OBSERWATORIUM . BIZ

ISBN 978-83-954468-1-8

Raport specjalny 2020

TRUSTED ECONOMY
w nowej rzeczywistości.
Ograniczanie ryzyka związanego z szybką cyfryzacją

PARTNER GŁÓWNY:

EFPE ON-LINE

PARTNERZY:

Deloitte. Legal

asseco DATA SYSTEMS

POLSKA 5.0

GŁÓWNE WNIOSKI RAPORTU

Pandemia COVID-19 przyspieszyła procesy cyfryzacji; większość przedsiębiorstw podjęło intensywne działania w tym zakresie przez ostatnie sześć miesięcy. Firmy skupiały się na umożliwieniu telepracy i przeniesieniu procesów wewnętrznych do świata on-line, rzadziej realizowały projekty związane z digitalizacją obsługi i sprzedaży.

Europa potrzebuje interoperacyjnych rozwiązań w zakresie obiegu elektronicznych dokumentów – rozwiązaniem może tu być eDelivery, które sprawdziło się już na niektórych rynkach, a na innych jest planowane lub już wdrażane. Ale aby je właściwie wdrożyć, niezbędna jest komunikacja i partnerska współpraca sektora komercyjnego i regulatorów na poziomie europejskim i krajowym.

Przedsiębiorstwa wiedzą o podpisie elektronicznym i korzystają z niego głównie do czynności administracyjnych, ale mniej niż połowa z nich zamierza go wykorzystać do planowanych projektów cyfrowej transformacji. Usługi zaufania, aby stać się bardziej powszechnymi, muszą być łatwiej integrowane z dotychczasowymi rozwiązaniami IT firm, uwzględniać ergonomię użytkownika oraz być na tyle tanie, aby skokowo zwiększyła się dostępność ich zastosowań.

Wzrost popularności wideoweryfikacji w sektorze komercyjnym oraz profilu zaufanego w administracji publicznej w Polsce wskazuje na ogromny popyt na usługi elektronicznej identyfikacji, którego zaspokojenie może być uzupełnione rozwiązaniami komercyjnymi.

Sama elektroniczna identyfikacja staje się kluczową usługą, która powinna mieć przejrzyste ramy funkcjonowania prawnego w administracji publicznej i świecie komercyjnym i być wdrożona w sposób wygodny oraz bezpieczny dla klientów końcowych w możliwie największej liczbie procesów on-line.

Pieczęci elektroniczne mają niewykorzystany i niedoceniony potencjał jako narzędzia, które są w stanie bardzo szybko sprawnie zaadresować potrzeby firm i konsumentów w zakresie bezpiecznej i potwierdzonej komunikacji elektronicznej między poszczególnymi aktorami życia gospodarczego i administracyjnego.

Usługi zaufania mają również potencjał wykorzystania w zupełnie nowych, rodzących się dopiero na naszych oczach procesach biznesowych, związanych z rozwojem tzw. przemysłu 4.0. W tym przypadku rozwój usług zaufania wspierać będzie kluczowe procesy wielkiej skali np. poprzez zwiększenie ich skalowalności, dostępności, wydajności, rozliczalności lub anonimowości. Tu pojawią się nowe zastosowania usług zaufania i synergie z technologiami wspierającymi procesy przemysłowe, tj. IoT, 5G, Blockchain. Rozerwanie światowych łańcuchów dostaw spowoduje konieczność walidacji transakcji pomiędzy poszczególnymi ekosystemami gospodarczymi.

Spis treści

#biznesbezpapieru #paperless

Rozwijaj swój biznes z usługami zaufania Certum

SimplySign by asseco

Mobilny kwalifikowany podpis elektroniczny

- Ma taką samą moc prawną jak podpis własnoręczny
- Działa na smartfonach, tabletach i komputerach
- Umożliwia zintegrowanie z usługą poprzez API
- Zapewnia dodatkowe bezpieczeństwo poprzez dwuetapowe uwierzytelnienie

Pieczęć elektroniczna by asseco

Kwalifikowana pieczęć elektroniczna

- Zapewnia integralność dokumentów elektronicznych
- Identyfikuje podmiot, który jest autorem dokumentu
- Zmniejsza wydatki związane z przetwarzaniem dokumentów

WebNotarius by asseco

Kwalifikowana usługa walidacji

- Sprawdza autentyczność podpisów elektronicznych z całej UE
- Generuje dowody walidacji uznawane w postępowaniu sądowym
- Weryfikuje czy podpisany dokument elektroniczny nie został zmieniony w sposób nieautoryzowany

Znacznik Czasu by asseco

Kwalifikowany znacznik czasu

- Chroni dokumenty elektroniczne przed sfałszowaniem i antydatowaniem
- Potwierdza istnienie dokumentu w danym czasie
- Wywołuje skutki prawne daty pewnej w rozumieniu przepisów KC

