IDA JÓŹWIAK[1]

LIABILITY OF TRUST SERVICE PROVIDERS - SELECTED ASPECTS[2]

INTRODUCTION

The use of trust services, that is electronic services whereby electronic signatures, electronic seals, electronic time stamps, recorded electronic delivery are created, verified, validated and preserved, websites are authenticated with certificates[3] essentially seeks to confirm the identity of the person signing an electronic document as if they had presented their ID card to the declaration recipient when setting their hand and to protect the document against unauthorised content modification[4], alternatively to append it with a certified date[5] or confirmation the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt[6]. All the category of trust services diversified in terms of type is oriented towards eliminating the risky anonymity of participants in activities undertaken by electronic means and at the same time making their activities credible by such measures as the authentication of the identity of the transacting party[7], ensuring the integrity (unchangeability) of the content of the declarations of intent submitted[8], confirmation of the time of transactions[9].

However, in the era of rapid technological progress coupled with growing threat of cybercrime, electronic legal trade can be fully guaranteed as secure no more, just as traditional

[1] University Cardinal Wyszyński in Warsaw.
[2] Artykuł przetłumaczony ze środków finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego na działalność upowszechniającą naukę (DUN), nr decyzji 810/P-DUN/2018. Article translated from funds financed by the Ministry of Science and Higher Education for the dissemination of science (DUN), Decision No. 810 / P-DUN / 2018.
[3] Article 3 (16) of 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 (OJ L 257, 28.8.2014 p. 73–114), hereinafter referred to as the 'eIDAS Regulation'.
[4] Conf. Article 26 (d) and Article 36 (d) of the eIDAS Regulation.
[5] In Poland, as of 8 September 2016, a qualified electronic time stamp has triggered the effects of a certified date. (Article 81 § 2 (3) of the Civil Code).
[6] Conf. Article 43 (2) of the eIDAS Regulation.
[7] Conf. Article 26 (b) and Article 36 (b) of the eIDAS Regulation.
[8] Conf. Article 26 (d), Article 36 (d), Article 41 (2), Article 43 (2) of the eIDAS Regulation.
[9] Conf. Article 41 (2), Article 43 (2) of the eIDAS Regulation.

trading with the use of handwritten documents is not completely free of risks such as forged signatures, additions, loss or destruction of documents. As the use of electronic services require appropriate software, which can be remotely accessed by a supplier or unauthorized person who carries out a hacking attack, a question emerges of the liability of software and hardware providers that enable the use of trust services for their security, that is the liability of trust service providers. The paper presents selected aspects of this issue, vital for security of users and recipients of trust services. The text volume being limited, basic concepts and problems, such as for instance definitions of particular trust services, differences between qualified and non-qualified services, their legal framework and effects and practical application will be omitted or mentioned only in passing.

Given that the subject matter of the liability of trust providers under the current 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[10] (commonly referred to as the eIDAS Regulation as the acronym for the English-language name *electronic IDentification, Authentication and trust Services*; hereinafter referred to as the "eIDAS Regulation"), has not been developed further in doctrine, and its regime is based on the experience with the implementation of Directive 1999/93/EC, I will make comparisons as appropriate and refer to the acquis arising from the previous legal status. So far, this issue has not been interpreted by the Court of Justice of the European Union, either under the Directive or the Regulation.

LEGAL FRAMEWORK FOR TRUST SERVICE PROVIDERS

The business of trust service providers is handled in the eIDAS regulation, supplemented in the Republic of Poland with the Act of 5 September 2016 on *trust services* and electronic identification[11] (hereinafter referred to as the "Act on trust services", "u.u.z."). The eIDAS Regulation superseded Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[12] (hereinafter "Directive 1999/93/EC"), which aimed at creating a Community framework for the use of electronic signatures, allowing the free, cross-border movement of related products and

[10] OJ L 257, 28.8.2014 p. 73–114.
[11] Consolidated text Dz.U.-Journal of Laws of 2019 item 162.
[12] OJ L 013, 19.1.2000, p. 12 – 20.

services be held and ensuring that its legal effectiveness is recognized to a fundamental extent[13]. However, its scope did not cover formal requirements for the conclusion and effectiveness of contracts which are governed by the internal rules of the Member States.

