OBSERWATORIUM . BIZ

ISBN 978-83-954468-1-8

Special Report 2020

TRUSTED ECONOMY
in the new reality.
Mitigation of the risks associated with rapid digitization

MAIN PARTNER:

EFPE ON-LINE

PARTNERS:

Deloitte. Legal

asseco DATA SYSTEMS

POLSKA 5.0

KEY REPORT CONCLUSIONS

The COVID-19 pandemic has accelerated digitization processes, most enterprises have taken intensive measures in this regard over the last 6 months. Companies have focused on enabling teleworking and transferring internal processes to the online sphere, less frequently pursuing projects related to customer service and sales.

Europe needs interoperable electronic document workflow solutions; one of them could be eDelivery which has worked well in some markets, and is planned or already being implemented in others within the framework of digital transformation, but in order to be properly put in place, communication and partnerships are necessary between the commercial sector and regulators at the European and national levels.

Enterprises know about electronic signature and use it mainly for administrative tasks, but less than half of them plan to use it for projected digital transformation projects. Trust services must be more easily integrated with companies' existing IT solutions, take into account user ergonomics and have such a pricing model that will dramatically increase the availability of their applications.

The growing popularity of video-onboarding in the commercial sector and the Trusted Profile in public administration in Poland points to a huge demand for electronic identification services, which could be supplemented with commercial solutions.

Electronic identification itself becomes a key service that should have a transparent legal framework in public administration and the commercial world, and be implemented in a convenient and safe manner for end customers in as many online processes as possible.

Electronic seals have an untapped and underestimated potential as tools that are able to quickly and efficiently address the needs of companies and consumers in the field of secure and confirmed electronic communication between individual business and administrative actors.

Trust services also have the potential to be used in completely new, only now emerging new business processes related to the development of the so-called industry 4.0. In this case, the development of trust services will support key large-scale processes, e.g. scalability, high availability, efficiency, accountability or anonymity. This is where new applications of trust services and synergies with technologies supporting industrial processes, i.e. IoT, 5G, Blockchain, will appear. The disruption of global supply chains will necessitate validation of transactions among individual economic ecosystems.

Table of contents

#paperless

Grow your business with Certum trust services

SimplySign by asseco

Mobile qualified electronic signature

- It has the same legal value as a handwritten signature
- Works on smartphones, tablets and computers
- Enables integration with the service via API
- Provides additional security through two-step authentication

Electronic seal by asseco

Qualified electronic seal

- Ensures the integrity of electronic documents
- Identifies the entity that is the author of the document
- Reduces expenses related to document processing

WebNotarius by asseco

Qualified Validation Service

- Checks the authenticity of electronic signatures from across the EU
- Generates validation evidence recognized in court proceedings
- Verifies that the signed electronic document has not been changed in an unauthorized manner

Time Stamp by asseco

Qualified time stamp

- Protects electronic documents from forgery and anti-dating
- Confirms the existence of the document in time
- It has legal effects of an authenticated date within the meaning of the Civil Code regulations

Hotline +48 91 4801 300
www.certum.eu

Certum by asseco

Introduction

The main purpose of this Report is to answer the question in which areas and how the accelerated digitization of enterprises and public administration proceeded during the COVID-2019 pandemic between March and September 2020. While focusing on the Polish experience, we wish to expand this perspective to other European countries for which the experience of the first months of the pandemic and its consequences was just as if not more difficult. We wanted to pay special attention to the legal aspects in order to be able to verify how legislation was able to keep up with the changes that happened at a pace not seen before.

The situation not only intensified the previously functioning processes of transferring communication or work to the remote formula, but forced digitization in the area of transactions - declarations of will, identification, contract signing. In those areas, for some time already we had had a legal framework in the form of eIDAS, that is a European framework, as well as a tool framework consisting of trust services and electronic identification. Therefore, when working on the report, we tried to verify to what extent those services fulfilled their function and were actually utilized, and to what extent companies or public administration had to use different or substitute solutions. This will determine the answer to the next question; to what extent the developed technical and legal tools will stay with us for a longer time and what changes must occur in trust services and eID for them to become common and useful in the new post-covid normality.

For purposes of the report, electronic surveys were conducted among entrepreneurs and companies declaring implementation of digital transformation projects (N = 41), as well as surveys and direct interviews with law firms in European countries. Additionally, desk research was carried out, which included cataloging product changes of B2C and B2B service providers in terms of the development of electronic channels of customer contact and transaction execution. The development status of electronic identification and trust services was also examined to verify ongoing changes in the context of increasing the availability of such services to a wide group of consumers and companies in order to meet the challenges posed by the pandemic and social distancing requirements.

Chapter 1
COVID - Accelerated Digital Transformation

1.1 Introduction

The time of the COVID-19 pandemic has drastically changed the lives of many people, institutions, entire countries and economies. This difficult situation has taught us - and continues to teach us - in particular, respect for one of the basic needs of every human being: the need to feel safe. We cannot run a business feeling our life and health are in danger, but we also cannot not run a business if we want to survive economically.

The answer to this conflict was the digitization of our daily functioning - the fulfillment of basic needs of life, work, and also handling of consumer and civic matters.

The digital revolution in specific areas of life had already been well advanced before the pandemic. In Poland, the financial market had been at a particularly advanced level in terms of digitization. Actions undertaken in recent years have made it possible to increase the number of citizens using the Trusted Profile, an e-identification tool in contacts with Polish public administration, and the number of available e-services. Across Europe, there has been a systematically growing number of trust service providers operating within a legal framework clearly defined by eIDAS Regulation. On the other hand, many spheres of public and commercial life have remained on the sidelines of the mainstream development of electronic services and remote communication. Often, the electronic document flow mirrored the internal organization of enterprises, not permitting safe and reliable exchange of information or electronic documents among individual business entities, not only cross-border but even locally.

1.2 Fast "post-covid" digitization - business and legal changes

The onset of the pandemic meant for many entities the beginning of rapid changes due to the need to move as many processes as possible to electronic channels. It can be assumed that some of those changes had been planned earlier, but the extraordinary circumstances forced a decidedly faster adoption of numerous implementations.

1.2.1 Remote work

The lockdown made it necessary for millions of Europeans to practically overnight switch to working from home. The Polish legislator noted the need to regulate that sphere of life, which suddenly had to change radically. The legal definition of the place of work performance outside its permanent location opens up a whole range of further issues that need to be solved by entrepreneurs. These include communication within the company and with business partners, preparation of daily corporate records, seeking internal approvals, contracting, and discharge of public legal obligations. All these activities are based on the activities of employees of individual companies or bodies, who in the era of social distancing should be able to perform them remotely via digital channels.

It seems that, at least among Polish entrepreneurs, most changes were made to enable remote work. In the online surveys conducted for purposes of this Report, 23 (56%) out of 41 responding entrepreneurs indicated that during the pandemic their businesses carried out projects to prepare and implement remote work, and 18 (44%) said that they implemented projects to digitize a broadly understood area of human resources management (HR). At the same time, although the law largely allows for the adoption of such digital activities, still not all companies have made use of those tools.

NEW LEGAL SOLUTION

The so-called anti-crisis shield includes temporary provisions allowing an employer to instruct an employee to perform work specified in the employment contract outside the place of its permanent performance. In the near future, according to labor ministry announcements, analogous regulations are expected to be introduced permanently in the Labor Code.

1.2.2 Remote document flow and online contract signing

Another area in which digitization projects were carried out most often during the first six months of the pandemic consisted of in-company internal processes; this was indicated by 21 (51%) out of 41 respondents. COVID-19 contributed to the acceleration of already ongoing efforts to digitize processes within the organization and to instantaneous launch of new initiatives of key significance for daily operation of enterprises.

The experiences of European countries most affected by the pandemic in its first months should be noted in particular. Italy, with had the most advanced and mature e-delivery system in Europe, was able to use it to rapidly migrate business and administrative processes to the online world. The specific nature of that system that certifies electronically the exchange of documents among natural persons, enterprises and administration made it possible to effectively execute transactions, declarations of will, and sign contracts without the need to build dedicated systems for each process and its variants.

MARKET EXAMPLE
Hungary:

TrustChain, an online contracting platform popular in Hungary (but also present in 37 other countries), using, in particular, qualified electronic signatures, recorded an increase in the number of users from 1,000 to 1,500 in the first few months of 2020 alone.

The absence of full effective interoperability at the level of all EU states with regard to e-delivery resulted in the fact that many document flow chains at the level of the common market, which had been paper-based or dependent on physical contact between the parties, became disrupted or a documents flow within those chains significantly slowed down.

At the same time, the conclusions from surveys among European law firms are that virtually all countries participating in our study noticed a significant increase in the use of digital channels in everyday activities (whether factual or legal). Currently, the basic tool facilitating remote business operations

is an electronic signature. In Poland, over 600,000 qualified certificates have been issued, but the number still stands in contrast to the volumes of issued payment cards (43 million, i.e. definitely more than one card per adult resident of the country), which are mass products. However, one should note an increase by approx. 100,000 certificates (17%!) year-on-year. This means that the "paperless" revolution is still far behind the "cashless" revolution rapidly progressing in Poland.

On the one hand, over the years, the tool of the "paperless" revolution was the systematic introduction in Poland of an obligatory qualified electronic signature for selected documents. Currently, the documents signed electronically in Poland are: annual financial statements, employee records, financial documents and powers of attorney.

MARKET EXAMPLE Poland:

Over the last 12 months, the number of qualified certificates in Poland increased 17% from approx. 500,000 to approx. 600,000.