Infolinia 801 540 340
www.certum.pl

Certum by asseco

Wstęp

Głównym celem niniejszego Raportu jest odpowiedź na pytanie, w jakich obszarach oraz w jaki sposób odbyła się przyspieszona cyfryzacja przedsiębiorstw oraz administracji publicznej w okresie pandemii COVID-19 od marca do września 2020 roku. Koncentrując się na doświadczeniach polskich, chcieliśmy rozszerzyć to spojrzenie na inne kraje europejskie, dla których doświadczenie pierwszych miesięcy pandemii i jej konsekwencji było tak samo lub nawet jeszcze bardziej intensywne i trudne. Drugim ważnym celem Raportu jest zastanowienie się, na ile usługi zaufania oraz elektroniczna identyfikacja (eID) - rozwiązania, które powstały i rozwijały się specjalnie po to, aby stać się podstawowymi narzędziami cyfryzacji, sprawdziły się w tej sytuacji swoistej „próby". Zamierzaliśmy zwrócić szczególną uwagę na aspekty prawne – aby móc zweryfikować, w jaki sposób legislacja była w stanie nadążyć za zmianami, które działy się w tempie do tej pory niespotykanym.

Zaistniała sytuacja nie tylko wzmogła funkcjonujące już wcześniej procesy przenoszenia komunikacji czy pracy do formuły zdalnej, ale także wymusiła digitalizację w obszarze transakcji – oświadczeń woli, identyfikacji, podpisywania umów. W tych obszarach już od pewnego czasu mieliśmy do dyspozycji ramy prawne w postaci eIDAS, czyli uregulowania europejskie oraz ramy narzędziowe w postaci usług zaufania i elektronicznej identyfikacji. Staraliśmy się zweryfikować, na ile te usługi spełniły swoją funkcję i były rzeczywiście wykorzystywane, a na ile firmy czy administracja publiczna musiały stosować rozwiązania inne czy zastępcze. Warunkuje to odpowiedź na kolejne pytanie – w jakiej mierze wypracowane narzędzia techniczne i prawne zostaną z nami na dłużej i jakie zmiany muszą nastąpić w sferze usług zaufania i eID, aby stały się powszechne i użyteczne, a jednocześnie niosły ze sobą wciąż swoją największą wartość w postaci zapewnienia bezpieczeństwa transakcji w sytuacji nowej pocovidowej normalności.

Na potrzeby raportu przeprowadzono elektroniczne badania ankietowe wśród przedsiębiorców i firm deklarujących realizację projektów transformacji cyfrowej (N=41) oraz badania ankietowe i wywiady bezpośrednie z kancelariami prawnymi państw europejskich. Dodatkowo przeprowadzono badania desk research, w ramach których katalogowano zmiany produktowe dostawców usług B2C i B2B w zakresie rozwoju elektronicznych kanałów kontaktów i realizacji transakcji z klientem. Przyjrzano się również stanowi rozwoju usług elektronicznej identyfikacji i zaufania, aby zweryfikować postępujące zmiany w kontekście zwiększania dostępności tych usług dla szerokiego grona konsumentów i firm chcących sprostać wyzwaniom związanym z sytuacją pandemiczną i wymogom społecznego dystansu.

Rozdział 1
COVID – przyspieszona transformacja cyfrowa

1.1 Wprowadzenie

Czas pandemii COVID-19 drastycznie zmienił życie wielu ludzi, instytucji, a także całych państw i gospodarek. Ta trudna sytuacja nauczyła nas – i nadal uczy – w szczególności szacunku do jednej z podstawowych potrzeb każdego człowieka – potrzeby bezpieczeństwa. Nie można prowadzić biznesu w poczuciu zagrożenia życia i zdrowia, ale nie możemy też nie prowadzić biznesu, jeśli chcemy przetrwać gospodarczo.

Odpowiedzią na tę sytuację stała się cyfryzacja naszego codziennego funkcjonowania – realizacji podstawowych potrzeb życiowych, pracy, ale i załatwiania spaw konsumenckich czy obywatelskich.