QUALIFIED AND NON-QUALIFIED SERVICES

E-signatures[14], electronic seals[15], electronic time stamps[16], registered electronic delivery services[17] and certificates for website authentication[18] may be non-qualified (ordinary) or qualified in form, and furthermore, for electronic signatures and electronic seals, their advanced forms are identified, which can be defined as intermediate forms between ordinary and qualified, as they meet the technical requirements set for the qualified form, whereas unlike the qualified form, they failed to be awarded with the qualified certificate required by the eIDAS Regulation. A qualified trust service is defined as a trust service that meets the relevant requirements set out in the Regulation[19]. Qualified services are linked to specific legal effects and presumptions[20].

APPLICATION OF TRUST SERVICES

As assumed by the European legislator, trust services should be applied in a number of ways both in private law relations and in contacts with public administration, including e-

[13] Recitals 4 and 16 of Directive 1999/93/EC.
[14] Within the meaning of Article 3 (10) of the eIDAS Regulation 'electronic signature' means 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.
[15] Within the meaning of Article 3 (25) of the eIDAS Regulation 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
[16] Within the meaning of Article 3 (33) of the eIDAS Regulation 'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.
[17] Within the meaning of Article 3 (36) of the eIDAS Regulation 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.
[18] Within the meaning of Article 3 (38) of the eIDAS Regulation 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.
[19] Article 3 (17) of the eIDAS Regulation.
[20] Conf. Article 25 (2), Article 25 (3), Article 35 (2), Article 35 (3), Article 41 (2), Article 41 (3), Article 43 (2) of the eIDAS Regulation.

banking, invoice issue, contract conclusions, tax returns, health care system, *online* transactions[21]. The nature and quantity of the data exchanged, required level of security and the implications of possible data leakage differ materially in each of examples of application areas, hence, individual forms of trust services (ordinary, qualified, advanced) carry different legal effects, as per the level of security they offer. Electronic signature-based services (creation, verification, validation and maintenance) are best known. The National Clearing House, a qualified Polish trust service providers, illustrates the use of Szafir, electronic signature it issues in declarations to the Social Insurance Institution ZUS in the Płatnik software, submission of financial reports to the National Court Register, electronic reports to tax offices, electronic invoices, signing medical documentation, participation in tenders and electronic auctions, provision of information to the General Inspector of Financial Information and contacts with authorities[22]. Asseco, a supplier of electronic signature Certum, supplements the list with applications for subsidies to the Polish Agency for Enterprise Development, business relations (B2B) and business relations with clients (B2C), applications in the judiciary and penitentiary, that is for mutual communication between courts and penitentiary services, development of electronic records, transmission of pleadings in electronic proceedings by writ of payment[23].

PRINCIPLES OF LIABILITY OF TRUST SERVICE PROVIDERS

The basic provision governing the liability of trust service providers, Article 13 of the eIDAS Regulation, sets out the basic principles of liability, rules for the allocation of the burden of proof and provides for limiting the provider's liability. At the same time, it should be borne in mind that the Regulation fails to comprehensively stipulate for liability, and should be applied under national liability laws[24], including the definition of the concept and extent of damage or intent or negligence.

Under Article 13(1) of the Regulation, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with

[21] *European Union Agency for Cybersecurity*, A digital Europe built on trust – ENISA supports relying parties and end users to implement the eIDAS Regulation, 29.06.2017, online access: https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust (access date: 07.09.2019)
[22] *National Clearing House*, Qualified certificates, online access: http://www.elektronicznypodpis.pl/oferta/certyfikaty-kwalifikowane/ (access date: 07.09.2019)
[23] *Certum*, Electronic signature. Area of application, online access: https://www.certum.pl/pl/cert_oferta_epodpis_zastosowania/ (access date: 07.09.2019)
[24] Conf. Recital of 18 of the eIDAS Regulation.

the obligations under this Regulation. Liability arises from damage, intention to cause damage or negligence of the trust service provider and the causal link between the damage and default laid down in the Regulation.