The listing of those documents follows from the legal regulations currently in force, which require most of those documents to be prepared electronically. At present, filing documents only in an electronic form (i.e. signing them in particular with a qualified electronic signature) is necessary, among others, in the following situations:

- **financial statements submitted to the National Court Register;**
- **beneficial owner registration at the Register of Beneficial Owners;**
- **filing ofcompany and natural person tax declarations 8 declarations;**
- **filing of vat register forms;**
- **applications to ZUS (Social Insurance Institution); and soon**
- **filing of reports on payment periods used in commercial transactions.**

The results of the survey of enterprises conducted for purposes of this report show that the majority of respondents who already have a qualified electronic signature use it very often, over 20 times a month. Therefore, it seems that holders of a qualified electronic signature also use it for other purposes in addition to the public legal obligations that can only be completed electronically. This is good news as it proves that the potential of qualified signatures has actually been noted by the customers who have used it at least once.

GROWTH OF POPULARITY

SimplySign - qualified electronic signature service in Poland:

Tomasz Litarowicz
Head of the Security and Trust Services Division
Asseco Data Systems

"The COVID-19 pandemic has resulted in all industries showing a growing interest in digital tools that facilitate remote work and allow business continuity without the need for physical meetings or coming to the office. With their help, we can also improve the flow of documents. Signed printouts do not need to be inserted in envelopes to be sent to the sender by traditional mail. It is enough to sign a file electronically and send it by email or via an internal document flow. Additionally, with the use of a mobile qualified electronic signature, SimplySign, we can carry out our tasks at any place and time. At the peak of the lockdown, interest in that tool was 600 percent higher than the year before. The fact that we are increasingly adapting to working remotely makes us more willing to use tools of this type."

asseco DATA SYSTEMS

In addition to electronic signature as a tool in itself, the time of the pandemic has also opened up space for the development of so-called signature platforms that make it possible to conveniently execute and secure the entire process of creating and signing an electronic document using electronic signatures that may or may not be qualified, but have the nature of, for example, an advanced signature and, which is very important, should always be chosen by customers based on prior risk analysis and legal requirements.

GROWTH OF POPULARITY

Platforma Autenti:

Tomasz Plata,
Vice President of the Management Board
Autenti

In the current situation, interest in Autenti platform services has increased significantly. Only in March and April of this year, we noted a nearly fourfold increase in interest compared to the previous months. This is a very big leap. E-signature has become an indispensable tool in business operations. Those who were still hesitating and were not convinced about this type of solutions had to quickly adapt to today's reality. Entrepreneurs will not return to traditional solutions in business operation and will appreciate the e-signature which is simply a very straightforward, effective and also sustainable tool.

AUTENTI®

MARKET EXAMPLE
BFF Banking Group

Paperless in the financial sector - a case study on the implementation of trust services by Asseco Data Systems at BFF Banking Group in Poland.

The aim of the project was to create a process aimed to conclude operational contracts that would eliminate manual registration and signing of documents, while maintaining compliance with legal and transaction security standards.

Key services used in the project:

- Qualified electronic signature through the SimplySign service
- Qualified electronic seal
- Qualified time stamp
- Qualified validation service

Implementation results:

- Shortening the period of signing operational contracts from 7 days to 1 day
- A convenient and safe process for BFF's members of the management board andemployees, enabling the signing of documents at any place and time
- Possibility to verify the identity of the BFF's contractors by its employees in order to issue a qualified electronic signature

Development plans:

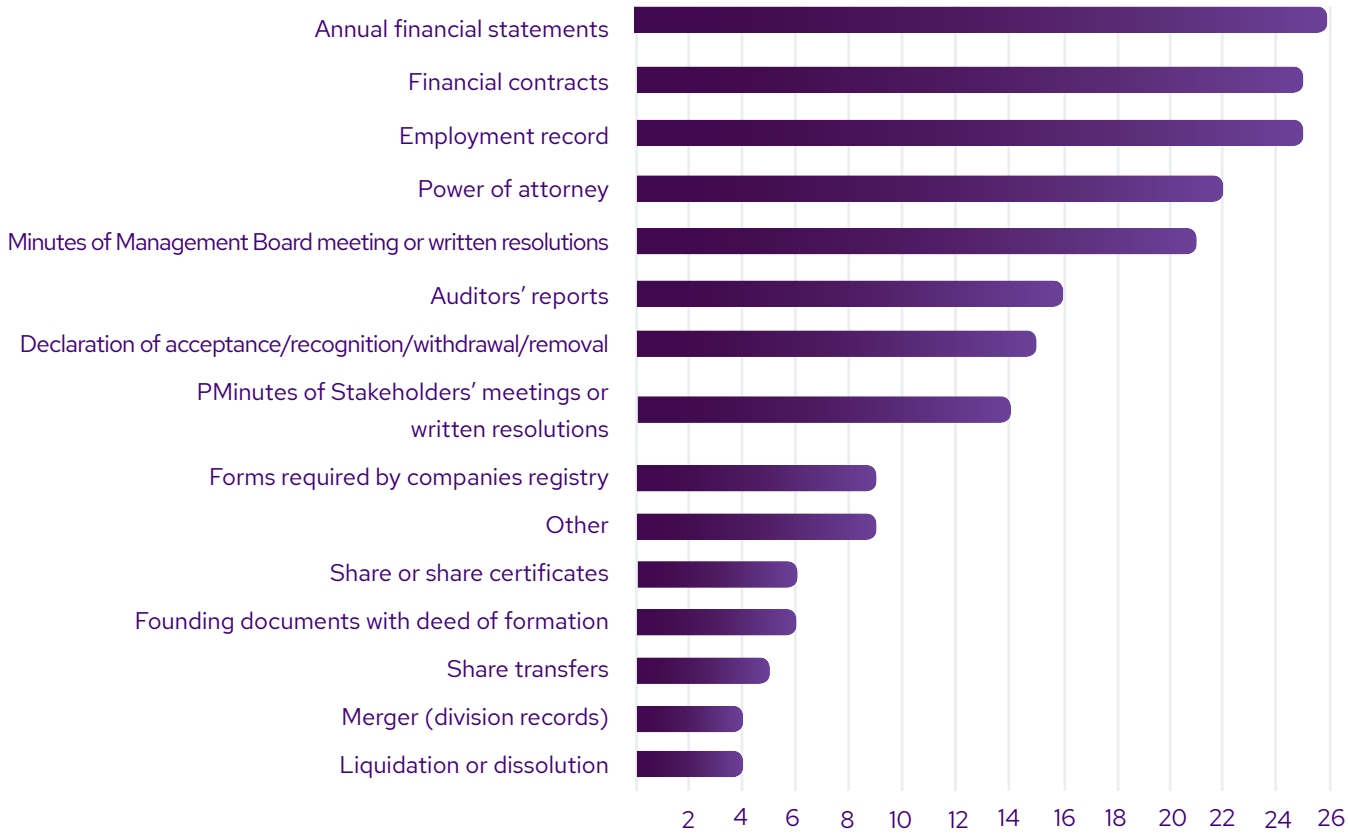
- Integrating the Electronic Document Circulation with a qualified validation service
- Implementation of the process of electronic delivery, enabling the sending of documents in electronic form with acknowledgment of receipt – the implementation depends on the adoption of relevant legal regulations
- Implementation of electronic files of employees

The impact of COVID-19 on the implementation of the process:

- In March 2020, BFF accelerated the completion of the process – already in place – of abandoning paper by signing operational contracts in the electronic form;
- Only those documents that, for various reasons, could not be signed in electronic form, are still signed in paper form
- The requirement to stamp documents with a certain date, necessary from the point of view of the provisions of the Restructuring Law and the Bankruptcy Law Act, was met thanks to the use of a qualified electronic time stamp;

As part of our online survey, we asked respondents to indicate the type of formal documents for which they would use an electronic signature. Here, we can distinguish three groups of documents. Most frequently indicated were annual financial statements (26 responses - 63%), financial agreements, i.e. loan agreements, security agreements, investment agreements, etc., received 25 responses (61%), while employment records, including employment contracts, internal policy documents, regulations, internal requests /employee applications also got 25 affirmative responses - 61%, powers of attorney (22 responses - 54%), minutes of board meetings or written resolutions (21 responses - 51%). The following chart shows a list of all identified uses along with the number of respondents:

For witch formal documents would you use an electronic signature?



MARKET EXAMPLE
Santander Consumer Bank

Is a pen needed to sign a contract? - a mini case study of implementation by Asseco Data Systems of an advanced one-time electronic signature for customers at Santander Consumer Bank SA.

The aim of the project was to create a process of signing a consumer loan agreement in line with the idea of paperlessness, EU eIDAS regulations and the highest user experience standards for the Bank's customers and employees.

Asseco Data Systems and Bank Santander built a solution that combines all aspects of the process involved in executing a loan agreement: legal, technical and organizational issues.

Key services used in the project:

- Advanced one-time electronic signature, authorized with an SMS code, placed by the Bank's Customer
- Qualified SimplySign electronic seal - placed by Account Manager on behalf of the Bank
- Qualified validation service

Implementation results:

- 30% shorter process of concluding a contract with a client
- 80% of Bank's counterparties attest to process simplicity
- 40% of Bank's counterparties consider the absence of paper in the process as its key advantage

Development plans:

- Electronic signature available to over 30,000 Bank's counterparties
- Electronic signature available to Bank's customers in over 300 branches

Santander Consumer Bank

1.2.3 Electronic invoices

In Poland, a popular paperless area are accounting transactions, in particular, electronic invoicing. Electronic invoicing had already been widely used before the COVID-19 pandemic. As a consequence, companies' financial departments in particular are digitized to a large extent, while commercial departments operate based on previous habits and using old, analog processes.

