ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Gregušová, Daniela; Halásová, Zuzana; Peráček, Tomáš

Article

eIDAS regulation and its impact on national legislation: The case of the Slovak Republic

Administrative Sciences

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Gregušová, Daniela; Halásová, Zuzana; Peráček, Tomáš (2022) : eIDAS regulation and its impact on national legislation: The case of the Slovak Republic, Administrative Sciences, ISSN 2076-3387, MDPI, Basel, Vol. 12, Iss. 4, pp. 1-18, https://doi.org/10.3390/admsci12040187

This Version is available at:
https://hdl.handle.net/10419/275457

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/4.0/

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

administrative sciences

MDPI

Article

eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic

Daniela Gregušová [1], Zuzana Halásová [2] and Tomáš Peráček [3,*]

[1] Independent Researcher, 811 02 Bratislava, Slovakia
[2] Cyber Security, Ministry of the Interior of the Slovak Republic, 812 72 Bratislava, Slovakia
[3] Faculty of Management, Comenius University Bratislava, Odbojarov 10, 820 05 Bratislava, Slovakia
* Correspondence: tomas.peracek@fm.uniba.sk

Abstract: The eIDAS Regulation has become a key and, in a way, a ground-breaking piece of legislation of the European Union. It is crucial, in particular, with regard to its ambitious objectives and ground breaking because it was adopted at a time when the Member States of the European Union already had this issue more broadly or narrowly regulated by national laws. In our scientific study, we focus primarily on the critical analysis of the adopted eIDAS Regulation, its impact on the existing e-signature legislation and the amendments adopted, which are necessary to unify the legal framework for electronic signature of the Member States of the European Union. Our main objective was therefore to analyse the legal aspects of the electronic signature. We draw attention to those areas which, because of the regulation adopted, had to be recast and incorporated into the new Trust Services Act, as it emerged from the eIDAS Regulation for us. When processing the topic, we used legal analysis, compliant and available scientific methods as well as selected application problems from practice. In researching and developing a new legal framework for the electronic signature, we also used scientific and doctrinal interpretations associated with the application of scientific and scientific literature contained in the Web of Science and Scopus databases. The results of the study indicate that, despite the multi-annual effectiveness of the eIDAS Regulation, there are still problems that need to be addressed by amending it.

Keywords: eIDAS; electronic signature; European Union; public administration

check for updates

Citation: Gregušová, Daniela, Zuzana Halásová, and Tomáš Peráček. 2022. eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic. *Administrative Sciences* 12: 187. https://doi.org/10.3390/admsci12040187

Received: 24 November 2022
Accepted: 5 December 2022
Published: 6 December 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The electronic IDentification And Services (eIDAS) is Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services in the internal market and repealing Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (European Parliament and Council 1999, 2014). According to Ravšelj et al. (2022), the eIDAS Regulation completely replaces the Directive as well as a substantial part of the legislation contained in the conditions of the Slovak Republic in Act No 215/2002 Coll. On the electronic signature, as amended, and in the relevant decrees of the National Security Authority, which implemented this Directive. The eIDAS Regulation has been applicable throughout the European Union as well as in the Slovak Republic since 1 July 2016. As stated by Jankelova et al. (2021) in the Slovak Republic, in addition to the eIDAS Regulation, special Act No 272/2016 Coll. on trust services for electronic transactions in the internal market, as amended, also regulates the area of trust services, which entered into force on 18 October 2016 (National Council of the Slovak Republic 2016).

As follows from paragraph 2 of the preamble of this regulation, "its aim is to strengthen trust in electronic transactions in the internal market by ensuring a common basis for secure electronic interactions between citizens, businesses and public administration bodies, thereby increasing the effectiveness of public and private online services, e-business and

e-commerce in the Union" (European Parliament and Council 2014). As indicated by Handrlica (2019) and Jankelova and Masar (2021), the adoption of the eIDAS Regulation also in the light of the existing electronic signature legislation in the Slovak Republic and the existing Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (hereinafter referred to as the "Electronic Signatures Directive") pursued a number of objectives. According to Malatinec (2017) and Vel Vel Kalisz (2021), it was necessary to highlight the impact of the eIDAS Regulation on the already existing and functioning provider environment, the benefits it will bring to users themselves (citizens, entrepreneurs and public administrations) and what new services and obligations the Regulation has introduced. These were issues that had to be addressed in the context of the adoption of the eIDAS Regulation when it was applied to the legal order of the Slovak Republic.

Despite the fact that the eIDAS Regulation has been in force for six years, its importance remains "around the door" according to Alimehaj et al. (2021). In our view, the lack of interest in researching this particularly topical topic by legal theorists is, in our opinion, a serious problem that we would like to eliminate at least in part by this scientific study. This view is also based on research in the Web of Science and Scopus databases, which contain relatively few records with the keyword "eIDAS".

From the point of view of systematics, our scientific study is divided into five parts, each focusing on selected issues. In the individual sections, we pay attention to the eIDAS Regulation itself. In the introduction, we explain the importance of our chosen topic. Within the theoretical basis, we present the opinions of selected experts. According to the title of the scientific study, in addition to the analysis of the eIDAS Regulation, it is also the subject of our examination of its impact on the development of the Slovak legislation. We have divided the fourth focus chapter into several parts, where we pay attention to several questions. These are, for example, individual types of electronic signatures, the Electronic Signature Act of 2002, and the related Act on Trusted Services for Electronic Transactions in the Internal Market. This chapter also includes the supervision of administrative authorities. We also devote some scope to the legal regulation of the use of identity cards with chips, which represent the practical impact of the eIDAS Regulation on streamlining public administration's activities in the context of its electronicisation. Beside the method of analysis, we use also the synthesis as a process of combining the results of multiple primary research aimed at testing the same conceptual hypothesis. As part of the complexity of our research, we also use the comparative method. As a crucial part of comparative method, we analyse the development of the Czech legislation, and we compare it to the Slovak legislation.

2. Literature Review

As stated by Funta and Ondria (2021), the adoption of the eIDAS Regulation marked a shift in the development of online transactions and in increasing the credibility of electronic communications within the European Union. This Regulation replaced Directive 1999/93/EC of the European Parliament and of the Council, which was the first attempt to regulate electronic signatures across borders. The basic objective of the eIDAS Regulation is according to paragraph 2 of the preamble to provide citizens, entrepreneurs as well as national authorities of the Member States with a common legal basis for secure electronic communications that would increase the credibility of electronic transactions in the internal market of the European Union and thus make more active use of them. According to Handrlica et al. (2022), it is precisely the inconsistency of national regulations in this area that hinders the development of the digital economy, including new products and services on the market. In addition to simplifying trade, the eIDAS Regulation also seeks to provide European Union citizens with an efficient and effective tool to use the online services offered by Member States, including by ensuring cross-border access to them. Alonso et al. (2020) considers that, in order to achieve the above objectives, the eIDAS Regulation regulates the conditions for the mutual recognition of a means of electronic identification

of legal and natural persons between Member States, while at the same time setting up a legal framework for the different means of identification, namely electronic signatures, electronic seals, electronic time stamps and web authentication services, together with electronic registered delivery.

As further noted by Berbecaru and Lioy (2018), according to paragraph 12 of the preamble in the case of the mutual recognition of electronic identification means, the eIDAS Regulation introduces an obligation for Member States to accept electronic identification means issued by other Member States when accessing an online service. In other words, where a Member State offers its citizens certain online services requiring electronic identification, that Member State must also recognise, for the purposes of cross-border identification, the electronic identification methods (options) established in another Member State (Cirlig 2016). This view is shared by Erdogan and Saran (2021), pointing out that the mutual recognition obligation is limited to those electronic identification means that meet the requirements set out in Article 6 of the eIDAS Regulation (included in the list published by the Commission, assurance level equal to or higher). According to Berbecaru et al. (2019), the first precondition that an electronic identification means must fulfil in order to be recognised on the territory of another Member State is a sufficient level of guarantee for that means, which must be at least significant or high. In the event of a low level of guarantee, it is left to the discretion of each individual Member State to accept such a means of identification or not.