DAMAGE

Under Directive 1999/93/EC, a certification-service-provider was liable only for a few types of damage referred to in Article 6(1)(a), Article 6(1)(b) and Article 6(1)(c), that is:

d) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
e) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
f) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates both of them.

Hence, damages from other causes than non-compliance or incompleteness, completeness, truthfulness and complementarity of the data remained outside the scope of the Directive's standardisation and, unless covered by broader national law provisions (the Directive provided for a minimum level of protection required in all Member States), would be subject to general liability rules in the relevant country.

In the eIDAS Regulation, the European legislator resigned from enumerating situations in which a trust service provider may be liable for damages, but instead established a criterion for linking damage to failure to comply with the obligations laid down in the Regulation. By way of illustration, several types of damage may stem from a breach of security or loss of integrity of trust services: disclosure or interception by an unauthorised person of confidential correspondence or documents, leakage of personal data, including sensitive data, modification of the content of documents, declarations of intent (loss of document integrity), false declarations of intent, false signatures under declarations of intent, interception of login data

for various websites on the Internet, including public administration services provided by electronic means, extortion of money, blackmail.

Obviously, the above situations may trigger further damage. If the contents of a confidential document containing large scale business secrets were to be disclosed, the loss from the publication of that information could be counted in millions of euros. A lot depends on the type of service concerned, its use, type and scale of the breach, speed with which the trust service provider reacts and others. The competent national court will identify the damage, its extent and the compensation to be paid, in particular determining whether it should cover solely actual loss *(damnum emergens)* or also lost profits *(lucrum cessans)* on a case-by-case basis, in accordance with the interpretative directives adopted by the relevant jurisdiction.

CAUSAL LINK BETWEEN DAMAGE AND DEFAULT ON THE REGULATORY OBLIGATIONS

Liability of trust service providers, both qualified and non-qualified, is primarily contingent on a causal link between damage and default on the obligations laid down in the eIDAS Regulation. Hence, the proper performance of the duties overseen by the network of European supervisory authorities exempts the trust service provider from liability for damage.

The scope of the obligations to render trust services varies for non-qualified and qualified providers, this being entirely legitimate given that different types of services carry divergent legal effects. Part of the requirements of the eIDAS Regulation apply to qualified and non-qualified suppliers (Articles 15, 19), part only to qualified suppliers (Articles 20, 24).

Common obligations for qualified and non-qualified trust service providers include:

6) Take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide,

7) Ensure that the level of security is commensurate to the degree of risk, having regard to the latest technological developments,

8) Take measures to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents,

9) Notify the supervisory body and other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity; where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider the natural or legal person shall also be notified,

10) Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Qualified trust service providers are also required to:

16) Verify identity and any special attributes when issuing a qualified certificate for trust services,

17) Inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities,

18) Hire personnel and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and apply administrative and management procedures which correspond to European or international standards,

19) Maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law,

20) Inform, in a clear and comprehensive manner of the precise terms and conditions regarding the use of that service, including any limitations on its use,

21) Use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them,

22) Use trustworthy systems to store data in a verifiable form,

23) Take appropriate measures against forgery and theft of data,

24) Record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service,

25) Have an up-to-date termination plan,

26) Ensure lawful processing of personal data,

27) Establish and keep updated a certificate database,

28) Register certificate revocation and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request,

29) Provide at all times to any relying party[25] information on the status of validity or revocation of qualified certificates automatically, reliably, free of charge and efficiently, provide to any relying party information on the validity or revocation status of qualified certificates in an automated manner that is reliable, free of charge and efficient,

30) Be audited at their own expense at least every 24 months by a conformity assessment body, and by the supervisory body or a sub-commissioned conformity assessment body at any time – at any time.