Rewolucja cyfrowa w poszczególnych obszarach życia była mocno zaawansowana już przed wybuchem pandemii. W Polsce na szczególnie zaawansowanym poziomie w zakresie digitalizacji był rynek finansowy. Podjęte w ostatnich latach działania pozwoliły zwiększyć liczbę obywateli korzystających z profilu zaufanego – narzędzia e-identyfikacji w kontaktach z polską administracją publiczną oraz liczbę dostępnych e-usług. W całej Europie zwiększała się systematycznie liczba dostawców usług zaufania, funkcjonujących w jednoznacznie zdefiniowanych przez rozporządzenie eIDAS ramach prawnych. Z drugiej strony wiele sfer życia publicznego i komercyjnego pozostało poza głównym nurtem rozwoju usług elektronicznych i zdalnej komunikacji. Często elektroniczny obieg dokumentów odwzorowywał wewnętrzną organizację przedsiębiorstw i nie pozwalał na bezpieczną i wiarygodną wymianę informacji oraz dokumentów elektronicznych miedzy poszczególnymi podmiotami gospodarczymi nie tylko na poziomie transgranicznym, ale nawet lokalnym.

1.2 Szybka cyfryzacja „pocovidowa” – zmiany biznesowe i prawne

Początek pandemii oznaczał dla wielu podmiotów początek szybkich zmian związanych z koniecznością przeniesienia jak największej liczby procesów do kanałów elektronicznych. Można przypuszczać, że część tych zmian była planowana już wcześniej, jednak wystąpienie nadzwyczajnych okoliczności wymusiło zrealizowanie wielu wdrożeń w trybie zdecydowanie przyspieszonym.

1.2.1 Praca zdalna

Lockdown spowodował konieczność pracy z domu dla milionów Europejczyków, praktycznie z dnia na dzień. Polski ustawodawca zauważył potrzebę uregulowania tej sfery życia, która nagle musiała ulec radykalnej zmianie. Określenie prawne miejsca wykonywania pracy poza jej stałym miejscem otwiera cały szereg kolejnych zagadnień, które muszą rozwiązać przedsiębiorcy. Chodzi tu o komunikację wewnątrz firmy oraz z kontrahentami, sporządzanie bieżącej dokumentacji korporacyjnej, uzyskiwanie zgód wewnętrznych, kontraktowanie, dopełnianie obowiązków publicznoprawnych. Wszystkie te czynności opierają się na działaniach pracowników poszczególnych firm lub organów, którzy w dobie społecznego dystansowania powinni móc je wykonywać zdalnie w kanałach cyfrowych.

Wydaje się, że przynajmniej wśród polskich przedsiębiorców najwięcej zmian dokonano w celu umożliwienia pracy zdalnej. W przeprowadzonych na potrzeby tego Raportu badaniach internetowych 23 (56%) z 41 udzielających odpowiedzi przedsiębiorców wskazało, że zrealizowano w ich przedsiębiorstwach w okresie pandemii projekty związane z przygotowaniem i wdrożeniem do pracy zdalnej, a 18 (44%) wskazało, że realizowane były projekty związane z cyfryzacją szeroko rozumianego obszaru zarządzania kadrami (HR). Jednocześnie, mimo że prawo w dużej mierze daje możliwości wdrożenia właśnie takiej cyfrowej działalności, wciąż jeszcze nie wszystkie firmy skorzystały z tych narzędzi.

NOWE ROZWIĄZANIE PRAWNE

W tzw. tarczy antykryzysowej znalazły się tymczasowe przepisy mówiące o możliwości polecenia pracownikowi przez pracodawcę wykonywania pracy określonej w umowie o pracę poza miejscem jej stałego wykonywania. W najbliższym czasie – zgodnie z zapowiedziami resortu pracy – można przewidywać wprowadzenie analogicznych regulacji do Kodeksu Pracy na stałe.

1.2.2 Zdalny obieg dokumentów i podpisywanie umów on-line

Drugim obszarem, w ramach którego najczęściej realizowano projekty cyfryzacyjne w pierwszych sześciu miesiącach pandemii, były procesy wewnętrzne w firmie – wskazało tak 21 (51%) z 41 respondentów. COVID-19 przyczynił się do przyspieszenia już realizowanych działań mających na celu digitalizację procesów w organizacji oraz do natychmiastowego uruchomienia nowych inicjatyw, kluczowych dla bieżącego funkcjonowania przedsiębiorstw.

W szczególności warto zwrócić uwagę na doświadczenia europejskich państw najbardziej dotkniętych pandemią w jej pierwszych miesiącach. Włochy, posiadające najbardziej zaawansowany i najbardziej dojrzały system elektronicznych doręczeń (e-delivery) w Europie, były w stanie wykorzystać go do szybkiej migracji procesów biznesowych i administracyjnych do świata on-line. Specyfika tego systemu, polegająca na poświadczonej elektronicznie wymianie dokumentów między osobami fizycznymi, przedsiębiorstwami i administracją, zapewniła możliwość skutecznej realizacji transakcji, oświadczeń woli, podpisywania umów bez konieczności budowania dedykowanych systemów pod każdy proces i jego warianty. **Brak pełnej faktycznej interoperacyjności na poziomie wszystkich państw Unii Europejskiej w zakresie e-delivery spowodował, że wiele łańcuchów obiegu dokumentów na poziomie wspólnego rynku, które do tej pory były papierowe lub uzależnione od fizycznego kontaktu stron, uległo przerwaniu, albo obieg dokumentów w ich ramach uległ znacznemu spowolnieniu.**

PRZYKŁAD RYNKOWY
Węgry:

Popularna na Węgrzech internetowa platforma do kontraktowania przy użyciu w szczególności kwalifikowanego podpisu elektronicznego – Trust Chain, tylko w okresie kilku pierwszych miesięcy 2020 roku odnotowała wzrost liczby użytkowników ze 100 do 1500.