Provisions of the act on tax on goods and services allow the use of both paper and electronic invoices. An electronic invoice is an invoice that is issued and received in any electronic format.

The condition for electronic invoicing is to ensure the authenticity of origin and integrity of the content of invoices issued in this form. These features may be guaranteed, in particular, by a qualified electronic signature or a qualified seal. However, this is only one of the ways of meeting those conditions, that can be replaced by a different business control procedure.

1.2.4 Remote meetings of corporate bodies

The Polish so-called anti-crisis shield has made permanent amendments to the Commercial Companies Code, which permit both meetings of supervisory boards, management boards and owners ,meetings (shareholders' meetings, general meetings) to be held using means of remote communication.

Remote proceedings themselves with the use of ICT systems were previously available to Polish companies to a limited extent. The novelty is that the right to hold such remote meetings will now also apply in a situation where it is not explicitly provided for in the company's deed of formation or articles of association. However, the deed of formation or the articles of association may exclude that option.

The need for remote meetings of corporate bodies seems to be more universal. Certainly, in some countries it had previously been possible to make corporate decisions electronically (e.g. in Serbia and, in some cases, in Malta). As to other surveyed countries, virtually all of them at least temporarily introduced this option in their local laws during the pandemic. These include the following common market countries: Norway, Sweden, Denmark, Portugal, Ukraine, Slovenia, Hungary, the Netherlands, Italy, Romania.

1.2.5 Remote client registration and on-boarding

Public administration

In Poland, the essential tool related to electronic identification, developed as a direct response to the pandemic, is a temporary electronic identification mean called Trusted Profile.

It is somewhat of a sub-type of the standard Trusted Profile. Trusted Profile itself is no longer a new tool. It is a free electronic identification means that permits confirmation of users identity in electronic administration systems. It was created to enable fully electronic contacts with public administration (agencies, ministries).

A temporary trusted profile is simply a trusted profile of a much shorter period of validity, which is three months at the moment. On the other hand, a completely new aspect that distinguishes a temporary trusted profile is that it may be obtained completely remotely, even if one is unable to set up a trusted profile through electronic banking. Identity confirmation occurs during an online video interview with an official.

NEW PRODUCT SOLUTION

Greece:

In Greece, it was during the pandemic that the „Single Digital Portal" began to operate, supporting execution of over 500 administrative matters for Greek citizens and business entities conducted online with an official.

During this holiday season, a trusted profile was set up by over 624,000 people, as reported by the Ministry of Digitization, and the service is already being used by almost 8 million citizens - there are also Foreigners using TP but they need to have PESEL. In the e-summary of this year's holiday season, we can find a note that between the beginning of July and the end of August, „well over a quarter million electronic general filings" were made and nearly 26,000 births of children were reported online. The digitization ministry announced that „this year's holiday season, that is from the beginning of July to the end of August, exactly 624,128 people set up their trusted profile. This is almost a quarter million more than during the same time of last year.

The stream of these changes and e-administration building encompasses, for example, the introduction of e-box, but also the long functioning gov.pl portal, serving as an intermediary step to the ePUAP platform for all those who do not have a trusted profile. The need to build modern e-administration is a trend that goes beyond our domestic Polish market.

Banks

The issue of video verification as a method of credible identification of people without the need for their physical presence at a customer service point has long been discussed in the context of talks about full digitization of business processes. It is obvious that the first step in counterparty relationships is to confirm their identity. In an overwhelming majority of these relationships, there are no legal obstacles to carry out such verification by all available means, making sure merely that the probative value of the process is safeguarded.

However, there are sectors deprived of this freedom to choose identification tools or methods due to the absence of appropriate legal regulations or excessively restrictive interpretation of the existing laws.

Banks and financial institutions are subject to significant regulatory rules meant to secure transactions and ensure market transparency. The legal framework for preventing and combating money laundering and terrorist financing as well as implementation of the Payment Services Directive requires banks, in particular, to verify the identity of their customers (KYC procedure, strong authentication) in order to assess the potential risk of illegal practices.

In the European market, two-factor authentication (known as 2FA) is most commonly used. Strong authentication is achieved by using in parallel two different identifying data (e.g. password and card/token).

Meanwhile, already in 2019, the Polish Financial Supervision Authority published an official position on customer identification and verification of customer identity in banks and branches of credit institutions based on the video-verification method (the position of the PFSA Office of 5 June 2019), in which, above all, the PFSA directly stated that "the bank can use the vid-

MARKET EXAMPLES EUROPE

Germany:

The German Anti-Money Laundering Act (Geldwäschegesetz, GwG) provides that identity verification can be carried out not only on the basis of a conventional ID card. According to that act, verification can also be carried out on the basis of an electronic ID card or even a qualified electronic signature.

Portugal:

In the banking sector, the entire process starting with client identification and identity confirmation can be carried out remotely through the use of videoconferencing and the support of trust service providers.

Mobile applications also often use mechanisms based on customer biometric data, such as fingerprint and face shape recognition.

Greece:

In the Executive Committee Act 172/1/29.05.2020 (Executive Committee Act), the National Bank of Greece defined the terms and conditions for digital on-boarding of clients of banks and other regulated entities. Key methods in this process are:

- video-conference with a properly trained employee, deemed to provide the highest level of security; and
- automated procedure using a dynamic selfie, which requires additional security measures.

eo-verification method."

At the outset, however, it was pointed out that in the case of remote customer registration, the means of electronic identification referred to in eIDAS, including in particular a qualified electronic signature, are the most reliable to use

"The position of the PFSA Office of 5 June 2019 contains a number of guidelines on the use of video-verification services that should be considered by the bank when choosing this method of customer identification. In the first instance, it is recommended that the principles and best practices related to that service be framed into a formal procedure"

The PFSA, formally opening the way for banks to use video-verification, also indicated that, while maintaining the principles and best practices described in the position discussed, video-verification services may also be offered by other

MARKET EXAMPLES POLAND:

Alior Bank

The client proves his/her identity during the loan purchase process, if he/she so wishes. This is intended to facilitate and speed up the entire process, and make it less stressful for the client. Another solution which is based on the same photo ID service allows for remote on-boarding of new clients - identity is confirmed through recognition of customer's biometric features and their comparison against the photo in the ID card.

Nest Bank

Another bank that offered or actually expanded the option for its clients to set up a bank account using video verification is Nest Bank. The bank had been offering this option practically since the beginning of its operations, but it was disabled in April and restored in May for individual clients, and in June, the bank made the functionality available also to corporate clients. The identity verification process is the same for both client groups and requires only an ID card and a computer with a webcam. The service is available during consultants' working hours.

supervised institutions.

Banks can also be identity providers for eID solutions offered by the so-called identity brokers; one example is the mojeID KIR service, which already has a total of 13 implementations, including in entities such as PGNIG or PZU, and according to press reports, in August alone, Totalizator Sportowy acquired 10,000 new clients with the use of mojeID.

It should be emphasized, however, that in digital identity it is crucial for it to be widely open to both "givers" and "takers" of identity, with business aspects posing the only limitation.

Digital identity enables the development of modern remote trust services (e.g. electronic signature in the cloud) that make it necessary to address the issue of a comprehensive remote authentication mechanism. According to the eIDAS regulation, user registration in such a service may be carried out on the basis of electronic identification with a medium or high level of reliability, provided that initially identity was confirmed in person. Thanks to the electronic identification mechanism, the user who wants to use a qualified service does not have to appear in person at the registration point and the entire service can be performed remotely. Also other trust services, if they require the initial user registration, will use electronic identification mechanisms.

REPORT EXPERT

Miłosz Brakoniecki
Partner Obserwatorium.biz

Regulators in the European Union are looking for a solution that ensures a uniform and interoperable model of electronic identification at the common market level. The "European eID" can be an identification service to be provided by notified commercial entities or by national states. The new approach in this area must certainly meet the highest security standards while simultaneously being universally available and operable in administrative and commercial e-services in all EU countries.

OBSERWATORIUM . BIZ

Insurance companies

The Polish insurance market has also accelerated comprehensive digitization of its services. Regulators have intensely and consistently supported this trend. Regardless of the position of the PFSA Office of 5 June 2019, strictly in connection with the COVID-19 epidemic, the PFSA issued the Supervisory Impulse Package [Supervisory Impulse Package for Security and Growth in the Insurance Market Area] which expressly allows the process of concluding an insurance contract to be carried out by electronic means, subject to client's consent. In this case, however, one must remember to properly document the individual elements of the contracting process.

Independently, the Polish Chamber of Insurance has issued "Recommendations of pro-customer measures for the insurance market", in which it recommends, inter alia, introducing a simplified process for contract renewal, new contract execution or, at the client's request, contract extension for contracts expiring during the pandemic. The recommendation also mentions remote visual inspection and telemedicine.

Trust service providers

When talking about remote identity verification, it should be added that trust service providers must also use rigorous client identification procedures similar to those of financial institutions. Here, too, a change in the approach to the methodology of such verification can be observed.

The first processes have emerged for remote identification of contractors wishing to purchase a trust service from a provider for the first time.

MARKET EXAMPLE
Switzerland:

In Switzerland, it was precisely in connection with the pandemic that e-signature providers were allowed to onboard new clients in the process of videoconference-based e-identification.