The above obligations are complementary and their scope is partly overlapping but also supplement one another, establishing a set of security principles in the operations of trust service providers. If they are applied properly, the risk of damage is marginal and should it materialise, its extent will be reduced. Some of them will be discussed below, with a particular emphasis on the potential consequences of their non-performance or inadequate performance.

[25] Within the meaning of Article 3 (6) of the eIDAS Regulation 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service. "Reliance" means that a person has checked a certificate pertinent to a trust service (for instance following receipt of an electronic document bearing an electronic signature, electronic seal or electronic time stamp) and, having ensured that it is valid, has trusted the content of the received document or website secured by a certificate of website authentication. A relying party does not need to be an active user of trust services. On the contrary, many people acquire the attribute of a relying party without being aware of it, be it by opening legal acts or other official documents in electronic form on Biuletyn Informacji Publicznej [*Public Information Bulletin website]*.

PREVENTING SECURITY INCIDENTS AND INFORMING STAKEHOLDERS OF THEIR NEGATIVE CONSEQUENCES

Article 19(1) of the eIDAS Regulation requires Trust Service Providers to take appropriate technical and organisational measures to manage risks, in particular by taking measures to prevent or minimise the impact of security incidents. A security incident is defined as an event or sequence of events that creates a significant probability of disrupting business processes that are critical to the organisation or of disclosing information that is of high value to the organisation or is protected by law[26]. Examples of security incidents include: breach of confidentiality (disclosure to unauthorized persons), of integrity (damage, destruction), of availability (disabling access), malware, unauthorized access to the system or its parts, password fraud, theft or destruction of IT equipment and data carriers[27]. It is security incidents that will most often directly cause damage to users of trust services, such as: violation of correspondence secrecy, loss of funds (for instance due to interception of login data to the electronic banking system), arising of contractual obligations and liability (in a case of data theft to make appropriate declarations of intent to conclude a contract), submission of false statements in relations with public administration (be it false tax declaration in a case of using data to make an electronic signature), etc. Hence, comprehensive security of ICT systems and networks is a key element of the operations pursued by trust service providers.

The trust service provider must inform stakeholders of the adverse consequences of any security incident. A stakeholder may be both a user of trust services and any entity that has suffered or may suffer damage as a result of the incident, for instance by making a false declaration of intent using the user's data. Informing the stakeholder is intended to enable it to take actions that will limit or eliminate further damage, for example by changing access passwords or revoking declarations of intent that have been made with the use of its data.

[26] Definition inPN-ISO/IEC 27000:2017-06.
[27] *D. Łydziński*, Procedury zarządzania incydentami bezpieczeństwa, IT Professional, 2 września 2016 r., dostęp: http://www.it-professional.pl/temat-numeru/artykul,6780,procedury-zarzadzania-incydentami-bezpieczenstwa.html (access date: 10.09.2019 r.).

NOTIFICATION OF COMPETENT AUTHORITIES AND USERS OF TRUST SERVICES

Under Article 19(2) of the eIDAS Regulation, qualified and non-qualified trust service providers are required to notify the supervisory body and other relevant entities, such as the competent national information security body (in Poland the minister in charge of computerisation) or the data protection authority (in Poland the President of the Personal Data Protection Office), of any breach of security or loss of integrity that has a significant impact on the service or the personal data processed within it. Notification of the authorities should be made without undue delay, and in any case not later than within 24 hours after having become aware of an event. The information obligation must also be complied with forthwith for a natural or legal person to whom the trust service has been provided if the event is likely to adversely affect that person. The notifications are to reduce the scale and extent of damages by issuing warnings and recommendations and, in more serious cases, by having certificates suspended or revoked. Thus, the rapid detection and reporting of a security incident is essential for the extent of liability for damages.

