporary and not a permanent loss of validity of the certificate. The Regulation allows Member States to maintain or to introduce rules on temporary suspension of qualified certificates of electronic signatures but calls for a clear and public indication of the suspension period.

A number of provisions also specify the certification of qualified electronic signature devices and the requirements for the validation of qualified electronic signatures. Lastly, the Regulation requires that preservation service for qualified electronic signatures is provided solely by trust service providers who use technologies and procedures capable of extending the trustworthiness of the qualified electronic signature, and foresees the introduction of a number of standards for the provision of this service.

Electronic seals

Similarly to electronic signatures, electronic seals are recognized the same legal effect as regular seals. Pursuant to the terms of the Regulation electronic seals represent data in electronic form which is attached to or logically associated with other data in electronic form to ensure its origin and integrity. The fact that they are created and function in electronic environment should not deprive them of their purpose and effect. On the contrary, with regard to qualified electronic seals, the Regulation asserts the presumption of integrity and the correctness of data, to which they are linked. Further, the qualified electronic seal is enforced as the highest security-level seal which may be requested for the cross-border use of an online service provided by a public sector body. The certificates for the qualified electronic seals are, here again, of an utmost importance. They are subject to specified mandatory requirements which may not, on the discretion of Member States, be furthered than what is previewed in Annex 3 of the

Regulation. Nevertheless, Member States may introduce additional, although non-mandatory, specific attributes to qualified certificates for electronic seals, provided these attributes do not hinder the cross-border interoperability and recognition of electronic seals. Rules on the revocation and the temporary suspension of qualified certificates for electronic seals are introduced in a manner very similar to the one applicable to qualified certificates for electronic signatures. With regard to the rules on the creation devices for qualified electronic seals and to the requirements pertaining to the validation and preservation of qualified electronic seals, without going into unnecessary restatements, the European legislator directly refers to the respective requirements applicable to qualified electronic signatures.

Electronic time stamps and electronic registered delivery services

Electronic time stamps and electronic registered delivery services are also recognized a legal effect that shall not be denied only because of their electronic form. With respect to qualified electronic time stamps, the Regulation again underlines the importance of the mutual recognition amongst Member States. Regarding electronic registered delivery services, it confirms the importance of the establishment of a legal framework for the cross-border recognition of such trust services. Considering the need for the built-up of a coherent and efficient legal framework with regard to the qualified electronic time stamps and the qualified electronic registered delivery services, the Regulation lays down a number of requirements which are to be observed for the purposes of the recognition and the effective use of these trust services.

Website authentication

The Regulations contains further requirements regarding website authentication. Website authentication provides electronic means by virtue of which the visitor may be assured that there is a genuine and legitimate entity standing behind a given authenticated website. This is an essential service which substantially contributes to the building of trust and confidence in the online business environment amongst Member States. The Regulation emphasizes that the provision and the use of website authentication remains entirely voluntary. Notwithstanding, in order to guarantee better user experience and to boost the trust on the European digital single market, service providers which are involved in providing website authentication are subjected to a set of minimal security and liability obligations laid down by the Regulation.

Electronic documents

Lastly, with regard to electronic documents, the Regulation reiterates their valid legal effect which is deemed to be equal to the effect of regular documents. In essence, the Regulation makes a step further towards an easier, more efficient, workable and up-to-date document turnover across the EU digital single market by prohibiting that electronic documents are denied legal effect and

admissibility as evidence in legal proceedings merely because of their electronic form.

3. PROCEDURAL APPROACH

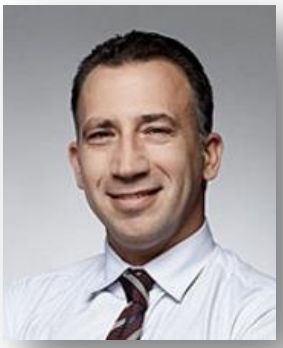
It is noteworthy that the Regulation's added value and contribution to the development of the European digital single market may be grasped not only throughout the legal innovations it brings in substance to the EU legal framework but also through its methodological and procedural approach with regard to the adoption, enforcement and application of its rules. In order to complete some technical tasks in an adaptable and rapid manner, the European legislator has delegated to the European Commission the power to adopt secondary legislative acts. Secondary legislative acts, conferred to the European Commission, may be delegated acts or implementing acts. In accordance with Article 290 of the Treaty on the Functioning of the European Union (TFUE), Regulation No 910/2014 provides for the adoption by the Commission of one delegated act. This power, conferred to the Commission, relates exclusively to the establishment of criteria to be met by the appointed by Member States private or public bodies in charge of the certification of qualified electronic signature creation devices. A lot more numerous, namely 28, are the implementing acts that the Commission has been given powers to adopt. As scheduled, several implementing acts have already been adopted by the Commission, with regard to electronic identification (on aspects relating to the procedural arrangements for cooperation between Member States on electronic identification; the interoperability framework; the minimum technical specifications, standards and procedures with regard to assurance levels) and to trust services (on aspects of the electronic signature and seals formats to be recognized by public sector bodies; of the technical specifications and formats of trusted lists; and of EU trust mark for qualified trust services). This delegation of powers towards the European Commission, in some limited, mainly technical domains seeks to lighten the legislative burden and to ensure that, throughout the work of the Commission, international standards and technical specifications will be taken into due account.

Additionally, the Regulation provides for a transitional period between its adoption and the entry into force of its provisions. In a pursuit of legal certainty for market operators, users and public bodies, provisions regarding issues previously regulated under the E-Signature Directive or with respect to certificates and devices issued under the terms of the latter will enter into force not earlier than mid-2016, when the directive will be considered effectively repealed and non-applicable. Until then, secure signature creation devices the conformity of which has been determined according to the terms of the Directive will be considered as qualified electronic signature creation devices under the Regulation. Similarly, qualified certificates issued to natural persons under the Directive will be considered as qualified certificates for electronic signatures under the Regulation.

The Regulation will start applying as of 1st July 2016. The voluntary recognition of electronic identification schemes may begin as from the end of 2015 and the mandatory cross-border recognition of these schemes is scheduled for September 2018.
And although a few more years remain until we see the widespread effect of the notorious innovation brought by Regulation No 910/2014 and the full application of its provisions, its mechanisms are already raising.

Contacts

Prof. Dr. George Dimitrov
Dimitrov. Petrov & Co. Law Firm
28 Todor Alexandrov Blvd., fl.7
1303 Sofia, Bulgaria
Tel.: +359 2 421 42 01
Fax: +359 2 421 42 02
Email: george.dimitrov@dpc.bg
Website: http://www.dpc.bg



Svilena Dimitrova
Dimitrov. Petrov & Co. Law Firm
28 Todor Alexandrov Blvd., fl.7
1303 Sofia, Bulgaria
Tel.: +359 2 421 42 01
Fax: +359 2 421 42 02
Website: http://www.dpc.bg
Email: svilena.dimitrova@dpc.bg