REPORT EXPERT

Andrzej Ruciński
Asseco Data Systems

We are observing a very disturbing development in Poland. A foreign provider, while being subject to regulators in his own country, may, for example, use a method approved in that country for automatic video verification of the identity of a person applying for a qualified signature certificate. Thus, that provider can serve customers, for example, in the territory of Poland. On the other hand, the lack of unequivocal legal regulation of solutions based on video verification and remote paths at the level of our country causes interpretation chaos, which significantly hinders the use of such solutions by Polish providers. This puts our companies at a disadvantage on the market of trust services, not only in Europe, but even our own country.

1.2.6 Education and CSR activities

Serious barriers to the implementation of the above-mentioned digital solutions have often included: the lack of digital competence or the costs and unfavorable infrastructural conditions for using this type of services. When building and developing qualified services that guarantee the right tools and security, it is worth using those experiences in the context of disseminating, popularizing and increasing the availability of solutions which ultimately have a chance to bring the culture of safe use of digital products and services to a higher level

1.2.7 Untapped opportunities – remote contracting in utilities and telco sectors

The pandemic has not been a sufficient incentive for functional changes in the utilities and telco markets in terms of implementing effective remote customer acquisition processes. Purchasing utilities services is a domain where there has been little change for several years, which we have already pointed out as Obserwatorium.biz in the report "Digitization energy - the status and directions of development of a digital service channel for energy and gas suppliers in Poland" in 2017. Among the leading Polish energy and gas suppliers, only two offer online contract signing to potential customers. Those suppliers are Energa, a gas and electricity supplier focused on northern and central Poland, and Lumi, an entity operating in Warsaw, originating from the PGE brand. In the first case, a new customer may receive the contract by email, in the second case, the contract is signed via the previously described Autenti signature platform. Such solutions not only make it easier to change the energy supplier, but permit greater conversion; a potential customer does not have to read the offer on the Internet, make an appointment at the office and sign the contract there. The new customer is served comprehensively within one channel and can arrange everything there without leaving the computer. The solution is also ensured by the Rachuneo platform working with Lumi.

Signing a contract with electricity supplier	Enea	Tauron	PGE	Energa	Innogy	Lumi PGE
Online process	NO	NO	NO	YES	NO	YES
Online application, completed by courier	NO	YES	NO	YES	NO	YES
Contact form	YES	YES	YES	YES	YES	YES

The market of mobile operators looks similar. Only two of the leading providers offer products that can be purchased entirely online, including contract signing; it should be noted here that these are not "standard" offers from those suppliers, but rather products addressed to selected market segments. Those providers are Orange with its Orange Flex offer and T-Mobile (the Heyah brand with the Heyah 01 offer). In the case of Orange Flex, the service is activated via a mobile application also used to manage the service and payments; Heyah 01 uses the MojeID KIR solution in the process, more on which in the frame. In the case of the remaining major operators in Poland, apart from signing the contract in person at the operator's office, it is only possible for the contract to be signed via a courier.

New number	Play	Plus	Orange	T-Mobile	Heyah 01
Online process	NO	NO	YES	NO	YES
Online application, completed by courier	YES	YES	YES	YES	YES
Contact form	YES	YES	YES	YES	NO

As for electronic contracting of Internet or Internet and television services, again only a few providers offer that option. One of the larger, local providers allowing their potential customers to conclude contracts remotely via the electronic channel is Toya in Łódź, where the process looks very similar to that of Energa: the customer receives the contract by email, once the contract is accepted work continues and the Internet is hooked up. Another practice is used by the Canal + platform which only supplies television; a new customer can sign the contract via the Internet and payment of the fee is considered equal to execution of a binding contract (of course, with the option of termination within 14 days).

TV + Internet	Inea	Netia	TOYA	Orange	Canal +	Cyfrowy Polsat
Online process	NO	NO	YES	NO	YES	NO
Online application, completed by courier	NO	NO	NO	NO	NO	YES
Contact form	YES	YES	YES	YES	YES	YES

Therefore, from the user's perspective, there is no option of fully remote customer service in terms of registration and remote contracting. This is definitely a broad business area to be developed by the providers of electronic identification and trust service-based solutions, especially since in the coming months restrictions on the operation of branch offices in those sectors and inefficiency of courier companies may increase again.

REPORT EXPERT

RISKS INVOLVED IN "CARELESS" DIGITIZATION

Michał Tabor
Partner
Obserwatorium.biz

Accelerated digitization of business processes was often necessary at the time we were surprised by the pandemic and the resulting lock-down, followed then by the continuing limitations arising from social distancing, greater popularity of remote work or restricted operation of many "on-ground" commercial and administrative entities. At the same time, implementation of makeshift solutions for the time being, due to their imperfections, carries an entire pool of risks, starting with the fact that many of those "quick implementations" could remain virtually unchanged due to the costs incurred. Other risks involved in "careless" digitization are:

- Implementation cycle too short, hence omitted analysis of risks and compliance, and resilience testing;
- Solutions implemented without analyzing user ergonomics, which may discourage customers from using a given functionality in the long term;
- Lack of market analysis or legal analysis prior to implementation, hence the cheapest or random solutions are chosen, that may ultimately prove to be useless, non-scalable or may not meet security requirements.

It is important that, given the experience to date, we adopt changes in processes based on business analysis and risk analysis, taking into account the functioning and available trust services.

OBSERWATORIUM . BIZ

Chapter 2
REGULATORY PERSPECTIVE – POLAND EU

2.1 Definitions and concepts

One of the main legal aspects of the digitization of business and administrative processes has always been the issue of effective electronic contracting (remotely and without generating the need to send paper documents).

According to the eIDAS Regulation, there are three levels of electronic signatures in legal transactions:

the so-called **ordinary electronic signature** - the most basic one, without any specific technical requirements;

advanced electronic signature which meets technological and legal requirements specified in eIDAS;

qualified electronic signature that is one based on a qualified electronic signature certificate and created with the use of a qualified signature creation device;

The eIDAS Regulation introduces a clear rule: an electronic signature cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that the signature is in an electronic form or that it does not meet the requirements for qualified electronic signatures (Article 25(1) eIDAS).

On the other hand, the key legal effects with regard to a QUALIFIED ELECTRONIC SIGNATURE are stated in para. 2 of that Article 25 eIDAS. Namely, the provision states that **qualified electronic signature shall have the equivalent legal effect of a handwritten signature.**

In other words, a qualified electronic signature, already under EU law, may replace a handwritten signature without the need to adopt additional provisions in national legislation. This significantly distinguishes its legal force from other types of electronic signatures.

When we add to this, in accordance with Article 25.3, its cross-border nature: a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member States, we obtain one strong tool for declarations of will throughout the EU.

If one wishes to perform possibly all transactions electronically and use the provisions of eIDAS, it is important to know what type of signature can be used for a given legal transaction.

First of all, it should be noted that, both in Poland and in the vast majority of European Member States, civil law expresses the principle of freedom to choose the form of a legal transaction. It is only if a specific form is stipulated for a specific transaction, then the choice of tools for that transaction should be limited or it should be considered whether the possible consequences of not keeping the form stipulated by law would be acceptable to us (the effect will not always be invalidity of the transaction).

In Poland, we distinguish in particular:

written form
-the most common form of legal transactions.

It is very much embedded in our culture. In order to preserve a written form of a legal transaction it is sufficient to affix a **handwritten signature** on the document which expresses the transaction's content.

electronic form - equivalent to written form.

In order to preserve an electronic form of a legal transaction, two conditions must be met: a declaration of will must be made in an electronic form and a qualified electronic signature must be affixed on the declaration.

documentary form

To preserve this form, it is sufficient to make a declaration of will in the form of a document in a way that permits identification of the person making the declaration. The document is simply any information medium which makes it possible to read the information content. The main difference between this form and the written form (or electronic form) is, therefore, no need to affix a handwritten signature (or a qualified electronic signature) on the document. We preserve the documentary form in the case of a text document with a signature duplicated mechanically (e.g. photocopy, scan), as well as an electronic message (email) ended with the first and last name of the author or the data permitting identification of the author. But in some situations this will also be clicking on „Accept" on the website. All of these forms are meant to associate an identifiable person with the information stored electronically. Therefore, the documentary form will include the use of both an ordinary electronic signature and an advanced electronic signature.

The point is to identify which of the above forms of legal transactions will be appropriate for the activity we wish to digitize. With this knowledge, we can properly select the level of electronic signature.

Forms of legal transactions (Civil Code)	Preserving legal form electronically
Notarial Deed	**No electronic form**
Written form with notarized signatures	No equivalent electronic form - possible **electronic copy** of the paper original, certified true by a notary public with a qualified signature.
Written form with officially certified date	**Electronic form + qualified time stamp** a document bearing a qualified electronic signature and marked with a qualified time stamp (certified date)
Written form	**Electronic form** – - an electronic document bearing a qualified electronic signature - there is a legal presumption of authenticity of the document and the signature
Documentary form	**Any method of registering** a declaration of will making it possible to read the content of the declaration and to identify the person making the declaration. In the case of electronic form, depending on the type of electronic signature used, the probative value of the electronic document will be different.
Paperless form (np. forma ustna lub domiemana)	**Important:** If the law stipulates, under pain of nullity, that a legal transaction must have a written, documentary or electronic form, a transaction performed without observing the stipulated form is invalid.

Important: If for a given legal transaction (e.g. contract execution) a written form is required under pain of nullity, failure to comply with that requirement results in the transaction being null (e.g. invalid contract)

In the practice of various EU Member States, the legal weight of individual e-signatures varies considerably.

One more concept underlying the EU regulation of Trust Services and electronic identification should be mentioned. Namely, technology-neutrality, as a guarantee that legal regulations related to electronic turnover will not become obsolete and inadequate to the development of new technologies. This is a characteristic feature commonly included in legal regulations concerning electronic identification and electronic turnover. The principle of technology-neutrality is also the basis for equal treatment by public authorities of various technologies and for the creation of conditions for their fair competition, including preventing the ability to eliminate competing technologies when expanding the ICT services market.