Some difficulties may arise in interpreting the vague concepts of 'significant influence' and 'likelihood of adverse affecting a person'. It appears that in the assessment of the extent of the breach and the likelihood of adverse impact one should take into account in particular the findings of risk analysis, relevance of the breach to the continuity and integrity of the service, type of service provided, number of persons affected and the need for supervisory measures by the competent body, in particular the suspension or revocation of certificates. Compared to the obligation to inform stakeholders of the adverse effects of any security incident (Article 19(1) of Regulation (EC) No 1049/2001), covering even minor events that have caused no harm, the obligation to report security breaches and security breaches with a significant impact on a service or the personal data processed within it concerns more severe situations, which are systemic rather than individual.

In this context, it is worth quoting one of the most famous examples of security incidents that ultimately led to the bankruptcy DigiNotar, Dutch company, which issued certificates on its own behalf and as an intermediary in the issuance of governmental certificates that provided electronic access to public administration services. In 2009 SSL protocol for secure transmission of encrypted data, often used for logging in to electronic banking systems or e-mails (an Internet user can easily verify whether a website is protected by the protocol - in such

a case, the website address is preceded by https:// and a padlock sign is displayed), revealed a vulnerability that allowed a hacker attack known as *Man in the Middle* to be launched, whereby access was obtained to information exchanged between the unaware parties of correspondence. For this reason, a recommendation was issued to use updated versions of the protocol and information came out about the potentially major threat from the use of the protocol, that is breaking into the server of the main certification centre and gaining access to data for generating counterfeit certificates, accepted by web browsers as true. Over five hundred false certificates were generated in a few weeks, including entities such as CIA, Mossad, Google, Facebook, Twitter, Microsoft, Skype, and cybercriminals accessed the content of confidential conversations and information. Although the attack came to Diginotar attention on 19.07.2011, it did not admit it until late August 2011, when the operators of popular web browsers started to remove the certificates issued by DigiNotar from the list of trusted certificates. On 3 September 2011 a decision was taken to revoke the governmental certificates issued by the company, cutting many Dutch citizens from *online* administration services. The investigation revealed that the company lacked antivirus protection on the public server, failed to update its software, and its prevention system had not blocked the external attack, and that cybercriminals had broken the administrator's password to gain unrestricted access to all related servers. The number of persons have remained undetermined, who suffered damage due to violation of correspondence secrecy, hackers' access to login data to many systems or access to eGovernment services, however, bearing in mind the global range and particular sensitivity of data held by some of the above entities, whose certificates were falsified, aggravated by DigiNotar's over-a-month-long inertia to the event, the potential damage is difficult to overestimate[28].

The history of DigiNotar illustrates the use of insufficient, weak and obsolete security measures, ineffective mechanisms for detecting security incidents and, at the same time, the lack of proper response of the service provider to the existing security threats, which ultimately led to the total loss of reputation and the bankruptcy. The severe sanction applied by the Dutch government - revocation of certificates - reflects the severity of the infringements. It is worth noting that the eIDAS Regulation establishes a network of cooperation between supervisory

[28] Based on: *M. Marucha-Jaworska*, Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym, Warszawa 2015, p. 147-148 and *European Union Agency for Network and Information Security*, Mitigating the impact of security incidents. Guidelines for trust service providers – part 3, ver. 1.0, December 2013, online access: https://www.enisa.europa.eu/publications/tsp3-incidents/at_download/fullReport (access date: 08.09.2019), p. 23.

authorities[29] (in Poland this function is performed by the minister in charge of computerisation), and the exchange of information between supervisory authorities from countries affected by security breaches or loss of integrity[30]. is one of the forms of cooperation. Moreover, the supervisory body should notify ENISA[31] (European Union Agency for Network and Information Security) about the cross-border event. Furthermore, where the notified supervisory body considers that disclosure of the breach of security or loss of integrity is in the public interest, it shall make the information public or require the provider to do so[32].