The second requirement then, according to Maliappis et al. (2019), is that the electronic identification means has been notified to the European Commission and subsequently published in the Official Journal of the European Union. Publication shall be preceded, first, by the communication of all the documentation and schemes relating to the means in question and, on the one hand, by its assessment by the European Commission and by experts from each Member State. Only after a thorough evaluation of the funds' compliance with all the requirements laid down in the eIDAS Regulation can they be published in the Official Journal of the European Union according to Bodea and Purnus (2018).

Pelikánová and Cvik (2019) is of the opinion that the obligation of mutual recognition of electronic identification means that successfully undergoing the above procedure is imposed by the eIDAS Regulation only on public authorities of the Member States. Private legal persons and natural persons are not bound by this obligation and can therefore continue to decide for their own purposes whether or not to use the electronic identification means thus determined. The second theme covered by the eIDAS Regulation, especially starting with Article 3, is the uniform regulation of electronic signatures, electronic seals, electronic time stamps, electronic recommended delivery services and authentication of electronic pages. The basic premise of the eIDAS Regulation is that all electronic identification means referred to above must not be denied their legal effects and at the same time not be refused as evidence in judicial and administrative proceedings in the Member States solely because, according to Chochia and Nässi (2021), they are electronic.

Authors other than Schmidt et al. (2021) believe that, as a new institute, the eIDAS Regulation defines so-called Conformity Assessment Bodies (CABs), whose task is to assess the above-mentioned electronic services offered by national providers for their compliance with the eIDAS Regulation. If the services they offer meet all the requirements of the eIDAS Regulation, these providers may be included in the list of qualified trust service providers. This should, according to Sararu (2017), enhance trust in the cross-border use of electronic identification, as the services provided by qualified providers comply with European standards. The eIDAS Regulation, as a whole, places the greatest emphasis on services based on qualified means (use of qualified electronic signatures or qualified seals, etc.). According to several authors such as Pavelek and Zajíčková (2021), services using qualified means are better protected against unauthorised use, in particular because the cryptographic key of the service cannot be exported from a qualified means and make a copy of it. This, in their view, ensures a greater level of safety and control of the use of

qualified resources. Currently, qualified means can be found mainly in the form of USB tokens or smart cards.

3. Results

3.1. The eIDAS Regulation

In particular, the subject matter of the eIDAS Regulation is the area of rules for trust services; in particular, services for the creation, validation and validation of electronic signatures can be considered key. According to Article 3(16) of the eIDAS Regulation, an 'trusted service' is an electronic service, which is generally provided for remuneration and consists of:

1. The production, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
2. In the production, verification and validation of certificates for website authentication; or
3. The storage of electronic signatures, seals or certificates related to these services.

The issue of electronic signatures, both within the European Union and within individual Member States, is not a new topic. In order to understand the historical context and to improve orientation in this area, it is necessary to state the main reasons why part of the issue already regulated within the European Union (e-signature directive and national transposition laws on electronic signature) is now regulated by another legal instrument of European law, which is the eIDAS Regulation.

The eSignature Directive was adopted in 1999 and set out the legal framework for the use of electronic signatures. It was based on the principle of technological neutrality, because it did not explicitly talk about any particular technology. It has put in place a system of supervision and control of certification service providers as well as an institution verifying the correctness of electronic signature creation devices. A key provision was the equalisation of a guaranteed electronic signature with a handwritten signature. The eSignature Directive has been transposed into our legal order by Act No 215/2002 Coll. on electronic signature and amending certain acts, which also amended related legislation, particularly in relation to the legal effects of electronic signature (National Council of the Slovak Republic 2002). Following the transposition of the eSignature Directive, the European Commission carried out an evaluation of its implementation. As Dumortier et al. (2003) points out, this very detailed report found that almost all Member States had taken steps towards legal acceptance of electronic signatures. However, the very nature of the directive was problematic because a directive as a legal act, unlike a regulation, is not a legislative act of general application and is binding only in light of the objective to be achieved, the form and manner of which it is for the Member State to decide. This caused almost all Member States to declare full transposition of the eSignature Directive, but its implementation across Member States was so different that it was a frequent source of incompatibilities. The difference concerned in particular:

- The conditions for international recognition of guaranteed/qualified electronic signatures;
- The degree of safety;
- The obligation to use secure products or applications for the creation of electronic signatures, etc.

In particular, the issue of the mutual cross-border recognition of electronic signatures was only at the level of science fiction, thus increasingly closing national markets and national environments. The eSignature Directive only laid down minimum criteria and allowed Member States to adopt a number of exceptions (e.g., for the use of electronic signatures in national/public administrations), which caused national measures to create de facto barriers to the mutual recognition (interoperability) of electronic signatures across the European Union, as well as to electronic identification, e-authentication and related

trust services. The Directive is a legal instrument in this area, as addressing this issue has been assessed as insufficient and, in particular, it has been replaced by the directly applicable eIDAS Regulation for the reasons set out above.

According to Chochia and Nässi (2021), the main objective of the eIDAS Regulation was therefore to increase trust in pan-European electronic transactions as well as to ensure cross-border recognition of electronic identification, authentication, signature and related trust services for legal purposes, on the one hand, as well as to ensure a high level of data protection and consumer involvement in the internal market. The Regulation is formally divided into five chapters, but from the point of view of the already existing legislation in national law, we consider two chapters to be the most important: electronic identification (Chapter II) and trust services describing electronic delivery and electronic signature (Chapter III).

The eIDAS Regulation should significantly remove obstacles to the functioning of the internal market so that citizens, businesses and authorities can benefit from the mutual cross-border recognition of electronic identification, authentication, signature and other trust services. After an in-depth analysis of the Regulation and the related adoption of Act No 272/2016 Coll. on trust services for electronic transactions in the internal market and amending certain acts (the Trust Services Act), as amended, we are of the opinion that the adoption of the Regulation was the most appropriate legal instrument on the basis of which it applies directly and has become directly binding on all Member States of the European Union (National Council of the Slovak Republic 2016). This has reduced legal fragmentation and thus provides greater legal certainty. The eIDAS Regulation therefore focused directly on cross-border aspects of electronic identification and did not already address the issuance of electronic identification means, which it thus retained as a "exclusive prerogative of Member States".

As stated by Nováčková and Vnuková (2021), the regulation is legally binding and directly applicable with immediate effect. General binding means that it is a general normative act in force in all Member States. Direct applicability means that the regulation is not transposed into law (in law); it is directly applicable and thus automatically becomes part of the national legal order as if it were adopted by the legislative authority of a Member State. The eIDAS Regulation also under Poiană (2017) lays down rules for the provision of trust services for electronic transactions in the internal market, classifying services provided for electronic signatures and defining some new trust services that did not exist so far in all Member States. These include, in particular, services for the creation, verification and validation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and services for the production, verification and validation of certificates for website authentication and the conditions under which Member States certify and recognise devices for the creation of a qualified electronic signature and recognise the means of the electronic identification of natural persons and legal persons that are part of a notified electronic identification scheme of another Member State. According to Kutyłowski and Błaśkiewicz (2023), that regulation also defines the conditions under which Member States recognise means for the electronic identification of natural and legal persons issued by other Member States.

3.2. Types of Electronic Signature

According to the security level, the eIDAS Regulation defines several types of electronic signatures:

- Electronic signature,
- Advanced electronic signature,
- Advanced electronic signature based on a qualified certificate, and
- qualified electronic signature.