2.2 Barriers to digitization vs operating practices in various

The world of digitally-run business should probably be divided into that from before the COVID-19 pandemic and after the spread of COVID-19. In the pre-pandemic world, it was clear and repeatedly raised in various forums, that the ability to run business fully electronically in relations with customers, public administration and internal resources was severely limited in many countries.

What was a barrier to digitization at that time has remained such to some extent, although for obvious reasons it has lessened in importance in the face of the urgent need for social distancing across all economic activities.

„Not in all European countries preservation of a written form is the main cause of delays in digital ."

Still, the main problem remains the need to preserve a written form for various types of transactions. However, it must not be forgotten that, under Polish law, that form will not be necessary for a vast majority of transactions. On the other hand, those transactions that require a written form can be freely replaced with a qualified electronic signature.

MARKET EXAMPLE

England:

In England, the concept of „in writing" and „in document" seems to be no longer controversial. In 2001, the Law Commission published the advice addressed to the UK Government explaining the above concepts, stating that both could also exist in an electronic form.

[Electronic commerce: formal requirements in commercial transactions – Advice from the Law Commission (2001), https://www.lawcom.gov.uk/project/electronic-commerce-formal-requirements-in-commercial-transactions/

Poland:

In order to obtain information about a contractor from the Economic Information Bureau (BIG), an appropriate authorization signed personally by the consumer must be submitted. This requirement is stated directly in the BIG instructions for completing authorizations. As a result, the authorizations must be submitted in writing, although no similar requirement is found in legislative provisions.

However, the entrepreneurial practice lacks:

- reliable verification of legal requirements - most often we simply assume that a handwritten signature on paper will be required, even where the law does not stipulate any specific legal form for a given transaction;
- confidence in the legal effectiveness of electronic signatures.

MARKET EXAMPLE

Romania:

In Romania, the legal situation is peculiar as the act which was supposed to adapt the national law to eIDAS has not yet been adopted. On the other hand, eIDAS itself leaves some freedom in shaping specific requirements as to the legal form of selected transactions.

While a qualified electronic signature is generally honored in commerce, the legal effectiveness of an ORDINARY ELECTRONIC SIGNATURE and an ADVANCED ELECTRONIC SIGNATURE is not entirely clear.

Controversies are mainly related to the practice of signing an employment contract with non-qualified electronic signatures. The problem boils down to the practice of the Territorial Labor Inspectorate which is reluctant to consider thus signed contracts as valid, which in turn may expose the employer to fines for potentially neglecting the duty to deliver the „original" employment contract to the employee.

Often the barrier is not the very form of the transaction provided for in the regulations, but the form in which the document can be accepted by a given state body, a public registry, whether because of specific implementing regulations or because of established practice. While the position of a registry may not generally affect validity of a document, it may be necessary to register the document in order to make it enforceable in Poland or abroad. Therefore, whether the registry can or will accept signatures in a certain form has real significance for the effectiveness of the legal transaction in question.

We are still afraid to use electronic versions. Many concerns result from poor knowledge of the technical capabilities of electronic signatures and the legal consequences of their use. Are they used correctly? Are they legally valid for a given transaction? What is their probative value? As we go down to the level of very specific processes, detailed practical problems also begin to emerge.

Such legal issues that are difficult for recipients of trust services include, for example:

- **Is the fact that an electronic document does not have one or a limited number of original copies a disadvantage or an advantage?**

Here, it obviously depends on the process. Considering, for example, electronic invoices, it is worthwhile for that reason to ensure good control of access points to the document in order not to duplicate related management activities, such as multiple payments of one invoice. Nevertheless, the „multiplicity" of originals is precisely one of the main advantages of e-documents making it possible to optimize the workflow in which there is no need to wait for one paper original to „circulate" through all its stakeholders.

- **Can each of the parties to the contract sign it in a different legal form?**

This is principally considered acceptable. This will be especially practical in a situation where one party will want to sign the contract with a qualified electronic signature, while the other party will not want or be able to place an electronic signature. Then it will be possible to conclude one copy in a standard written form and one copy in an equivalent electronic form. However, it is necessary to remember to first check the statutory requirements for the form of transaction and the related clauses of the contract itself. After signing the contract, it is also necessary to ensure that the parties exchange copies of the signed contracts.
.

- **How to demonstrate the powers of a given person to act on behalf of a legal entity when signing a contract electronically?**

In Poland, this is not an easy question. In technological terms, it is perfectly feasible to include a job description and the company being represented in an electronic signature. This option is available, for example, for electronic signatures issued by Asseco.

Similarly, on e-signature platforms, there are sometimes fields with details about the company being represented by the signatory and his/her capacity within that company.

To enhance the probative value, one may consider placing additionally a qualified seal of the entity on whose behalf the contract is to be entered into next to the personal electronic signature.

Nevertheless, the above-mentioned additional elements in the e-signature, and even the addition of e-seal of the represented entity has basically no legal value, apart from possibly enhancing the probative value of the thus performed transaction should it become necessary to demonstrate that a given party's intention was not to act in his/her own name but in the name of another entity.

MARKET EXAMPLE

Portugal::

In addition to classic identification and signature tools, Portugal has:

- national eID (Cartão de Cidadão [Citizen's Card] - CC eID), i.e. electronic card eID;
- mobile eID (Chave Móvel Digital [Digital Mobile Key] - CMD eID), which is a means of authentication and digital signature certified by the Portuguese state;

introduced one more solution:

- the Professional Attributes Certification System (Sistema de Certificação de Atributos Profissionais - SCAP).

SCAP is used to authenticate the functions that the owner (natural person) of a Portuguese CC eID or mobile CMD eID performs in the society as a qualified specialist or the powers and the scope of authorization he/she holds in a public or private company.

Both CC eID and CMD eID can be combined with a qualified electronic signature. On the other hand, by integrating all these functions within SCAP, we obtain an extremely interesting solution that combines professional qualifications or functions within an organization of a given natural person using a QUALIFIED ELECTRONIC SIGNATURE with the act of signing a specific electronic document.

The use of SCAP eID is optional for holders of a valid Portuguese CC eID or CMD eID aged 16 and over.

The limited framework of this report does not allow us to focus on each of the problems and controversies (even among the most common ones) that users of trust services have to face. However, these are not unresolved issues. Therefore, it is worth independently taking care of a reasonable and comprehensive approach to implementing digital solutions in the company, and if in doubt, consult it.

2.3 Security of electronic documents turnover

Probative value

If no legal provision stipulates a specific form for a given transaction, there is no need to consider validity or invalidity of an electronically signed transaction. However, there is still the issue of the probative value of a transaction performed in this form.

An ordinary electronic signature may meet all the requirements for a document signed with it to be recognized as actually „signed" in the legal sense. The thus signed document may then be admitted as evidence in court proceedings

Article 25(1) eIDAS says: An electronic signature cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that the signature is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

However, the parties will also have to consider the probative value of a thus prepared electronic document in the event of a dispute, for example, as to who actually signed the document, whether it expresses the party's intention to be bound by a given contract, or what is the document's content.

Under Polish law, for evidence reasons, the most desirable electronic form of documents drawn up in relations with counterparties seems to be an electronic form with a qualified electronic signature. This is due to the fact that such a form constitutes a private document as defined in the Code of Civil Procedure. A private document is any text document containing the issuer's own handwritten or qualified electronic signature. The use of an ordinary electronic signature will not be sufficient to create a private document (in the meaning of procedural regulations).

Meanwhile, it has the advantage of enjoying the presumption of truthfulness (authenticity), i.e. the presumption that the document comes from the person who signed it. In addition, it also enjoys the presumption that the person signed in the document made the declaration contained in the document.
From a practical point of view, if in a dispute the other party argues that a private document (a document signed with a qualified electronic signature) is not authentic, that party will have to prove its point.

As mentioned at the beginning, a document validly signed with an ordinary electronic signature or an advanced electronic signature should also be admitted as evidence in a case. However, its probative power will be much more up to the judge's discretion.

When using this lower electronic form, it would be advisable to ensure that the transactions of this type are documented to an appropriate extent for purposes of possible evidentiary proceedings. In particular, it should be possible to fairly easily demonstrate in the event of a dispute:

- that access to the electronic document was obtained from a specific email account or computer, and at a specific location;
- that access to the document was obtained with the use of a password, PIN, encryption key and/or other authentication process;
- that the time of signing was specified;
- whether there are any differences between the signed document versions held by various parties.

Certainty of turnover

The fact that an electronic signature is legally binding does not yet determine how secure and reliable it is, nor does it decide its probative value. Meanwhile, it cannot be denied that security and reliability are important for the parties.

Uncertainty or ignorance of legal regulations makes it difficult to use electronic signatures. Practical issues, such as security of electronic signatures, their availability and ease of use (intuitiveness) are also a significant barrier.

Users of the technology on which trust services are based will typically not understand its underlying system and may not be able to judge its reliability. Therefore, it is definitely advisable to consider the use of additional methods that will increase trust in the technologies used and introduce the necessary tools that provide greater certainty, e.g. as to correct identification of the parties, their authorization to act on behalf of another person or entity, correct content (version) of the document to be signed. Properly selected methods can facilitate evidence gathering in the event of a dispute.

One of such methods that guarantee a certain service level and technology security is the use of a trusted third party (TTP) subject to certification and constant supervision. In the are of Trust Services, the role of such trusted third party is fulfilled by qualified trust service providers. Standardization of Trust Services at the EU level and certification of their providers is meant to guarantee safety for users, that is, according to the eIDAS terminology, for the "relying party".