Jednocześnie wnioski z badań europejskich kancelarii prawnych są takie, że praktycznie wszystkie państwa uczestniczące w naszym badaniu dostrzegły znaczny wzrost wykorzystania kanałów cyfrowych w realizacji codziennych czynności (zarówno faktycznych, jak i prawnych).

Aktualnie podstawowym narzędziem ułatwiającym zdalne prowadzenie biznesu jest podpis elektroniczny. W Polsce wydano ponad 600 tys. certyfikatów kwalifikowanych, co jednak cały czas kontrastuje z liczbą wydanych kart płatniczych (43 mln sztuk, czyli zdecydowanie więcej niż jedna karta na jednego dorosłego mieszkańca kraju), które są produktami masowymi. Trzeba zjednak zaznaczyć wzrost o ok. 100 tys. certyfikatów (17% !) w skali rok do roku. Mimo to rewolucja „paperless" jest jeszcze daleko w tyle za szybko postępującą w naszym kraju rewolucją „cashless".

PRZYKŁAD RYNKOWY
Polska:

O 17% z ok. 500 tys. do ok. 600 tys. wzrosła liczba certyfikatów kwalifikowanych w Polsce w ciągu ostatnich 12 miesięcy (czerwiec 2019/czerwiec2020)

Z jednej strony przez lata narzędziem rewolucji „paperless" była systematycznie wprowadzana w Polsce obligatoryjność kwalifikowanego podpisu elektronicznego dla wybranych dokumentów. Aktualnie podpisywanymi elektronicznie dokumentami w Polsce są kolejno: roczne sprawozdania finansowe, dokumentacja pracownicza, dokumenty finansowe oraz pełnomocnictwa.

Wskazanie tych właśnie dokumentów wynika z obowiązujących obecnie regulacji prawnych, wymuszających sporządzenie większości z nich w postaci elektronicznej. Aktualnie złożenie dokumentów wyłącznie w postaci elektronicznej (czyli podpisanie ich w szczególności kwalifikowanym podpisem elektronicznym) jest konieczne m.in.w następujących przypadkach:

- **składanie sprawozdania finansowego do Krajowego Rejestru Sądowego;**
- **rejestracja beneficjenta rzeczywistego poprzez Centralny Rejestr Beneficjentów Rzeczywistych;**
- **składanie deklaracji CIT i NIP 8;**
- **składanie formularza JPK;**
- **składanie wniosków do ZUS;**
- **składanie sprawozdań o stosowanych terminach zapłaty w transakcjach handlowych** (wkrótce).

Wyniki przeprowadzonego na potrzeby raportu badania przedsiębiorstw wykazują, że większość respondentów, którzy już posiadają kwalifikowany podpis elektroniczny, używa go bardzo często, bo ponad 20 razy w miesiącu. Wydaje się zatem, że posiadacze kwalifikowanego podpisu elektronicznego wykorzystują go również do innych celów poza realizacją obowiązków publicznoprawnych, które można wypełnić wyłącznie elektronicznie. Jest to dobra wiadomość, bo świadczy o tym, że potencjał podpisów kwalifikowanych rzeczywiście został dostrzeżony przez klientów, którzy przynajmniej raz z niego skorzystali.

WZROST POPULARNOŚCI!

SimplySign – usługa kwalifikowanego podpisu elektronicznego w Polsce:

Tomasz Litarowicz
Dyrektor Pionu Usług Bezpieczeństwa i Zaufania
Asseco Data Systems

„Pandemia COVID-19 sprawiła, że we wszystkich branżach odnotowywany jest wzrost zainteresowania cyfrowymi narzędziami, które ułatwiają pracę zdalną i pozwalają zachować ciągłość biznesową bez konieczności odbywania fizycznych spotkań czy przychodzenia do biura. Za ich pomocą możemy również usprawnić obieg dokumentów. Podpisanych wydruków nie trzeba pakować w kopertę, aby tradycyjną pocztą nadać je do adresata. Plik wystarczy podpisać elektronicznie i przesłać mailowo lub przy użyciu wewnętrznego obiegu dokumentów. Dodatkowo, dzięki zastosowaniu mobilnego kwalifikowanego podpisu elektronicznego SimplySign, możemy wykonywać nasze zadania w każdym miejscu i czasie. W szczytowym momencie lockdownu zainteresowanie tym narzędziem było 600 proc. wyższe niż rok wcześniej. Fakt, że coraz bardziej przystosowujemy się do pracy na odległość, sprawia, że chętniej korzystamy z tego typu narzędzi".