To explain the difference between those types of electronic signatures, it is necessary to compare the legal definitions laid down in eIDAS Regulation (especially Section 4 Article

25 et seq) and to consider the legal value of each. There are four levels of the e-signature within eIDAS Regulation, each associated with different legal values.

An electronic signature is the basic level and is defined as: Data in electronic form, which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Simple electronic signature has a very low level of complexity, which makes it widespread and easy to adopt. Just a few examples to imagine of what a simple electronic signature can be: an email footer, a scanned image of the handwritten signature sent by email, the tick used to accept the Terms and Conditions of a website when logged in the account, etc. Unsurprisingly, this form of electronic signature does not present a great level of trustworthiness in case of litigation. This form of electronic signature cannot guarantee that the person signing the document is who he pretends to be. Moreover, the judge cannot rule it out as evidence just because it is a simple form, but can be required to back it up with other proofs.

The advanced electronic signature as a second type and second level is more secure and reliable than the simple one. For an electronic signature to be considered as advanced, it must meet several requirements, as laid down in article 26 of eIDAS Regulation:

- It is uniquely linked to the signatory;
- It is capable of identifying the signatory;
- It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Advanced electronic signature is able to guarantee that the signatory is who he says he is. In addition, this type of electronic signature is created with the help of a device in the sole possession of the signatory, adding an extra layer of security. The documents signed with an advanced electronic signature are also fairly protected, as the providers use encryption technology to protect the data. Finally, the advanced electronic signature enjoys a greater level of confidence compared to the simple one. In the case of litigation, it is up to the claimant to demonstrate its validity.

An advanced electronic signature based on a qualified certificate is the intermediate solution between the advanced signature and the qualified signature. This procedure requires face-to-face verification (physically or remotely) of the identity of the signer and can be used in specific cases.

The qualified electronic signature is the most advanced level of electronic signature security. Due to the definition of a qualified electronic signature laid down in Article 3 (12) of the eIDAS Regulation, a qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device (QSCD), and which is based on a qualified certificate for electronic signatures. Its legal effect is equivalent to a handwritten signature, whereas the other levels of electronic signature have a probative value. It is thus legally recognised in all the Member States of the European Union, not only in the Slovak Republic.

Průša (2015) claims that a qualified electronic signature guarantees the highest level of security. It is an electronic signature created by a natural person using electronic signature creation data (private key) that is securely stored in a qualified electronic signature creation device. The private signature key is issued with the corresponding public key for which, according to Mocanu et al. (2019), a qualified certificate has been issued to validate the qualified electronic signature as well as to prove the identity of the signatory's person. A qualified certificate may be issued only by the provider of a qualified trust service for the production and validation of certificates. Only a qualified electronic signature confers equivalent legal effect on a qualified electronic signature with a handwritten signature without the need for further examination, and this electronic signature must be recognised in all Member States. For this purpose, the eIDAS Regulation created the conditions for mutual recognition of the key cross-border means of communication such as electronic identification, electronic documents, e-signatures and electronic delivery services. The

eIDAS Regulation entered into force on 1 July 2016 and on that date the provisions relating to trust services became directly applicable and directly binding in all 28 Member States of the European Union.

According to Article 3(9) of the eIDAS Regulation, the signatory is exclusively the natural person who creates an electronic signature. Therefore, an electronic signature can only be created by a natural person who is the only one capable of expressing his will. This is a fundamental difference compared to the eSignatures Directive, where the electronic signature served as a means of authentication rather than allowing the use of an electronic signature by a legal person. To compare it to the previous legislation, as from the entry into force of the eIDAS Regulation, the issuance of a certificate for a legal person will be inadmissible. The signatory who creates an electronic signature is exclusively only a natural person. For legal persons, the eIDAS Regulation therefore introduces the new procedure, the so-called electronic seal, and the entity who creates an electronic seal is called a creator of the seal.

As is apparent from paragraph 59 of the preamble to the eIDAS Regulation, electronic seals are generally intended to serve as evidence that an electronic document has been issued by a legal person and to ensure certainty as to the origin and integrity of the document. As stated by Sararu (2016) of Article 35(2) of the eIDAS Regulation, two legal presumptions apply when using a qualified seal and the legal effects of such use. The first is the presumption of data integrity, i.e., that the electronic document to which the electronic seal is attached has not been altered. The second legal presumption is the presumption that the origin of the data is correct, which means that it comes from the legal person to which the qualified electronic seal is linked. An electronic seal certificate may only be issued to a legal person. Therefore, the electronic seal must not be understood as an electronic signature of a legal person.

For the first time in the history of European law, we are confronted with a provision concerning the prohibition of discrimination against electronic documents. This means that the legal effects of an electronic signature, an electronic seal, an electronic time stamp and data transmitted and served through an electronic registered delivery service and their admissibility as evidence in legal proceedings may not be refused solely on the grounds that they are in electronic form or do not comply with the requirements of the eIDAS Regulation. In order to contribute to the general cross-border use of trust services, it should be possible to use them as evidence in judicial proceedings in all Member States.

3.3. The Electronic Signature Act

As mentioned in the introduction, Act No 215/2002 Coll. on electronic signature and amending certain acts was adopted in the Slovak Republic in 2002 (National Council of the Slovak Republic 2002). Its main objective in the period of the evolving information society was to simplify the conditions for electronic communication and e-commerce, while at the same time ensuring equal treatment of the classical paper document with the electronic document. Since its entry into force, social needs have required a number of amendments. As stated by Horváthová and Čajková (2019), the explanatory memorandum to the proposed amendment to the Act on Electronic Signatures for the main intention to amend the Electronic Signatures Act provides an assessment of the practical experience of using the electronic signature for the last five years, as well as the continuous development of information technology. In the context of the involvement of the Slovak Republic in the initiative "Europe" and the "eEurope+" action plan, as well as the need to extend the use of electronic signatures in the field of public administration, it was necessary, following some experience, to adopt a number of substantial modifications to the existing eSignature Act.

In our view, these can be summarised in four main areas of problems:

1. The amendment to the Electronic Signature Act reacted to the problems most frequently encountered since the adoption of the E-signature Act in 2002,
2. The need to modify and supplement the terms (terminology) in the e-signature Act,

3. further define the status of the National Security Office as the central government authority for electronic signature and extend its tasks,
4. Modify the Authority's procedure for assessing the conformity of safe devices for producing and verifying a guaranteed e-signature with safety requirements and setting a time limit for decision-making.

In order to understand the decisive reasons relating to the amendment of the Electronic Signatures Act, these were some essential elements, which the law confers on the signature in legal practice. It should also be noted that in the current period, electronic signatures are still a specific category of signatures. In particular, its position and role in the information society gave rise to the adoption of a specific law on the electronic signature. Section 40(3) and (4) of Act No. 40/1964 Coll. The Civil Code, as amended (hereinafter referred to as the "Civil Code") provides that is valid if it is signed by the acting person; if a legal act is performed by several persons, their signatures do not have to be on the same document, unless the law provides otherwise (National Assembly of the Czechoslovak Socialist Republic 1964). The signature may be replaced by mechanical means in cases where this is customary. The legal meaning of the signature derives from the provisions of section 40(3) of the Civil Code itself, since the validity of a written legal act requires the signature of the person acting. In the sense of the above, we thus certify by signing a certain legal act or legal act. As further pointed out by Žofčinová et al. (2022), although the civil law is based on the principle of non-formality of legal acts made either explicitly, i.e., orally or in writing, or in an unspeakable manner (inclusively), in some cases, in particular where there are serious legal consequences with the legal act. The Civil Code also requires a form of such a legal act for the validity of a legal act, either in writing or even a notarial deed of a legal act. For the validity of a written legal act, the signature of the person acting is also required. Written form is required by law, e.g., for transfers of real estate but also in other cases, explicitly mentioned by law. Failure to comply with the legal form of a legal act renders it null and void. Skora et al. (2022) emphasise that the absolute nullity of a legal act occurs directly by law (ex lege) and operates from the outset (ex tunc) against everyone. This is not time-barred or extinguished because such an act does not result in legal consequences, either through additional approval (ratihabion) or by the absolution of a defect in the expression of will (convalidation). As Funta and Káliková (2022) points out, the validity of the written form of a legal act does not only mean capturing the content of the legal act and determining the person who made the legal act, but also requires the signature of the person acting, since such a form of legal act is valid only by the signature of the person acting. Distribution over electronic communications networks is envisaged for the processing of electronic documents as well as for their handling. From the point of view of the complete electronicisation of the administration and the legal acts associated with this, the identification of communicating parties and the authentication of electronic documents are also included. It is in this process that electronic signature plays a crucial role, using which we can reliably create an adequate level of security for communicating parties within electronic communications.