Pursuant to Article 46(8) in conjunction with Article 47(2)(1) of the Trust Services Act, the negligence of a qualified trust service provider who has its registered office or branch in the Republic of Poland may render it liable to a fine of up to PLN 50 000. The limitation of the scope of the subjective scope of the criminal sanction in the Polish Trust Services Act is incomprehensible given that the European regulation imposes an information obligation on both qualified and non-qualified suppliers, and it would be difficult to find arguments to support the thesis that serious security incidents in the latter do not have to be reported to the supervisory authorities, since non-qualified services also have a legal and procedural effect in the form of prohibition of discrimination (prohibition on refusing the legal effect of a trust service or an electronic document or its admissibility as evidence in court proceedings solely because of its electronic form or because it does not meet the requirements of qualified form). In particular, the argument for not imposing sanctions for failure to comply with disclosure requirements on non-qualified suppliers should not invoke a limited nature of supervisory activities with reference to non-qualified suppliers, which become devoid or purpose, since the overriding objective of including all trust service providers in the supervision system should be the protection of users and the operation of the internal market[33].

PREVENTION OF FORGERY AND THEFT OF DATA

The credibility of the assumption that an authorised person has affixed an electronic signature (or an electronic seal) depends, on the one hand, on the authenticity of the data contained in the certificate at the stage of its issue and, on the other hand, on the effectiveness

[29] Conf. Recital 42, Article 17 (4)(a), Article 18 of the eIDAS Regulation.
[30] Conf. Article 17 (4)(c,) Article 19 (2) of the eIDAS Regulation.
[31] Article 19 (2) para. 3 of the eIDAS Regulation.
[32] Article 19 (2) para. 4 of the eIDAS Regulation.
[33] Recital 36 of the eIDAS Regulation.

of safeguards protecting against unauthorized use of the certificate. From a technical viewpoint, the protection is based on asymmetrical cryptographic algorithms (that is mathematical functions) with easily encryptable data (it is easy to calculate the result of a given function), while their decoding (mathematically: recreating the function formula on the basis of the result) is so complicated that data can be read only with the use of a special key (held by an authorized person) and - from the cryptographic perspective – no[34] third person can do it [35].

However, not only personal data contained in the certificate may be forged or stolen, but also information (data) contained in an electronic document which has been insufficiently protected by the trust service. Forgery (unauthorized modification in a manner that is not easily recognizable) of the data contained in an electronic document constitutes a breach of its integrity, the protection of which is essential for an electronic signature, electronic seal, electronic time stamp and registered electronic delivery. On the other hand, data theft in electronic form differs from the seizure of material movables in that it involves unauthorized access to these data (theft) and possibly illegal copying, rarely are cases of data being parallelly erased from the place accessible to an authorized data holder (that is data holder's access to data being cancelled). As a consequence, data theft may escape data holder's notice for a significant period of time - in Poland one year on average[36]. Stolen data may be used for various purposes, including blackmail and other forms of extortion. An example of data theft is the *Man in the Middle* attack described above.

The group of entities that may potentially suffer damage from data forgery or theft is very wide.

First, the aggrieved party may be a trust service user who has suffered damage as a result of forgery or theft of data contained in the certificate or exchanged with other entities using trust services. User damage may involve unauthorized access to data, their disclosure, claims of entities whose data have been forged or stolen, asserted against the user, losses resulting

[34] Impossibility is not an absolute concept in cryptography, it means that an act cannot be performed with the use of means known at that moment in acceptable time. (after: *R. Wobst*, Kryptologia. Budowa i łamanie zabezpiecz*eń*, Warszawa 2002, p. 274.

[35] *M. Marucha-Jaworska*, op.cit., p. 106.

[36] *PAP*, GIODO: Polak średnio po roku dowiaduje się o kradzieży tożsamości, 18.05.2015, https://www.pb.pl/giodo-polak-srednio-po-roku-dowiaduje-sie-o-kradziezy-tozsamosci-793371 (access: 15.09.2019).

from actions or omissions, which would not have occurred has it not been for a forged content of the electronic document, etc.