asseco DATA SYSTEMS

Czas pandemii obok wykorzystania samego podpisu elektronicznego jako narzędzia, otworzył również przestrzeń dla rozwoju tzw. platform podpisowych, które umożliwiają wygodny sposób zawarcia i zabezpieczenia całego procesu utworzenia i podpisania elektronicznego dokumentu – przy użyciu podpisów elektronicznych, które mogą, ale nie muszą być kwalifikowane, a mają charakter na przykład podpisu zaawansowanego i, co jest bardzo istotne, powinny być zawsze wybierane przez klientów w oparciu o uprzednią analizę ryzyka i wymogi prawne.

WZROST POPULARNOŚCI!

Platforma Autenti:

Tomasz Plata,
Wiceprezes Zarządu
Autenti

W obecnej sytuacji zainteresowanie usługami platformy Autenti znacząco wzrosło. Tylko w marcu i kwietniu bieżącego roku odnotowaliśmy blisko czterokrotny wzrost zainteresowania w stosunku do poprzednich miesięcy. To bardzo duży skok. E-podpis stał się narzędziem niezbędnym w prowadzeniu biznesu. Ci, którzy się jeszcze wahali i nie byli przekonani do tego typu rozwiązań, musieli się szybko zaadaptować do dzisiejszej rzeczywistości. Przedsiębiorcy nie wrócą już do tradycyjnych rozwiązań w działaniu firmy i docenią e-podpis, który jest zwyczajnie bardzo prostym, efektywnym, a do tego ekologicznym narzędziem.

AUTENTI®

PRZYKŁAD RYNKOWY
BFF Banking Group

Paperless w sektorze finansowym – mini case study z wdrożenia przez Asseco Data Systems usług zaufania w BFF Banking Group w Polsce.

Celem projektu było stworzenie procesu zawierania kontraktów operacyjnych, które wyeliminowałyby manualną rejestrację i podpisywanie dokumentów przy zachowaniu zgodności z wymaganiami prawnymi oraz standardami bezpieczeństwa transakcji.

Kluczowe usługi wykorzystane w projekcie:

- Kwalifikowany podpis elektroniczny w usłudze SimplySign
- Kwalifikowana pieczęć elektroniczna
- Kwalifikowany znacznik czasu
- Kwalifikowana usługa walidacji

Rezultat wdrożenia:

- Skrócenie okresu podpisywania umów operacyjnych z 7 dni do 1 dnia
- Wygodny oraz bezpieczny proces dla członków zarządu BFF oraz pracowników, umożliwiający podpisywanie dokumentów w dowolnym miejscu i czasie
- Możliwość przeprowadzenia weryfikacji tożsamości Kontrahentów BFF przez jej pracowników w celu wydania kwalifikowanego podpisu elektronicznego

Plany rozwojowe:

- Zintegrowanie Elektronicznego Obiegu Dokumentów z kwalifikowaną usługą walidacji
- Wdrożenie procesu elektronicznych doręczeń, umożliwiającego wysyłanie dokumentów w formie elektronicznej za potwierdzeniem odbioru - realizacja planu uzależniona od wdrożenia odpowiednich regulacji prawnych
- Wdrożenie elektronicznych teczek pracowników

Wpływ COVID-19 na wdrożenie procesu:

- W marcu 2020 roku BFF przyśpieszyła zakończenie rozpoczętego już wcześniej procesu odejścia od formy papierowej na rzecz podpisywania umów operacyjnych w formie elektronicznej.
- Jedynie te dokumenty, które z różnych przyczyn nie mogą być podpisywane w formie elektronicznej nadal mogą być podpisywane w formie papierowej.
- Wymóg opatrywania dokumentów datą pewną, konieczną z punktu widzenia przepisów Ustawy Prawo Restrukturyzacyjne i Ustawy Prawo Upadłościowe spełniono dzięki zastosowaniu kwalifikowanego elektronicznego znacznika czasu.