In the context of securing electronic processes, an interesting phenomenon are **platforms for electronic signatures** and e-document exchange, including those fully automated, i.e. EDI (electronic data interchange).

The advantage of using such platforms is that they are accessible from anywhere and provide full visibility of the signing process as well as facilitating verification and editing of the electronic documents themselves.

Another advantage is that when a transaction is performed on the electronic signature platform, a digital footprint is generated, documenting the entire process. Document signatories (including their email and IP address), any additional steps taken to authenticate the signatory (e.g. a code sent to the signatory's mobile phone) are recorded, and the digital footprint itself usually includes an electronic seal or at least an electronic time stamp. This digital footprint can also be used in the event of a dispute during evidential proceedings.

"A variety of this type of platforms, especially recently gaining in importance, are electronic platforms for remote voting".

MARKET EXAMPLE

Norway:
In Norway, standard teleconferencing tools such as Zoom and Teams have become extremely popular for this purpose.

However, there are also many platforms specialized in arranging shareholders' meetings, enabling, for example, secret voting in a safe environment.

When using such platforms, one should not forget about the provisions on personal data collection and processing. In particular, it should be noted that these regulations may differ based on whose data are involved (citizens of which country).

Russia:
Under the Law of Place in the Russian Federal Law on Personal Data (No. 152-FZ), personal data of Russian citizens held by data controllers must be processed on servers physically located in Russia. Therefore, it is so important to identify and consider the risks associated with the use of foreign platforms.

2.4 Cross-border nature of trust services

eIDAS affirms the principle that all electronic signatures are inherently legally effective. Moreover, the EU regulation aims to ensure a common standard of electronic signature (including with particular emphasis on one, high standard of qualified electronic signature). The purpose of such standardization is, first of all, to ensure that the legal validity of a qualified electronic signature is recognized in all Member States, even though it is issued in only one Member State. Taking into account the results of our study, we can only talk about the formal cross-border nature of trust services, enshrined in EU regulations and theoretically respected in all national legal regimes. In practice, however, entities from a given Member State choose their national trust service providers, and electronic signatures of foreign providers are still rare. On the other hand, the borders of EU countries are crossed by platforms for signing electronic documents. DocuSign and AdobeSign, in particular, are the most widespread platforms and are present in virtually every Member State. Perhaps the cross-border nature of trust services will come this way, i.e. through their use on international signature platforms.

e-Notarization

The problem of the lack of cross-border nature is wider. The mere fact that a transaction performed with the use of an e-signature is recognized as valid does not yet guarantee its enforceability, and especially its enforceability in another country.

The cross-border enforceability of electronic legal transactions is related to at least 2 issues that are still waiting to be addressed in the process of commerce digitization. Namely:

1 the problem of **e-notarization** not resolved in most European countries;

2 no real possibility of electronic **legalization of foreign documents.**

e-notarization

Our study shows that transactions requiring participation of a notary could be named first among basic legal areas as those that still resist digitization.

Among the countries we have surveyed, participation of a notary public is generally required for:

- **legal transactions related to real estate;**
- **transactions performed in the area of family or inheritance law;**
- **drawing up founding deeds of commercial companies;**
- **sometimes also for transfers of shares ownership in a company.**

As regards the process of setting up commercial companies, it should be noted that it is likely to be fully digital soon in individual Member States. By 1 August 2021 at the latest, Member States are required to implement Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law. The Directive requires, among other things, that Member States ensure that the online formation of companies may be carried out fully online without the necessity for the applicants to appear in person.

In this context, it is to be expected that at least some of the national legislatures will have to introduce some type of remote notarization.

In Poland, work is already underway to draft regulations enabling online formation of a limited liability company, using a template prepared by a notary public but without physical presence at a notary's office.
https://www.gov.pl/web/aktywa-panstwowe/nowe-technologie-w-funkcjonowaniu-prawa-handlowego

PRZYKŁAD RYNKOWY

Germany:
Similar work has also been undertaken in Germany, where notaries can already officially certify certain documents and issue simple certificates in an electronic form.

Czech Republic:
The Czech Republic is also considering introducing changes that will allow companies to be formed entirely online using remote communication with a notary public.

There are also countries which, faced with the pandemic, immediately took further steps towards full digitization of notarial activities.

Belgium:
In Belgium, it has been possible for several months to sign notarial deeds using an electronic power of attorney.

Austria:
If a legal transaction, declaration or a legally significant factual circumstance requires the form of a notarial deed or other public or publicly certified deed to be effective, then, in order to prevent the spread of COVID-19, the notarial transactions required to prepare the deed may also be performed by means of electronic communication.

legalization of foreign documents

When using foreign documents in another country, in order to prove that they come from official state bodies, they often need to be legalized. In the countries which have ratified the 1961 Hague Convention, this means attaching an official apostille to the document. Currently, it is not possible to obtain an electronic apostille on an electronic document. As a result, documents that could potentially require legalization should be prepared as a precautionary measure in a traditional paper form.

2.5 Development of trust services in Europe

The European market has grown significantly in recent months in the context of emergence of new qualified trust service providers. Compared to 2019 (detailed analysis May 2019-June 2020), 58 new suppliers have appeared on the market. The market expansion results mainly from the availability and strengthening of electronic identification tools (e.g. video identification) that support registration and identification processes of entities for new trust services on an international scale

Number of trust service providers in Europe and selected national markets

Qualified trust service	Europe	Poland	Germany	Italy	Spain	France
Total service providers	249[1]	6	12	39	33	22
Issue of certificates	208	6	10	40	26	13
Time stamp	110	5	5	18	21	10
Preservation	12	1 (underway)			2	1
Registered electronic delivery	18		2		5	7
Validation of signatures and seals	15	1			2	1

List of qualified trust services - as of September 2020.

During the analyzed period, a growth of certificates issue (+48), time stamping (+18), signature and seal preservation (+11) and registered electronic delivery (+7) services has been particularly noticeable. In terms of signature and seal validation services, the market has expanded to include two new suppliers. Particularly positive was the development of registered electronic delivery services (France +3, Spain +2), which offer a great potential for the digitization of processes at the customer-public administration interface. As for the Polish market, no new qualified suppliers have appeared. In the previous report, "Paperless Business", we pointed to the potential of one-time certificates.

Currently, on the Polish market, one of the providers (KIR) offers the service for a one-time qualified signature certificate, and another provider, Asseco Data System, has implemented a one-time advanced signature in Santander Consumer Bank

2.6 Development of notified identification schemes in Europe

In the previous 2019 report, as Obserwatorium.biz, we emphasized the importance of internationalization of trust services through the use of electronic identification means between European Union countries. Under eIDAS, Member States are required to recognize notified electronic identification means in online services as long as they meet a certain level of reliability (security). Notification means designation of a national identification means as being available across the EU.

As of 14 September, 2020, 20 notified and pre-notified electronic identification schemes were published (+3 compared to 2019), encompassing various means of identification. The new electronic identification schemes include the schemes from the Netherlands, Lithuania and Denmark.

In the previous report, 9 out of 17 schemes were undergoing the notification procedure. Currently, 19 schemes have been notified and only one (the Portuguese professional scheme) remains in the pre-notification phase.

The most frequently notified means is an identification card (ID card) and the development of mobile services (mobile applications) is being observed.

Chapter 3
COMMERCIALIZATION
– PERSPECTIVE OF SERVICE RECIPIENTS

3.1 Application of trust services and eID in market practice

As part of the surveys carried out for this report with business representatives, only 3 (7%) out of a group of 41 indicated that in the last 6 months of the COVID-19 pandemic, their company did not implemented any project to move important business areas to digital channels.

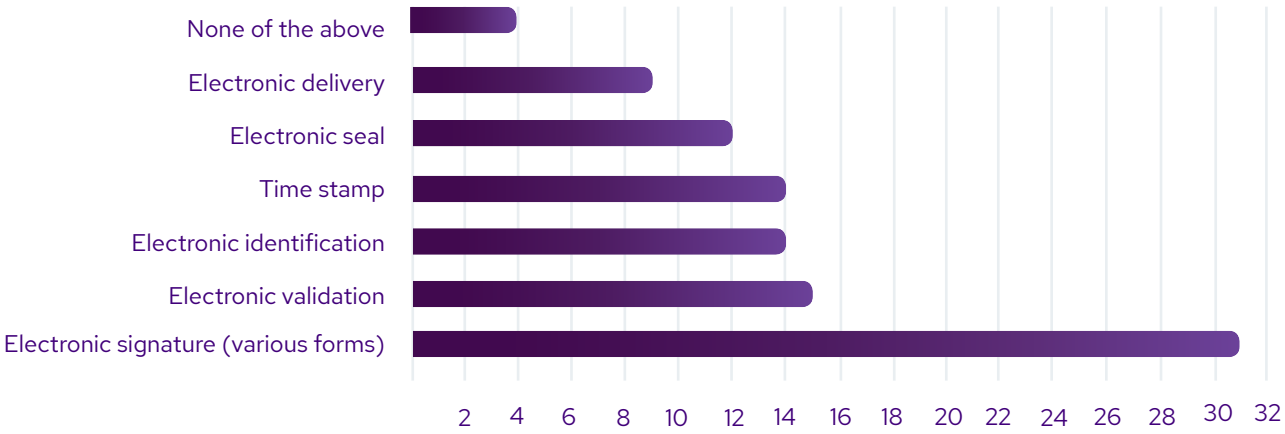
"During the pandemic, the vast majority of companies implemented solutions moving selected areas of their activities to the digital sphere".