Second, the injured party may be a relying party who, acting in reliance of the data contained in the certificate of a trust service user or in a document secured by a service, performed a transaction (for example concluded an agreement) or omitted it, whereas it would have done otherwise if the data had not been forged.

Third, injured parties may be persons whose personal data have been included in the certificate by a person forging data contained therein without their knowledge and consent - their damage may consist both in the unlawful use of their personal data and in claims of relying parties against them, acting in the conviction of the existence of a legal relationship between the relying party and the person whose data have been used in the certificate.

Fourth, injured parties may include entities concerned by forged or stolen data, which may involve a wide variety of situations, from forgery (modification) of information on this entity on a website protected by a certificate of website authentication, through forgery or theft of entity data contained in a document exchanged between parties using trust services, to mass theft of personal data filing system or corporate financial data and others.

The extent of the damage inflicted on the injured party will depend to a large extent on the use of the stolen data and the consequences of acting in reliance of the content of the forged data.

CONCLUSION

The basic principles of liability of trust service providers are laid down in Article 13 of the eIDAS Regulation, which sets out the basic principles of liability, rules for the allocation of the burden of proof and limit the liability of the provider. At the same time, it should be borne in mind that not all rules on liability of suppliers have been stipulated in the regulation, and the Member States must for example define the concept and extent of damage and co-apply it with national liability rules. Moreover, the liability of trust service providers may be limited by relevant provisions of national law and policies on the provision of services created by trust service providers, and respectively the court considering the case on this issue will have to determine the provider's liability for damages under European and national law and the

contractual provisions between the trust service provider and the trust service user. So far, neither Polish courts nor the Court of Justice of the European Union have ruled on the liability of trust service providers under the eIDAS Regulation (the author is also unaware of any decisions of courts of EU Member States), so the provisions in this respect are difficult to be assessed in practice, however, it seems that the "multi-tier nature" of the standards, which the court would reach for, may cause considerable difficulties in interpretation. In particular, it should be noted that the concept and extent of damage attributable to a supplier's default on its obligations will come under the scope of national law, which could potentially give rise to significant differences in the case-law of courts in individual Member States on suppliers' liability for damages.

BIBLIOGRAPHY

Marucha–Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015.

PN-ISO/IEC 27000:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia

Wobst R., *Kryptologia. Budowa i łamanie zabezpieczeń*, Warszawa 2002.

Certum, *Podpis elektroniczny. Obszar zastosowania*, online access: https://www.certum.pl/pl/cert_oferta_epodpis_zastosowania/ (access date: 07.09.2019).

European Union Agency for Cybersecurity, *A digital Europe built on trust – ENISA supports relying parties and end users to implement the eIDAS Regulation*, 29.06.2017, online access: https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust (access date: 07.09.2019).

European Union Agency for Network and Information Security, *Mitigating the impact of security incidents. Guidelines for trust service providers – part 3*, ver. 1.0, December 2013, online access: https://www.enisa.europa.eu/publications/tsp3-incidents/at_download/fullReport (access date: 08.09.2019).

Krajowa Izba Rozliczeniowa, *Certyfikaty kwalifikowane*, online access: http://www.elektronicznypodpis.pl/oferta/certyfikaty-kwalifikowane/ (access date: 07.09.2019)

Łydziński D., *Procedury zarządzania incydentami bezpieczeństwa*, IT Professional, 2 September 2016, access: http://www.it-professional.pl/temat-numeru/artykul,6780, procedury-zarzadzania-incydentami-bezpieczenstwa.html (access date: 10.09.2019).

PAP, *GIODO: Polak średnio po roku dowiaduje się o kradzieży tożsamości*, 18.05.2015, https://www.pb.pl/giodo-polak-srednio-po-roku-dowiaduje-sie-o-kradziezy-tozsamosci-793371 (access: 15.09.2019).