BFF BANKING GROUP

W ramach zrealizowanego badania internetowego poprosiliśmy respondentów o wskazanie rodzaju dokumentów formalnych, do jakich użyliby podpisu elektronicznego. Najczęściej wskazywane były roczne sprawozdanie finansowe (26 odpowiedzi – 63%); umowy finansowe, a więc umowy kredytowe, umowy zabezpieczeń, umowy inwestycyjne itp. uzyskały 25 odpowiedzi (61%), natomiast dokumentacja dotycząca zatrudnienia – w tym umowa o pracę, wewnętrzne dokumenty dotyczące polityki, regulaminy, wewnętrzne wnioski/wnioski pracowników również 25 pozytywnych odpowiedzi – 61%, pełnomocnictwo (22 odpowiedzi – 54%), protokoły z posiedzenia zarządu lub pisemne uchwały (21 odpowiedzi – 51%). Poniższe zestawienie wskazuje listę wszystkich wskazanych zastosowań wraz z liczbą respondentów.

Do jakiego rodzaju dokumentów formalnych użyłbyś/użyłabyś podpisu elektronicznego

PRZYKŁAD RYNKOWY
Santander Consumer Bank

Czy długopis jest potrzebny do podpisania umowy? – mini case study z wdrożenia przez Asseco Data Systems zaawansowanego jednorazowego podpisu elektronicznego dla klientów w Santander Consumer Bank.

Celem projektu było stworzenie dla Klientów oraz pracowników Banku procesu podpisywania umowy kredytu konsumenckiego zgodnego z ideą paperless, regulacjami unijnymi eIDAS oraz najwyższymi standardami user experience.

Asseco Data Systems wraz z Bankiem Santander zbudowało rozwiązanie, w którym połączyło wszystkie aspekty związane z procesem zawarcia umowy kredytowej: kwestie prawne, techniczne i organizacyjne.

Kluczowe usługi wykorzystane w projekcie:

- Zaawansowany jednorazowy podpis elektroniczny, autoryzowany kodem SMS - składany przez Klienta Banku
- Kwalifikowana pieczęć elektroniczna w usłudze SimplySign – składana przez Doradcę w imieniu Banku
- Kwalifikowana usługa walidacji

Rezultat wdrożenia:

- Proces zawarcia umowy z Klientem skrócony o 30%
- 80% Kontrahentów Banku potwierdzających prostotę procesu
- 40% Kontrahentów Banku uważa brak papieru w procesie za jego kluczową zaletę

Plany rozwojowe:

- Podpis elektroniczny dostępny dla ponad 30 000 Kontrahentów Banku
- Podpis elektroniczny dostępny dla klientów Banku w ponad 300 oddziałach

Santander Consumer Bank

1.2.3 Faktury elektroniczne

W Polsce popularnym obszarem depapieryzacji są operacje księgowe; w szczególności chodzi o wykorzystanie **elektronicznej faktury**. Z elektronicznych faktur korzystano powszechnie jeszcze przed pandemią COVID-19. W konsekwencji w firmach w dużej mierze zdigitalizowane są zazwyczaj działy finansowe, podczas gdy działy handlowe działają według dotychczasowych przyzwyczajeń i w ramach starych, analogowych procesów.

Przepisy ustawy o podatku od towarów i usług dopuszczają posługiwanie się fakturami zarówno w formie papierowej, jak i w formie elektronicznej. Faktura elektroniczna to taka faktura, która została wystawiona i otrzymana w dowolnym formacie elektronicznym.

Warunkiem wystawiania faktur elektronicznych jest zapewnienie autentyczności pochodzenia i integralności treści faktur wystawianych w tej formie. Cechy te mogą być zagwarantowane w szczególności kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią. Jest to jednak tylko jeden ze sposobów zapewnienia tych warunków, który może być zastąpiony innego rodzaju procedurą kontroli biznesowych.

1.2.4 Zdalne posiedzenia organów spółek kapitałowych

W ramach polskiej tzw. tarczy antykryzysowej wprowadzono na stałe zmiany do Kodeksu Spółek Handlowych, dzięki którym zarówno posiedzenia rad nadzorczych, zarządów, jak i zgromadzenia właścicielskie (zgromadzenia wspólników, walne zgromadzenia) mogą odbywać się przy pomocy środków porozumiewania się na odległość.

Samo prowadzenie obrad na odległość z wykorzystaniem systemów teleinformatycznych było już wcześniej w ograniczonym stopniu dostępne dla polskich spółek. Nowością jest fakt, że uprawnienie do odbywania takich zdalnych posiedzeń będzie teraz obowiązywać także w sytuacji, gdy nie jest to wprost przewidziane w umowie lub statucie spółki. Natomiast umowa albo statut może taką możliwość wyłączyć.