After excluding the 3 respondents who have not implemented a solution digitizing their activities, 35 (85% of the entire group of respondents) out of the remaining 38 respondents who made such implementations also answered „yes" to the following question: „Has the coronavirus pandemic and the related situation accelerated implementation of those projects?" Three respondents answered „no". Therefore, those results could be interpreted that the pandemic and the resulting limitations definitely contributed to the launch or acceleration of projects of that type.

Earlier we indicated that teleworking (23 respondents) and internal processes (21), as well as HR (18) were the most frequently named areas of change. Less frequently, projects digitizing business processes were carried out in the areas of customer service (13) and sales (12), which shows the still existing potential there, given the continuing situation of recommended social distancing and changing social preferences.

Another question asked to identify specific organizational and technical solutions from among electronic identification (eID) and individual trust services, that were utilized in the implemented digitization processes. The most popular was the electronic signature - 31 responses (76%), followed by electronic validation: 15 responses (37%). Electronic identification, time stamp, electronic seal and electronic delivery were named less frequently.

Popularity of the usage of eID tools and trust services in digitalization process



Then, we wished to verify the importance of individual aspects of carrying out digitization initiatives and projects in the context of companies' plans for the next 6 months. The awareness of eID tools and trust services proved so high that 17, i.e. 41% of the respondents, plan to include them. Very important proved to be the possibility of easy integration with existing processes and IT systems at companies: 16 (39%), as well as ergonomics and user experience (UX): 12 (29%), operational risk management and cybersecurity: 10 (24%).

"Companies are aware of trust services, but still less than half take them into account when planning projects and initiatives aimed to digitize business processes".

" The TOP 3 topics important for managers, in addition to the possible use of eID tools and trust services, are:

- **- solutions integration with existing IT systems;**
- **- ergonomics and user experience;**
- **- Operational risk management and cybersecurity".**

What is your biggest concern in the digital transformation process?

To the question: "What is your biggest concern in the digital transformation process?" respondents could point to a maximum of two responses. The biggest concern turns out to be the lack of know-how within the organization: 18 responses (by 44% of respondents), followed by high costs without a guarantee of success: 14 responses (34% of respondents) and the need to manage change (i.e. improve personnel qualifications, processes, structure, etc.): 13 responses (31%) as well as non-compliance with the law: 12 responses (29%).

3.2 Market development scenarios

Above, we have made an attempt to describe the current situation on the market of trust services and electronic identification in the context of the business situation where entrepreneurs and key management are seeking, often quite urgently, to find solutions for transformation to the digital environment. This is what is expected of them from customers given the changing preferences for behavior, shareholders due to the greater business efficiency of remote processes, colleagues and employees because they successfully pursue other life activities in the digital world. The pandemic only deepened and accelerated these developments. Let us now look at the market development scenarios for the services which, by definition, were to become a tool for safe implementation of that transformation, adding a trusted third party as a natural arbiter in an electronic contact between two entities, although, for ergonomic reasons, often remaining „in the shadow" of the entire transaction. What must happen on the market for trust services and eID to become a real guarantor of security of the ongoing changes in the economic life of Poland and Europe in terms of „paperless" processes?

Using the potential of e-seals

A qualified electronic seal is intended to allow legal entities (hence, in particular, companies) to authorize and secure documents electronically. As the name implies, it is supposed to be equivalent to a traditional company stamp, but for electronic data.

A qualified electronic seal on the basis of eIDAS does not replace a signature placed in accordance with legal entity's representation, but there are a number of options to secure the obligations of legal entities, such as certificates, purchase orders or documents created on the basis of previously signed contracts.

The future of e-seals is widely discussed both among lawyers and at the level of technologies. However, as to the potential use of e-seals in making declarations of will by legal entities, there seems to be no simple legislative solutions.

The e-seal, on the other hand, is a great tool when considering its use in the context of evidence. A qualified e-seal on a given electronic document guarantees the integrity and authenticity of that document. If the e-document is revised after an e-seal has been affixed, then at the verification stage we will receive a message that the e-seal is defective.

A similar effect can of course be obtained using other technological solutions. Nevertheless, the advantage of a qualified e-seal (certified in accordance with eIDAS) is that, as with a qualified electronic signature, the validity of a qualified e-seal is implied and, once issued in one Member State, it cannot be rejected in another Member State.

An interesting example of how this characteristic of an e-seal is utilized is where documents signed with an ordinary electronic signature are secured with an e-seal based on a qualified certificate (where a QUALIFIED ELECTRONIC SIGNATURE is not required for the transaction to be valid). For example, the Autenti platform is based on that principle. The authenticity and integrity of the content signed on a document platform is secured with Autenti e-seals.

It is difficult to predict the future of e-seal. It is still a tool with a great potential when its specific features are taken into account. In particular, it can work in areas that:

- Require ensuring a high level integrity and authenticity of documents;
- Automated issue of documents, avoiding the human factor;
- Transfer the responsibility for the issued document to the organization, the company affixing the e-seal (there is no need to look for a person individually responsible for the issued e-document).

Perhaps the e-seal will find an even wider application once AI or IoT are utilized to a greater extent in the processes of documenting specific transactions or events.

This is the time for e-identity, or eID

The pandemic has highlighted how important the aspect of parties identification is for comprehensive digitization. It took this incentive to start looking for other, remote identification solutions going beyond the comfortable mechanism of comparing a physically present human against his/her traditional ID card.

Remote on-boarding is only the first step toward e-identity. The key in fact is to make electronic identification and authentication means popular enough to be used daily in digital, including cross-border, commerce. At present, the scope of eID use is still unsatisfactory.

So what is the future of eID in Poland and throughout the European Union?

Public consultations on the planned revision of eIDAS began in summer. Undoubtedly, one of the drivers for such efforts is the COVID-19 crisis. The axis of the discussion on the necessary changes is, in particular, the desire to provide all European citizens and entrepreneurs with a commonly accepted and trusted digital identity.

Therefore, in the future, we may perhaps expect more intensive efforts to unify digital identity solutions meant to ensure broad access to key and sensitive public services throughout the European Union.

Cybersecurity - fewer gaps and risks

An inherent part of planning digital transformation is the need to ensure security of new solutions. Poorly designed digital processes are extremely susceptible to threats from the Internet, which is often a barrier to their implementation.

Trust services play a vital role in ensuring security of digital commerce. Similarly, the introduction of commonly recognizable electronic identification mechanisms (eID), enabling unambiguous verification of the identity of e-service users, is of great importance for the security of digital processes.

MARKET EKSPERT

Marcin Szulga,
Asseco Data Systems Polska

MAJOR TRENDS IN TRUST SERVICES:

The dynamic development of trust services has been taking place since the entry into force of the eIDAS Regulation, i.e. since 2016.In the last year, active growth is intensified by four trends affecting the market, which will undoubtedly continue in the coming years:

The COVID19 pandemic accelerated the digitization of classic processes: there is an increasing number of digital transactions that require the implementation of security features using trust services. There is a strong trend to move away from the popular subscription model towards a transactional model that ties together the fees for individual operations, such as on-the-fly signatures. Social isolation forces trust service providers to create new identification methods - the popularity of video identification is growing. It is complemented by electronic (eID) and hybrid identification methods.

New business processes – industry 4.0: the development of trust services will support key large scale processes such as scalability, high availability, efficiency, accountability, or anonymity. New applications for trust services and synergies with technologies supporting industrial processes such as IoT, 5G, Blockchain will emerge here. The disruption of global supply chains will require validation of transactions between individual economic ecosystems.

Standardization and legal changes: there is a strong trend towards reinforcing the cybersec layer, as evidenced by the implementation of the requirements for Remote Qualified Signature Creation Devices (Remote QSCDs) as an appendix to the EC 650/2016 Implementation Decision, in accordance with EN 419 241-2 and EN 419 221-5.Standardization is also progressing in the area of API for remote signature creation (ETSI TS 119 432, Cloud Signature) and in the area of signature formats.

Cybersec risks: the profitability of attacks on technologies used in trust services increases, most often targeting elements not protected by cryptography, in particular the process of identification of individuals.Here, artificial intelligence comes in handy to support algorithms that detect e.g. attacks related to real-time generation of 2D/3D masks. In the area of cryptography, we can also see movement (e.g. attacks on shortcut functions, development of quantum computers), which determines how to build trust services in the direction ensuring the so-called cryptographic agility (possibility of quick exchange of cryptographic algorithms).

asseco
DATA SYSTEMS

In order to ensure an adequate level of security of electronic identification mechanisms, all eID providers should be subject to similar requirements, in particular as regards the level of security they guarantee and the scope of their responsibility. Standardization of the requirements for hardware or software suppliers takes place at the EU and national level.

Recently, there have been efforts to accelerate larger scale adoption of cybersecurity regulations. In line with that trend, an amendment to the act on the national cybersecurity system in Poland has recently been announced. The planned changes are aimed, in particular, to introduce the ability to assess the cybersecurity risk of hardware or software suppliers. The amendment also provides for the establishment of centers for the exchange of information between entities of the national cybersecurity system (ISAC, i.e. Information Sharing and Analysis Center).

MARKET EXAMPLE

In our company we have implemented qualified electronic signatures on a large scale already before the pandemic. This is connected with tax obligations, but also results from other registration obligations which currently can be fulfilled electronically only. Nevertheless, last months showed us different application areas of electronic signatures we had never considered before.