3.4. Law on Trust Services for Electronic Transactions in the Internal Market

Act No 272/2016 Coll. on trust services for electronic transactions in the internal market and amending certain acts entered into force on the day of its publication in the Collection of Acts of the Slovak Republic, i.e., 18 October 2016. On that date, on the basis of section 19(1), it repealed Act No 215/2002 Coll. on electronic signature and amending certain acts, as amended (National Council of the Slovak Republic 2016). It represents the so-called implementing legislation and is intended to "supplement" the eIDAS Regulation. It addresses and regulates only those parts of the eIDAS Regulation that have become applicable since 1 July 2017, that is, the issue of trust services, or, if we are to be terminologically precise, trust-creating services. The law supplements the eIDAS Regulation only in those parts which are entrusted to the exclusive competence of the Member State.

According to Troitino et al. (2020), some legal institutes introduced into European law by the eIDAS Regulation are completely new in the European Union environment. However, they are nothing new in the legal order of the Slovak Republic, since they have already been regulated by existing legislation (time stamps, guaranteed electronic seals, etc.). We can therefore conclude that, in the adaptation of certain institutes, the Slovak Republic also exceeded the eIDAS Regulation in time. Where deviations from European legislation have been recorded, corrections and amendments have been made by the Trust Services Act so that the Slovak national legislation does not conflict with the directly enforceable eIDAS Regulation. Otherwise, the eIDAS Regulation would take precedence over the laws of the Slovak Republic.

The Trust Services Act amends the terminology previously introduced into the legal order of the Slovak Republic, namely the Electronic Signature Act. The Trust Services Act, in accordance with the rules for the implementation of generally binding acts of the European Union, does not contain a provision defining and defining the terms used by the eIDAS Regulation. The basic concepts also used by the Trust Services Act are defined in particular in Article 3 of the eIDAS Regulation and their definition has been resolved by reference to the eIDAS Regulation.

By adjusting the terminology, the term "guaranteed electronic signature" is changed in the Slovak legal order to the term "qualified electronic signature", while the technical implementation procedure is maintained. It is complemented by an additional possibility where qualified trust service providers managing data for the creation of a qualified electronic signature on behalf of the signatory may reproduce the qualified electronic signature creation data only for backup purposes. The legal effects of such a signature in the Civil Code are maintained. Similarly, by adapting the terminology, the term 'guaranteed electronic seal' is changed to 'qualified electronic seal' and 'time stamp' to 'qualified electronic timestamp'. In these cases, they were de facto only terminological changes, without altering their content, which was retained. Given that the Slovak Republic already had legislation on this substantive issue prior to the entry into force of the eIDAS Regulation and before the entry into force of the Trust Services Act, it was necessary to adopt transitional provisions in order to ensure a smooth transition to the new legal regime.

3.5. Institutional Framework and Designation of Supervisory and Conformity Assessment Bodies

From an institutional point of view, the Trust Services Act designated the National Security Office as the supervisory body under the eIDAS Regulation. In addition to exercising supervision, the Office grants so-called qualified statuses to qualified trust service providers, issues and revokes certificates to them. It further certifies qualified electronic signature and seal creation devices, maintains and updates trusted lists of trust service providers and is also a contact point for the European Union.

The provision of Article 20 paragraph 1 of the eIDAS Regulation determines the obligation of the administrative authority for conformity assessment to conduct audits of qualified trusted service providers at their own expense at least every 24 months. According to Stancetic (2020), the purpose of the audit is to confirm that the qualified service providers are trustworthy and the qualified trust services they provide meet the requirements set out in this regulation. Qualified trusted service providers shall submit the resulting compliance assessment report to the supervisory authority within three working days from its delivery. However, according to Troitino et al. (2017), it is not clear from the point of view of the institutional framework and the responsibilities entrusted to the exclusive competence of the Member States, for example, which body in the Slovak Republic is a conformity assessment body under Article 20 of the eIDAS Regulation. We consider this to be a significant lack of regulation, which renders some of the provisions of both the eIDAS Regulation and the Trust Services Act unenforceable. The conformity assessment body is a body defined in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No

339/93 (European Parliament and Council 2008). It is a body that is accredited as competent to carry out the conformity assessment of the qualified trust service provider and the qualified trust services provided by it. The accreditation scheme for the accreditation of these bodies is being developed at a European level, but it is not yet clear when it will be completed. Conformity assessment bodies should be accredited by national accreditation authorities.

The time necessary for the actual accreditation of conformity assessment bodies will take some time to verify whether the conformity assessment body is competent under Vogt (2016) to carry out a conformity assessment on qualified trust service providers. This is the time needed to establish a conformity assessment body. The conformity assessment body is to carry out audits of qualified trust service providers to confirm whether the qualified trust service providers and the qualified trust services they provide meet the requirements set out in the eIDAS Regulation. The time needed to carry out the audit itself by the conformity assessment body and the time needed for the supervisory body to verify the outcome of the audit, i.e., whether the trust service provider and the service provided by it comply with the requirements of the eIDAS Regulation for a qualified provider and for a qualified trust service, will also take a significant time. The above-mentioned absence of a conformity assessment body creates a deadlock, in which no candidate for the qualified provision of trust services is in a position to submit to the supervisory body the resulting conformity assessment report, since there is no body in the Slovak Republic designated as a conformity assessment body and accredited in the manner described above. This caused significant problems, in particular after 1 July 2017. On the basis of the transitional provisions of the Trust Services Act, an accredited certification service provider accredited under the existing Electronic Signatures Act is considered to be a qualified trust service provider to which the Office has granted "qualified status providing a qualified trust service". However, such a provider shall submit a conformity assessment report from the conformity assessment body to the Authority by 1 July 2017 at the latest. In the absence of a report, its status as a trust service provider with qualified status providing a qualified trust service expired on 2 July 2017. There was a real risk that, as of 2 July 2017, a trust service provider with qualified status would not be able to provide or use any trust service in the Slovak Republic.

3.6. Use of Electronic Signature in Contact with Public Authorities

According to Kusber et al. (2020), the eIDAS Regulation left to the discretion of the Member States of the European Union what kind of electronic signature they would require for online public services or transactions (under the conditions of the Slovak Republic, understood as a "guide with public authorities"). Certain restrictions are provided only if an advanced electronic signature is required. In that case, according to Article 27(1) of the eIDAS Regulation, it must also recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures and qualified electronic signatures. Where an advanced electronic signature based on a qualified certificate is required for these public services, it shall also recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures from other Member States. The main principle is that if a certain type of electronic signature is required, an equivalent species must always be recognised, or even higher from other Member States. Member States shall thus not require for cross-border use of the online service offered by a public sector body an electronic signature of a higher level of security than a qualified electronic signature.

3.7. Use of Qualified Certificates within eID in Contact with Public Authorities

Slovak citizens may use the eID card for identification and authentication and for storing and renewal of qualified certificates and creation of a qualified electronic signature. The qualified electronic signature functionality in the eID may be activated upon the citizen's request either during document pick-up or later at a registration authority office.