Potrzeba zdalnego odbywania obrad organów korporacyjnych wydaje się bardziej uniwersalna. Oczywiście w niektórych państwach już wcześniej możliwe było elektroniczne podejmowanie decyzji korporacyjnych (np. w Serbii oraz w niektórych sytuacjach na Malcie). Natomiast spośród pozostałych badanych przez nas państw praktycznie wszystkie przynajmniej tymczasowo wprowadziły podczas pandemii taką możliwość do swoich lokalnych przepisów. Wśród nich są następujące kraje wspólnego rynku: Norwegia, Szwecja, Dania, Portugalia, Ukraina, Słowenia, Węgry, Niderlandy, Włochy, Rumunia.

1.2.5 Zdalna rejestracja i onboarding klienta

Administracja publiczna

W Polsce zasadniczym narzędziem związanym z elektroniczną identyfikacją, które powstało jako bezpośrednia odpowiedź na pandemię, jest tymczasowy profil zaufany.

Jest to niejako podtyp standardowego profilu zaufanego. Sam profil zaufany nie jest już nowym narzędziem. To bezpłatne środek identyfikacji elektronicznej, dzięki któremu można potwierdzić swoją tożsamość w systemach elektronicznej administracji. Został stworzony aby umożliwić w pełni elektroniczne kontakty z administracją publiczną (urzędami, ministerstwami).

Tymczasowy profil zaufany jest natomiast profilem zaufanym o znacznie krótszym okresie ważności, wynoszącym obecnie trzy miesiące. Natomiast zupełnie nowym aspektem wyróżniającym tymczasowy profil zaufany jest możliwość uzyskania go całkowicie zdalnie nawet w przypadku, gdy nie ma się możliwości założenia profilu zaufanego poprzez bankowość elektroniczną. Potwierdzenie tożsamości następuje w trakcie wideorozmowy przeprowadzanej on-line z urzędnikiem.

NOWE ROZWIĄZANIE PRODUKTOWE

Grecja:

W Grecji właśnie w okresie pandemii zaczął funkcjonować „Single Digital Portal" pozwalający na realizację ponad 500 różnych spraw administracyjnych przez obywateli greckich i podmioty gospodarcze.

W czasie tegorocznych wakacji profil zaufany założyło ponad 624 tys. osób – o czym poinformowało Ministerstwo Cyfryzacji, a z tej usługi korzysta już niemal 8 mln Polaków. W e-podsumowaniu tegorocznych wakacji znajdziemy informację, iż od początku lipca do końca sierpnia złożono także „grubo ponad ćwierć miliona elektronicznych pism ogólnych" i zgłoszono on-line niemal 26 tysięcy narodzin dzieci. Resort cyfryzacji podał, że w tegoroczne wakacje, czyli od początku lipca do końca sierpnia, profil zaufany założyło dokładnie 624 128 osób. To o niemal ćwierć miliona więcej niż w tym samym czasie w ubiegłym roku.

W nurcie tych przemian i budowania e-administracji mieści się m.in. wprowadzenie eSkrzynki, ale też funkcjonujący już od dawna portal gov.pl, będący niejako pośrednikiem do platformy ePUAP, dla tych wszystkich, którzy nie posiadają profilu zaufanego. Potrzeba budowania nowoczesnej e-administracji jest trendem wykraczającym poza polski rynek.

Banki

Zagadnienie wideoweryfikacji jako metody wiarygodnej identyfikacji osób bez konieczności ich osobistego stawiennictwa w punkcie obsługi klienta pojawia się już od dawna przy okazji rozmów o pełnej cyfryzacji procesów biznesowych. Oczywiste jest, że pierwszym krokiem w relacjach z kontrahentami jest potwierdzenie ich tożsamości. W przeważającej większości tych relacji nie ma prawnych przeszkód, by taką weryfikację przeprowadzić wszelkimi dostępnymi środkami, uwzględniając jedynie właściwe zabezpieczenie wartości dowodowej tego procesu.

Są jednak sektory pozbawione tej swobody doboru narzędzi i metod identyfikacji przez brak odpowiednich regulacji prawnych bądź zbyt zawężające interpretowanie istniejących przepisów.

Banki i instytucje finansowe podlegają istotnym rygorom regulacyjnym mającym na celu zabezpieczenie transakcji i zagwarantowanie przejrzystości rynku. Ramy prawne dotyczące zapobiegania i zwalczania prania pieniędzy oraz finansowania terroryzmu, jak również implementacja dyrektywy w sprawie usług płatniczych wymagają od banków w szczególności weryfikacji tożsamości ich klientów (procedura KYC, silne uwierzytelnienie), aby ocenić potencjalne ryzyko wystąpienia nielegalnych praktyk.

Na rynku europejskim najczęściej stosowane jest uwierzytelnianie dwupoziomowe (znane jako 2FA, tj. two-factor authentication). Silne uwierzytelnienie uzyskuje się dzięki równoległemu stosowaniu dwóch różnych danych identyfikujących (np. hasła i karty/tokena).