It appears that the use of qualified electronic signatures offers many more advantages. One of them is unequivocal and safe identification during various types of processes. Regardless of the pandemic, it seems that recently people tend to be more relaxed and carefree when providing their personal data in different type of situations. Meanwhile, today one has to be even more careful what kind of information is widely available as certain combinations allow to obtain authorization, which is a gateway to many potential frauds, including those which can also endanger the company's operations.

Tomasz Budny, CFO of an agrochemical company

Validation of electronic signatures

The growing popularity of electronic signatures also entails consequences in the need to properly recognize them, often among people or business entities that are not specialized in that regard. This, in turn, creates the requirement to acquire at least basic competences in this area among a very wide group of recipients. The qualified validation service comes to the rescue here, ensuring verification of qualified signatures regardless of the solution provider, but it is also still not very popular and we see a great potential for its development.

Electronic delivery

The above example from Italy, where electronic delivery has proven successful as a tool facilitating remote communication and handling of business and administrative matters in the most difficult periods of the pandemic, points to its so far underestimated potential. Currently, in the European Union, qualified e-delivery has been implemented in only five countries, while its capabilities as a tool, both as an alternative to registered paper deliveries and for securing business communication, are hard to overestimate, and with a positive approach of the regulator on a given market, electronic delivery could contribute significantly to the effective digitization of many business and administration areas in individual markets.

REPORT EXPERT

Marta Gocał
Deloitte Legal

One of the aspects of digital security is the concern about the ability to effectively prevent disclosure of sensitive data to unauthorized persons. Perhaps the most vivid breaches of that security are e-identity thefts.

Meanwhile, as a recent Deloitte study shows, consumers share a lot of their data, sometimes without knowing the terms on which they are shared. The number and severity of data privacy breaches have increased over the past year.

One may also say that European countries are past the stage of infancy as regards the General Data Protection Regulation (GDPR). One of the main goals of the GDPR is to make it easier for European citizens to understand how their data are used.

However, consumer awareness of the content of the general terms of use of applications or electronic devices is still low: About 80% of adults rarely, if ever, read them.

Deloitte's 2019 global mobile consumer survey is the world's largest multicountry survey of digital behavior trends

https://www2.deloitte.com/us/en/insights/industry/telecommunications/global-mobile-consumer-survey.html

Deloitte. Legal

3.3 How to successfully carry out digitization

1. Know your data and processes - create a map of documents and transactions involved in your business. Identify how they relate to each other.

2. Assess sensitivity of identified data - electronic processes give some freedom in managing business and legal risks. In order to apply only the necessary measures, it is necessary to know what potential risks are involved in a given case and against which we wish to (need to) protect ourselves to the highest possible extent, and which we are possibly ready to accept.

3. Identify legal requirements - remember that they largely depend on the country to which a given relationship will be subject (local law, but also including domain law) and on the industry in which you operate.

4. Customize your contracts - insert appropriate clauses to properly regulate the form you wish to use for a given relationship.

5. Account for the needs of your business and your counterparties - not all your employees and counterparties will necessarily be willing to change their habits, and not all will also have the appropriate technology and competences to adapt to the digital model of cooperation.

6 Prepare an internal e-signing policy – it should primarily take into account the results of a previous analysis and indicate at least:

- which documents and transactions could be executed electronically,
- what should be the electronic form (given the principle that we use the simplest possible form that guarantees a sufficient level of security and reliability),
- who should be empowered (and in what form) to perform a given type of electronic transactions.

MARKET EKSPERT

Artur Miękina,
Asseco Data Systems Polska

Digital transformation is primarily a process that should be properly planned, supervised and it should have a competent leader. A holistic approach to its implementation is a major challenge due to changes in different areas of the organization, so management level support is essential for the success of the transformation.

Trust services are very helpful as long as we treat them as part of a larger whole – they are supposed to support the creation of rather than create the processes themselves. Therefore, it is extremely important to look at the transformation through the appropriate lens of benefits behind it. With this perception and approach, the security elements overlap – the puzzle has to fall into place.

www.obserwatorium.biz

CONSULTANCY TRAINING ANALYTICS

#electronic signature
#trusted services
#electronic identification
#digital transformation
#digital services

OBSERWATORIUM . BIZ

Information about previous reports on eID and trust services

1.Report
Paperless Business - Commercialization of eID and trust services in Poland and Europe

The report presents a map of Polish providers of electronic identification services and trust services, a European perspective - how this market is growing abroad and what impact it will have on Poland and indicates the potential of commercialization of eID and trust services for individual market sectors - financial, telecommunications, postal and others. It also presents the necessary directions for the development of tools such as video verification, the use of identification from identity providers, on the fly electronic signature, signing platforms, signature validation, electronic delivery, to make them tools commonly used by consumers and enterprises.

Link to download the report: https://obserwatorium.biz/wp-content/uploads/2019/05/RAPORT.-Biznes-bez-papieru.-eID-i-us%C5%82ugi-zaufania-w-Polsce-i-Europie.pdf

2.Report
2017 eID Report - Electronic identification in Poland

The studies carried out for purposes of the report proved how important it is in the eyes of experts and individual market participants to ensure a systemic approach to the eID market. Aspects such as regulation, safety, business model, user awareness must be properly identified and addressed by the market and the regulator, because they may well become catalysts or barriers to the development of electronic identification in Poland

Link to download the report:
https://obserwatorium.biz/wp-content/uploads/2019/01/RAPORT_eID2017.pdf

3.Report
Breakthrough in online services. Development of trust services in Poland

The report was prepared based on analysis of the Polish and foreign markets for trust services and electronic identification, and their application in business and public administration. The digital revolution we are witnessing can enter the next stage when we, as citizens, customers and entrepreneurs, are able to conveniently and safely carry out transactions entirely in the electronic environment. The trust services referred to in the report are to be the response to the growing demand from all parties to a potential „transaction" for a coherent, predictable and universal organizational and legal framework for the provision of such services.

Link to download the report: https://obserwatorium.biz/wpcontent/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf

AUTHORS OF THE REPORT

Marta Gocał
Deloitte Legal

Simina Mut
Deloitte Legal

Aleksandra Witowska
Deloitte Legal

Mateusz Ordyk
Deloitte Legal

Michał Tabor
Obserwatorium.biz sp. z o.o.

Miłosz Brakoniecki
Obserwatorium.biz sp. z o.o.

Marcin Wolski
Obserwatorium.biz sp. z o.o.

Dominika Rzęsa
Obserwatorium.biz sp. z o.o.

Marcin Żywicki
Obserwatorium.biz sp. z o.o.

REPORT PARTNERS

MAIN PARTNER

PARTNERS:

Deloitte. Legal

asseco DATA SYSTEMS

POLSKA 5.0

PUBLISHER OF THE REPORT

OBSERWATORIUM.BIZ

Report preparation methodology

The report was prepared based on the knowledge of partners and experts in the field of digital transformation. Additionally, questionnaire surveys were carried out via an electronic channeland face-to-face interviews. All tests using the listed research tools were carried out in the period August-September 2020.As part of the preparation of the report, the following were carried out:

1. Analysis of the legal environment / Legal analysis - based on the available legal acts the pace of changes in the law caused by the pandemic has been verified, whether such changes occurred and whether existing law was prepared for such circumstances.
2. Electronic surveys (CAWI) - a survey conducted among entrepreneurs and companies declaring the implementation of digital transformation projects; the sample covered 41 respondents.
3. Face-to-face interviews with law firms of European countries; the attempt was 35 respondents.
4. Desk research method - a method in which product changes were cataloged B2C and B2B service providers in the development of electronic contact channels and checkout with the customer.
5. Market analysis - analysis of the area of development of electronic identification services and trust services. The analysis focused on verifying the progressive changes in the context of increasing the availability of these services to a wide range of consumers and businesses.

Sources

1. Digital Directive - Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law.
2. eIDAS - 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.
3. Civil Code Act of 23 April 1964 (consolidated text: Journal of Laws 2019, item 1145, as amended).
4. Code of Civil Procedure Act of 17 November 1964 (consolidated text: Journal of Laws

2019, item 1460, as amended).
5. Labor Code Act of 26 June 1974 (consolidated text: Journal of Laws 2020, item 1320).
6. Commercial Companies Code Act of 15 September 2000 (consolidated text: Journal of Laws 2020, item 1526).
7. Hague Convention - Convention Abolishing the Requirement of Legalization for Foreign Public Documents, signed at The Hague on 5 October 1961 (Journal of Laws 2005, No. 112, item 938).
8. The Anti-Crisis Shield - the Act amending the Act on special measures to prevent, counteract and control COVID-19, other infectious diseases and resulting crisis situations, and certain other acts, of 31 March 2020 (Journal of Laws, item 568, as amended).
9. Federal Law on Personal Data of 27 July 2006 No. 152-FZ (Russia).
10. Interpretation Act of 20 July 1978 (UK)
11. Executive Committee Act 172/1/29.05.2020 (Greece).
12. Act on the National Cybersecurity System of 5 July 2018 (consolidated text: Journal of Laws 2020, item 1369).
13. Act on Tax on Goods and Services of 11 March 2004 (consolidated text: Journal of Laws 2020, item 106, as amended).
14. Anti-Money Laundering Act (Geldwäschegesetz, GwG) of 25.10.1993 - (German: Gesetz über Aufspüren von Gewinnen aus schweren Straftaten, BGB 1., part I, p. 1770.) (Germany).

Legal disclaimer

Opinions found in this report have been expressed based on the knowledge gained from market research and the authors' experience. The authors do not take responsibility for decisions based on opinions expressed in the "TRUSTED ECONOMY in the new reality. Mitigation of the risks associated with rapid digitization" report. References to providers of electronic solutions are examples only and are not a recommendation.