ID card with electronic chip—a new type of identity card with an electronic chip that has been issued since December 2013. As stated by Šindleryová (2022), it serves, as before, to prove the identity of a citizen of the Slovak Republic in personal contact with authorities and institutions. It also includes an electronic chip. This makes it possible to prove the identity of a citizen in an electronic environment when using e-Government services. Slovak eID can also be used on foreign portals.

As part of the e-government process, e-Government services will be gradually made available to citizens via the Internet. E-services to which a citizen can access are, for example: reporting changes, filing requests, complaints, actions, auctions, public procurement, cadastre services, tax office services, eHealth, eVoting, etc. An essential and necessary requirement for access to electronic services is the unambiguous identification of a person and, consequently, his or her authentication. An ID card with an electronic chip is a trustworthy and secure carrier of the citizen's identification data, i.e., his or her electronic identity.

Act No 305/2013 Coll. on the electronic form of the exercise of the powers of public authorities and amending and supplementing certain acts (the e-Government Act), as amended ('the e-Government Act'), defines the concept of electronic identity of a person for the purposes of electronic communication and access to public administration information systems (National Council of the Slovak Republic 2013). It is a set of characters that are recorded in electronic form and which clearly distinguish one person from another, the electronic identity of the person is demonstrated by the identification of the person and verified by his/her authentication. The identification of a person is further demonstrated by the name and surname of the person in combination with his/her birth number (person identifier). Authentication is the process of verifying the identity of a person by a public authority. Only an electronic chip ID card (eID) and a security personal code (BOK) may be used to authenticate a person.

The ID card on the back is equipped with an electronic contact chip in which the data on the identity card (name, surname, residence, date of birth, etc.) are stored. A citizen under the age of 65 is obliged to choose his/her security personal code—BOK when applying; other citizens can do so or choose to do so at a later stage, e.g., when taking an identity card or at any time during its validity period. A security personal code is a combination of six arbitrary digits. According to Mucha and Mocarnikova (2018), a citizen is not obliged to use the available electronic services by issuing an identity card with a chip and entering a security personal code, only giving him the opportunity to communicate electronically. If the security personal code is not used by the citizen, it can be blocked at any time. In case it plans to use an ID card with a chip to access electronic services, it needs computer software and a contact smart card reader in addition to the card itself. The software can be downloaded free of charge from the portal of the Ministry of Interior of the Slovak Republic or from the Central Portal of Public Administration. Drivers to the card reader are obtained directly from the manufacturer of the reader.

When issuing an identity card with a chip, the citizen can apply for free of charge to upload three certificates, which will be stored on the electronic chip of the identity card. It is a qualified certificate (ACA), through which it is possible to create a qualified electronic signature (KEP, originally used as a ZEP advanced electronic signature), a certificate (PCA), which is used for signature by electronic signature and an encryption certificate (SCA). KEP PIN (six-digit code) and KEP PUK (eight-digit code) must be selected for signature certificates. Uploading these certificates is already possible online via the eID client application without the need for a personal visit to any department of documents, you just need to know your BOK. As stated by Peracek et al. (2021), users are always advised not to use PCA and SCA certificates when communicating with public authorities, as they cannot create a qualified electronic signature. Only an advanced electronic signature can be created through the PCA certificate, which is not accepted as a valid authorisation under the e-Government Act.

In order to create a qualified electronic signature for electronic submissions made via the portal www.slovensko.sk, it is necessary to have a freely accessible application D.Signer/XAdES installed in addition to the corresponding qualified certificate on the identity card. For the creation of a qualified electronic signature of attachments for electronic submissions, the attachments can be signed or signed attachments viewed and validated for information, e.g., by a free QES application.

3.8. EIDAS Regulation and Its Application in Legislation of the Czech Republic

As mentioned above, the eIDAS Regulation entered into force throughout the European Union on 1 July 2016 (European Parliament and Council 2016). Although a European Union Regulation is a legal act which is binding and directly applicable in each Member State and therefore does not require the adoption of further legislation, a number of laws have been approved by the Czech legislature to clarify and transpose the eIDAS Regulation into the legal order of the Czech Republic. As stated by Pelikánová et al. (2019), the First Act was passed following the eIDAS Regulation of Act No 297/2016 Coll. on Trust Building Services for Electronic Transactions ('the Confidential Services Act') (Parliament of the Czech Republic 2016). It modified some of the practices of trust service providers, such as providers of electronic signatures or seals, in particular the process of archiving documents related to the services provided, then the competence of the Ministry of Interior of the Czech Republic under the eIDAS Regulation and, last but not least, the practice of natural and legal persons in the provision of trust-generating services.

According to Dusek (2018), another act was subsequently Act No 250/2017 Coll. on Electronic Identification (hereinafter referred to as the "Electronic Identification Act") (Parliament of the Czech Republic 2017). This legislation focused in particular on a qualified electronic identification system (e.g., eID cards). The Act also addresses issues of how accreditation is granted and the supervision of its operation, which is entrusted to the Ministry of Interior of the Czech Republic, as well as offences in this area. A qualified electronic identification scheme can be imagined as consisting of both electronic identification means and the very system allowing electronic identification. An important provision of that law is Section 2, which reads as follows: 'Where legislation or the exercise of the scope of application require proof of identity, proof of identity using electronic identification can only be made possible by means of a qualified electronic identification scheme'. That provision thus allows the use of electronic identification even where the obligation to identify is required by law, which can be regarded as the cornerstone of the eIDAS Regulation in life. Its application has also encountered several pitfalls in the conditions of the Czech Republic.

As stated in Dusek (2017), in order to give member states the opportunity to sufficiently prepare for the requirements contained in the eIDAS Regulation and to make the necessary not only legislative but also technical changes, Article 52 of the eIDAS Regulation (Effectiveness Regulation) establishes several transitional periods. The problematic transition period expired on 19 September 2018. That date was laid down in Paragraph 19 of the Law on trust-generating services and was intended to serve as a transitional phase for the introduction in the public administration of the exclusive use of qualified electronic signatures based on a qualified means. The Law on Confidence Services in connection with the adoption of the eIDAS Regulation enshrines in its provision § 5 the obligation to use exclusively qualified electronic signatures for signatures by electronic signature, in order to increase the level of protection and credibility of the document bearing such a signature (Simonova and Amare 2019). So far, in addition to a qualified electronic signature, it has also been possible to sign a document with an advanced electronic signature based on a qualified certificate for electronic signatures, but it can no longer be used as of 20 September 2018. The above change and transition to qualified means under the eIDAS Regulation applies not only to electronic signatures, but to electronic seals and time stamps when used within the public administration.

As stated by Průša (2015) to private individuals and legal persons acting legally against the public administration, the possibility to sign electronic documents in both ways, i.e., a

guaranteed electronic signature based on a qualified certificate for electronic signatures or a qualified electronic signature, remains maintained after 19 September 2018. This follows from section 6 of the Confidence Services Act, which both electronic signatures combine under the term "recognised electronic signature".

Another very important milestone was 29 September 2018, with the entry into force of Article 6 of the eIDAS Regulation. This Article governs the mutual recognition of electronic identification means in the case of cross-border use of online services provided by public administrations of the Member States. As mentioned above, the mutual recognition process precedes the assessment and notification process, with the other Member States having 12 months from the date of publication of the notification in the Official Journal of the European Union to prepare their national systems for compatible use with the notified electronic identification means. The public administration of each Member State must then accept identification on the basis of the notified electronic means of identification.

3.9. Electronic ID Cards

Electronic ID card (also "e-OP" or "EOP") has been issued in the Czech Republic since 2012 (Parliament of the Czech Republic 2012). In the view of Handrlica et al. (2022), the legislative framework consists of an amendment to Act No 328/1999 on identity cards, details (requirements for technical translation of photographs, specimens of ID cards, forms and applications) laid down implementing sub-legal regulations. For example, Decree of the Ministry of the Interior of the Czech Republic No. 400/2011 Coll., which implements the Act on Citizenship Cards and the Act on Travel Documents, as amended (Ministry of the Interior of the Czech Republic 2011). In 2018, an e-OP meeting the conditions of the eIDAS Regulation with a new type of chip began to be issued. In this context, however, we must not forget the key Act No 365/2000 Coll. on information systems of public administration, which laid the "cornerstone of the electronisation of the Czech public administration" (Parliament of the Czech Republic 2000) and laid down the rights and obligations of all persons and bodies involved in the development of Public Administration Information Systems.

Since 1 July 2018, so-called electronic identity cards with machine-readable data and contact electronic chip have been issued to citizens of the Czech Republic, which represent the next step towards achieving the objectives of eGovernment (EOP). Unlike the 2012 'electronic identity cards' originally issued, they are already fully eligible for the electronic identification of their holder. They allow both identification in the use of online services and the creation of qualified electronic signatures or authentication of their holder against information systems. Thus, these EPOs already fully fulfil the idea of an identity card as a document through which it is possible to carry out fully online transactions and to act electronically. At the same time, the EPO meets all the requirements of the eIDAS Regulation, with a high level of protection. Electronic identification under the EPO can be used both in dealings with public authorities and in dealings with private entities, as the EPO can be used to electronically identify a natural person in all situations where it is required by law under the Confidence Services Act.

EPO badges automatically include information about the laissez-passer itself, namely the serial number of the license, the date of issue, the end of validity and the identification of the office that issued the EPO. In order to use the holder's electronic identification, it is necessary to activate this service at the office of any municipality with an extended scope. In this case, the data of the holder are uploaded to the EPO, such as first name and surname, gender, nationality, date, place and district of birth, birth number, permanent residence address and marital status. In the case of electronic signature or authentication, it is then necessary to upload an authentication certificate or a qualified certificate to create electronic signatures for a given EPO. Personal codes or PINs that are related to each of the above-mentioned services offered by the EPO serve as a security method. Therefore, according to Tsakalakis et al. (2016), it is essential to know six different numerical codes with 4 to 10 digits for maximum use of the EPO, which may not be considered a user-friendly solution

for the EPO user. The service application in this case is "eObčanka", which allows the use of the above services and at the same time it is possible to manage numeric codes and uploaded certificates.

4. Materials and Methods

As noted by Sararu (2019), public administration is an activity carried out by state authorities, self-governments and public institutions in the performance of public tasks. Its main objective is to work for the public good through the strengthening of civil society and social justice. In our scientific study, we focus primarily on the critical analysis of the adopted eIDAS Regulation, its impact on the existing eSignature legislation and the amendments adopted, which are necessary to unify the legal framework for the electronic signature of the Member States of the European Union. Our main objective was therefore to analyse the legal aspects of the electronic signature. We draw attention to those areas which, because of the regulation adopted, had to be recast and incorporated into the new Trust Services Act, as it emerged from the eIDAS Regulation for us. In order to achieve the main objective, we have also chosen milestones, and namely an analysis of:

- The eIDAS Regulation itself and the modification of the electronic signature contained therein,
- Selected Slovak legislation,
- The development of the use of identity cards with electronic chips, and
- Development of electronicisation of Czech legislation and use of electronic identity cards.

At the end of our study, we will critically evaluate the results of our research, compare the evolution of the electronicisation of Slovak and Czech public administration and propose possible options for improving the regulation of public administration activities.

We want to achieve the stated main objective and milestones by carefully examining the relevant European, Slovak and Czech legislation. Another major source of knowledge is the expert and scientific literary resources contained in the databases Web of Science and Scopus. Due to the nature of the scientific study, we use several scientific methods of knowledge suitable for knowledge of the law. This includes, in particular, the use of a critical analysis method to examine the legal situation and regulation, as well as methods of abstraction or synthesis. The results of the critical analysis of legislation are supported by the results of related research by relevant researchers. Since the Slovak Republic was part of the Czech and Slovak Federal Republic until 1993, in order to improve the quality of work, we also pay due attention to the impact of the eIDAS Regulation on the development of the electronicisation of public administration in the Czech Republic. At the end of our scientific study using a comparative method, we compare the development of both regulations.

5. Discussion and Conclusions

The eIDAS Regulation became the first concrete step of the European Commission's Digital Single Market strategy, which was set to become a reality in the European Union by 2020. Its aim was to facilitate not only e-commerce but also all cross-border transactions. The eIDAS Regulation repealed the Directive of the European Parliament and of the Council on electronic signature, and in the conditions of the Slovak Republic, the new Act on Trust Services repealed its transposing national law—the Electronic Signature Act. The main benefit of the eIDAS Regulation has been the possibility of full electronic submission in other Member States, as well as the possibility of dealing with many life situations remotely. Its applicability has also become significant for many commercial companies, which are thus able to participate much more easily in public tenders in other countries of the European Union, without having to deal with any paper documents. The practical impact of the new legislation is now acceptable to users of all Member States of the European Union.

We found that the eIDAS Regulation covers two main areas of 'electronic identification' and 'trusted services'. In electronic identification, the eIDAS Regulation creates the conditions for a "mutual recognition obligation". This is an obligation for those Member

States of the European Union that use certain specific electronic identification means (e.g., in the case of the Slovak Republic, a chip eID card) to recognise, for access to these services, the electronic identification means used by other Member States for access to these services, if notified to the European Commission. This obligation is to ensure that citizens of the European Union from one Member State can access public online services also available in other Member States. The eIDAS Regulation ties significant legal presumptions to the use of qualified services, unifies the legal effects associated with the use of these services across the European Union and also regulates their cross-border recognition.

Slovak legislation is based on current needs and has responded to the conditions and needs of an ever-changing practice with several amendments. We can evaluate electronic identity cards as a positive step towards electronicisation. Their indisputable advantage is the obligation for entrepreneurs to communicate with administrative authorities electronically, which reduces the cost of delivering documents by post. Such a procedure also clearly eliminates the scope for obstructions in the delivery of decisions of public administration bodies. This shortens the time of administrative and judicial proceedings.

In comparison with Czech legislation, we can only conclude that we are always "some year" behind the adoption of the necessary legislation. This finding is based not only on the year of adoption of the laws but also on the content of the explanatory memorandums to these laws, where as a rule, the already existing Czech legislation is referred to. This also has a significant impact on the content and similarity of our legislation in this area. However, this does not mean that the Czech legislation is better, because the legislation is always adapted to the current needs of a specific state. However, we also see the similarity of legal regulations in the way electronic ID cards work.

The eIDAS Regulation has been in force for more than six years. As the content of our study shows, the Regulation has had and has a fundamental impact not only on the modification of the legal institute of electronic signature, but also sometimes only indirectly, on several areas of the Slovak legal order. However, there are still areas that will need to be amended in the light of the objectives set out in the eIDAS Regulation (e.g., conformity assessment authority mentioned in Section 4.5). It can also be expected that the practical use of cross-border electronic identification within the European Union will bring further issues. Although substantial steps have already been taken to develop and streamline the execution of online transactions and the provision of online services, it can nevertheless be expected, in the light of the above, that the full implementation of the eIDAS Regulation in life will still take some time. Perhaps the end of the COVID-19 pandemic and the associated transition to the online space has brought about a number of challenges that will need to be addressed by amending the eIDAS Regulation (eIDAS 2.0), which is already published (European Parliament and Council 2021). As follows from the explanatory report to this regulation, the evaluation of the eIDAS 2 regulation demonstrated that the current regulation does not adequately address these new market requirements, mainly due to its natural limitations for the public sector, the limited possibilities and complexity of connecting private online providers to the system, the lack of availability of notified electronic identification solutions in all Member States and lack of flexibility to support different use cases. In addition, identity solutions outside the scope of the eIDAS regulation, such as those offered by social media providers and financial institutions, raise privacy and data protection concerns. These solutions are not able to respond effectively to new market demands and do not have sufficient cross-border coverage to address the specific needs of sectors where identification is sensitive and requires a high degree of certainty. It proposes to build a European digital identity. This should create a new system for secure transactions across the European Community, especially among selected entities such as residents, entrepreneurs, and the public sector. It should be possible to achieve this objective through electronic identification means and schemes mutually recognised between Member States in public sector electronic services. We are convinced that the amendment of the eIDAS Regulation will bring into practice, in addition to the proposed European digital identity, the unification of the regulation of trust services such as the

creation and validation of electronic signatures, electronic seals or electronic time stamps and others. For these reasons, as part of our future review, we will also focus on the selected issues of the amended eIDAS Regulation (eIDAS 2.0).

Author Contributions: Conceptualization, D.G. and T.P.; methodology, Z.H.; software, T.P.; validation, Z.H. and T.P.; formal analysis, Z.H. and T.P.; investigation, D.G. and Z.H.; resources, T.P.; data curation, D.G. and Z.H.; writing—original draft preparation, D.G., T.P. and Z.H.; writing—review and editing, T.P.; visualization, T.P.; supervision, T.P.; project administration, T.P.; funding acquisition, T.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by project: National infrastructure for supporting technology transfer in Slovakia II—NITT SK II, co-financed by the European Regional Development Fund.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

Alimehaj, Vlera, Arbnor Halili, Ramadan Dervishi, Vehbi Neziri, and Blerim Rexha. 2021. Analysing and comparing the digital seal according to eIDAS regulation with and without blockchain technology. *International Journal of Information and Computer Security* 14: 171–91. [CrossRef]

Alonso, Álvaro, Alejandro Pozo, Aldo Gordillo, Sonsoles López-Pernas, Andrés Munoz-Arcentales, Lourdes Marco, and Enrique Barra. 2020. Enhancing university services by extending the eIDAS European specification with academic attributes. *Sustainability* 12: 770. [CrossRef]

Berbecaru, Diana, and Antonio Lioy. 2018. On integration of academic attributes in the eIDAS infrastructure to support cross-border services. Paper presented at 2018 22nd International Conference on System Theory, Control and Computing (ICSTCC 2018), Sinaia, Romania, October 10–12; pp. 691–96.

Berbecaru, Diana, Antonio Lioy, and Cesare Cameroni. 2019. Electronic identification for universities: Building cross-border services based on the eIDAS infrastructure. *Information* 10: 210. [CrossRef]

Bodea, Constanta-Nicoleta, and Augustin Purnus. 2018. Legal implications of adopting Building Information Modeling (BIM). *Juridical Tribune* 8: 63–72.

Chochia, Archil, and Teele Nässi. 2021. Ethics and emerging technologies—Facial recognition. Revista de Internet. *Derecho y Politica* 34: 1–12. [CrossRef]

Cirlig, Ramona Elisabeta. 2016. Business and human rights: From soft law to hard law? *Juridical Tribune* 6: 228–46.

Dumortier, Jos, Stefan Kelm, Hans Nilsson, Georgia Skouma, and Patrick van Eecke. 2003. *Study on Legal and Market Aspects of the Application of Directive 1999/93/EC Laying Down a Community Framework for Electronic Signatures and on Practical Applications of the Electronic Signature*. Brusel: K.U. Leuven, Belgium for the European Commission, Directorate General Information Society.

Dusek, Jiri. 2017. Evaluation of Development of Cooperation in South Bohemian Municipalities in the Years 2007–2014. *European Countryside* 9: 342–58. [CrossRef]

Dusek, Jiri. 2018. How to Measure Intermunicipal Cooperation in Conditions of the Czech Republic. In *Modeling Innovation Sustainability and Technologies. Springer Proceedings in Business and Economics*. Cham: Springer, pp. 149–56. [CrossRef]

Erdogan, Ozgun, and Nurdan Ayse Saran. 2021. A survey on server-based electronic identification and signature schemes to improve eIDAS: With a new proposal for Turkey. *PeerJ Computer Science* 7: e734. [CrossRef]

European Parliament and Council. 1999. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. Available online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A31999L0093 (accessed on 11 September 2022).

European Parliament and Council. 2008. Regulation of the European Parliament and the Council (EC) no. 765/2008 of 9 July 2008, Which Establishes the Requirements for Accreditation and Market Surveillance in Connection with the Introduction of Products to the Market and Which Repeals Regulation (EEC) no. 339/93. Available online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32008R0765&qid=1663662006148 (accessed on 11 September 2022).

European Parliament and Council. 2014. Regulation of the European Parliament and the Council (EU) no. 910/2014 of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Available online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32014R0910&qid=1663662232182 (accessed on 11 September 2022).

European Parliament and Council. 2016. Directive (EU) 22016/1148 of 6 July 2016 on Measures to Ensure a High Common Level of Security of Networks and Information Systems in the EU. Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 11 June 2022).

European Parliament and Council. 2021. Draft Regulation of the European Parliament and of the Council Amending Regulation (EU) no. 910/2014 Regarding the Establishment of a Framework for a European Digital Identity. Available online: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52021PC0281&from=EN (accessed on 29 October 2022).

Funta, Rastislav, and Kristína Králiková. 2022. Obligation of the European Commission to review national civil court judgements? *Tribuna Juridica* 12: 215–26. [CrossRef]

Funta, Rastislav, and Peter Ondria. 2021. Data Protection in Law Enforcement and Judicial Cooperation in Criminal Matters. *TalTech Journal of European Studies* 11: 148–66. [CrossRef]

Handrlica, Jakub. 2019. Two faces of "international administrative law". *Juridical Tribune* 9: 363–76.

Handrlica, Jakub, Vladimír Sharp, and Kamila Balounová. 2022. The administrative law of the Czech Republic and the public law of Ukraine: A study in international administrative law. *Juridical Tribune* 12: 195–214. [CrossRef]

Horváthová, Zuzana, and Andrea Čajková. 2019. Framework of the sickness insurance in the Czech Republic and selected countries of the European Union. *European Journal of Transformation Studies* 7: 106–25.

Jankelova, Nadezda, and Dusan Masar. 2021. Knowledge management as a tool for increasing the efficiency of municipality management in Slovakia. *Knowledge Management Research and Practice 1–11*. [CrossRef]

Jankelova, Nadezda, Zuzana Joniakova, and Anita Romanova. 2021. Leadership competencies in communal policy. *Politicke Vedy* 24: 181–204. [CrossRef]

Kusber, Tomasz, Steffe Schwalm, Kalinda Shamburger, and Ulrike Korte. 2020. Criteria for trustworthy digital transactions—Blockchain/DLT between eIDAS, GDPR, data and evidence preservation. In *Lecture Notes in Informatics (LNI), Proceedings—Series of the Gesellschaft fur Informatik (GI), P-305*. Bonn: Gesellschaft für Informatik e.V., pp. 49–60.

Kutyłowski, Mirosław, and Przemysław Błaśkiewicz. 2023. Advanced Electronic Signatures and eIDAS—Analysis of the Concept. *Computer Standards and Interfaces* 83: 103644. [CrossRef]

Malatinec, Tomas. 2017. Legislative framework of green public procurement and Europeanisation of the Slovak practice. *Juridical Tribune* 7: 95–107.

Maliappis, Michael, Konstantinos Gerakos, Constantina Costopoulou, and Maria Ntaliani. 2019. Authenticated academic services through eIDAS. *International Journal of Electronic Governance* 11: 386–400. [CrossRef]

Ministry of the Interior of the Czech Republic. 2011. Decree No. 400/2011 Coll., Implementing the Act on Identity Cards and the Act on Travel Documents as Amended. Available online: https://www.zakonyprolidi.cz/cs/2011-400 (accessed on 11 September 2022).

Mocanu, Stefan, Ana Maria Chiriac, Cosmin Popa, Radu Dobrescu, and Daniela Saru. 2019. Identification and Trust Techniques Compatible with eIDAS Regulation. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 284*. Cham: Springer, pp. 656–65.

Mucha, Boris, and Katarina Mocarnikova. 2018. The Importance and Position of Public Company In the Slovak Business Law. Paper presented at 31st International-Business-Information-Management-Association Conference, Milan, Italy, April 25–26; pp. 3494–502.

National Assembly of the Czechoslovak Socialist Republic. 1964. Act No. 40/1964 Coll. Civil Code as Amended. Available online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1964/40/20191201 (accessed on 11 September 2022).

National Council of the Slovak Republic. 2002. Act No. 215/2002 Coll. on Electronic Signatures and Amendments to Certain Laws as Amended. Available online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2002/215/20160701 (accessed on 11 September 2022).

National Council of the Slovak Republic. 2013. Act No. 305/2013 Coll. on the Electronic form of the Exercise of the Powers of Public Authorities and on the Amendment and Supplementation of Certain Laws (the e-Government Act). Available online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/305/20201230 (accessed on 11 September 2022).

National Council of the Slovak Republic. 2016. Act No. 272/2016 Coll. on Trusted Services for Electronic Transactions on the Domestic Market and on the Amendment of Certain Laws (Act on Trusted Services) as Amended. Available online: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2016/272/20190801 (accessed on 11 September 2022).

Nováčková, Daniela, and Jana Vnuková. 2021. Competition issues including in the international agreements of the Eropean union. *Juridical Tribune* 11: 234–50. [CrossRef]

Parliament of the Czech Republic. 2000. Act No. 365/2000 Coll. on Public Administration Information Systems as Amended. Available online: https://www.zakonyprolidi.cz/cs/2008-300?text=365%2F2000 (accessed on 11 September 2022).

Parliament of the Czech Republic. 2012. Act No. 89/2012 Coll. Civil Code, as Amended. Available online: https://www.zakonyprolidi.cz/cs/2012-89 (accessed on 11 September 2022).

Parliament of the Czech Republic. 2016. Act No. 297/2016 Coll. on Trust-Creating Services for Electronic Transactions, as Amended. Available online: https://www.zakonyprolidi.cz/cs/2016-297 (accessed on 11 September 2022).

Parliament of the Czech Republic. 2017. Act No. 250/2017 Coll. on Electronic Identification, as Amended. Available online: https://www.zakonyprolidi.cz/cs/2017-250 (accessed on 11 September 2022).

Pavelek, Ondřej, and Drahomíra Zajíčková. 2021. Personal Data Protection in the Decision-Making of the CJEU before and after the Lisbon Treaty. *TalTech Journal of European Studies* 11: 167–88. [CrossRef]

Pelikánová, Radka MacGregor, and Eva Daniela Cvik. 2019. Awarenes and perception of modernized electronic public procurement—Czech case study. *Ad Alta—Journal of interdisciplinary research* 9: 34–40.
Pelikánová, Radka MacGregor, Eva Daniela Cvik, and Robert MacGregor. 2019. Qualified electronic signature—EIDAS striking Czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis* 67: 1551–60. [CrossRef]
Peracek, Tomas, Solomiia Fedushko, Yuriy Syerov, and Olha Trach. 2021. Development of Methods for the Strategic Management of Web Projects. *Sustainability* 13: 742. [CrossRef]
Poiană, Oana. 2017. An overview of the European energy policy evolution: From the European energy community to the European energy union. *Online Journal Modelling the New Europe* 22: 175–89. [CrossRef]
Průša, Jiří. 2015. E-identity: Basic building block of e-Government. Paper presented at 2015 IST-Africa Conference, IST-Africa 2015, Lilongwe, Malawi, May 6–8.
Ravšelj, Dejan, Lan Umek, Ljupčo Todorovski, and Aleksander Aristovnik. 2022. A Review of Digital Era Governance Research in the First Two Decades: A Bibliometric Study. *Future Internet* 14: 126. [CrossRef]
Sararu, Catalin Silviu. 2016. Considerations on the public services in the XXI century. *Juridical Tribune-Tribuna Juridica* 6: 160–66.
Sararu, Catalin Silviu. 2017. General principles of European Administrative Law. In *European Administrative Space—Recent Challenges and Evolution Prospects*. Bucharest: International Academic Publisher, pp. 110–29.
Sararu, Catalin Silviu. 2019. Public domain and private domain. *Administrative Law in Romania* 1: 84–100.
Schmidt, Carsten, Robert Krimmer, and Thomas J. Lampoltshammer. 2021. "When need becomes necessity"—The single digital gateway regulation and the once-only principle from a European point of view. In *Lecture Notes in Informatics (LNI), Proceedings—Series of the Gesellschaft fur Informatik (GI), P-312*. Bonn: Gesellschaft für Informatik e.V., pp. 223–28.
Simonova, Stanislava, and Meseret Yihun Amare. 2019. Aspects of Digital Documents Archiving by the Organizations in the Czech Republic in Context of the EU eGovernment. Paper presented at International Conference on Information and Digital Technologies 2019 (IDT 2019), Zilina, Slovakia, June 25–27; pp. 460–67.
Šindleryová, Ivana Butoracová. 2022. Usability of Municipal Performance-based Budgets within Strategic Planning in Slovakia: Perception of Elected Local Representatives. *NISPAcee Journal of Public Administration and Policy* 15: 17–37.
Skora, Agnieszka, Mária Srebalová, and Ingrida Papáčová. 2022. Administrative judiciary is looking for a balance in a crisis. *Juridical Tribune* 12: 5–20. [CrossRef]
Stancetic, Veran. 2020. Spoils System Is Not Dead: The Development and Effectiveness of the Merit System in Western Balkans. *Croatian and Comparative Public Administration* 20: 415–38. [CrossRef]
Troitino, David Ramiro, Archil Chochia, and Tanel Kerikmäe. 2017. The incapacity of the union to act as a reliable actor in the international arena. *Current Politics & Economics of Europe* 28: 211–27.
Troitino, David Ramiro, Tanel Kerikmäe, and Archil Chochia. 2020. Foreign affairs of the European Union: How to become an independent and dominant power in the international arena. In *The EU in the 21st Century: Challenges and Opportunities for the European Integration Process*. Cham: Springer, pp. 209–30. [CrossRef]
Tsakalakis, Niko, Kieron O'hara, and Sophie Stalla-Bourdillon. 2016. Identity Assurance in the UK: Technical implementation and legal implications under the eIDAS Regulation. Paper presented at WebSci 2016—2016 ACM Web Science Conference, Hannover, Germany, May 22–25; pp. 55–65.
Vel Kalisz, Beata Gessel-Kalinowska. 2021. Admissibility of Electronic Awards in the UNCITRAL Model Law Jurisdiction: Polish Law Example. *Journal of International Arbitration* 38: 147–62. [CrossRef]
Vogt, Theresa. 2016. The new eIDAS-regulation—Chance and challenge for the public administration in Germany. *Information-Wissenschaft und Praxis* 67: 61–68.
Žofčinová, Vladimíra, Andrea Čajková, and Ratislav Kral. 2022. Local Leader and Labour Law Position in the Context of the Concept of 'Smart Cities' Through the Optics of the European Union. *TalTech Journal of European Studies* 12: 3–26. [CrossRef]