Tymczasem jeszcze w 2019 roku KNF opublikował oficjalne stanowisko dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji (stanowisko UKNF z 5 czerwca 2019 r.), w którym przede wszystkim wprost stwierdził, że „bank może posłużyć się metodą wideoweryfikacji".

PRZYKŁADY RYNKOWE - ROZWIĄZANIA PRAWNE W EUROPIE

Niemcy:

Niemiecka ustawa o przeciwdziałaniu praniu pieniędzy (Geldwäschegesetz, GwG) przewiduje, że weryfikacja tożsamości może być przeprowadzona nie tylko na podstawie konwencjonalnego dowodu tożsamości. Zgodnie z tą ustawą weryfikację można przeprowadzić między innymi również na podstawie elektronicznego dowodu tożsamości lub nawet kwalifikowanego podpisu elektronicznego.

Portugalia:

W sektorze bankowym cały proces od identyfikacji i potwierdzenia tożsamości klienta może być przeprowadzony zdalnie dzięki wykorzystaniu wideokonferencji oraz wsparcia dostawców usług zaufania.

W aplikacjach mobilnych często wykorzystywane są również mechanizmy oparte na danych biometrycznych klientów, takie jak rozpoznawanie odcisków palców i kształtu twarzy.

Grecja:

W ustawie o Komitecie Wykonawczym 172/1/29.05.2020 (Executive Committee Act) Narodowy Bank Grecji określił zasady i warunki cyfrowego onboardingu klientów banków i innych nadzorowanych podmiotów. Kluczowymi metodami w tym procesie są:

- wideokonferencja z odpowiednio przeszkolonym pracownikiem, którą uznaje się za zapewniającą najwyższy poziom bezpieczeństwa; oraz
- zautomatyzowana procedura za pomocą dynamicznego selfie, która wymaga zastosowania dodatkowych środków bezpieczeństwa.

Na wstępie zwrócono jednak uwagę, że przy zdalnej rejestracji klientów najbardziej pewne są środki identyfikacji elektronicznej, o których mowa w eIDAS, w tym przede wszystkim kwalifikowany podpis elektroniczny.

„W stanowisku UKNF z 5 czerwca 2019 r. znajduje się szereg wskazówek związanych ze stosowaniem usługi wideoweryfikacji, które powinien rozważyć bank, decydując się na tę metodę identyfikacji klientów. W pierwszej kolejności zaleca się ubranie zasad i dobrych praktyk związanych z tą usługą w ramy formalnej procedury"

KNF, formalnie otwierając bankom drogę do korzystania z wideoweryfikacji, wskazał ponadto, że przy zachowaniu zasad i dobrych praktyk opisanych w omawianym stanowisku, usługi wideoweryfikacji mogą być oferowane również przez pozostałe instytucje nadzorowane.

PRZYKŁADY RYNKOWE - POLSKA:

Alior Bank

Klient udowadnia swoją tożsamość podczas procesu zakupu kredytu, jeśli wyrazi taką wolę. Ma to ułatwić cały proces, przyspieszyć go, a także sprawić, by był on mniej stresujący dla klienta. Drugie rozwiązanie, opierające się na tej samej usłudze foto ID, pozwala na zdalny onboarding nowych klientów – potwierdzenie tożsamości odbywa się poprzez rozpoznawanie cech biometrycznych klienta i porównywanie ich ze zdjęciem z dowodu.

Nest Bank

Kolejnym bankiem, który udostępnił, a właściwie rozszerzył dla swoich klientów możliwość założenia konta przy wykorzystaniu wideoweryfikacji, jest Nest Bank. Bank udostępniał taką możliwość praktycznie od początku działania, została ona jednak wyłączona w kwietniu i przywrócona w maju dla klientów indywidualnych, a w czerwcu bank udostępnił tę funkcjonalność również dla klientów firmowych. Proces weryfikacji tożsamości wygląda tak samo dla obu grup klientów i wymaga jedynie dowodu osobistego oraz komputera z kamerą internetową. Usługa dostępna jest w godzinach pracy konsultantów.

Banki mogą również być dostawcami tożsamości dla rozwiązań eID udostępnianych przez tzw. brokerów tożsamości – przykładem jest tu usługa mojeID Krajowej Izby Rozliczeniowej, która posiada już łącznie 13 wdrożeń, w takich podmiotach jak PGNIG czy PZU, a według informacji prasowych, tylko w sierpniu Totalizator Sportowy pozyskał za pomocą mojeID 10 tys. nowych klientów.

Warto jednakże podkreślić, że w cyfrowej tożsamości kluczowe jest to, aby była ona szeroko otwarta zarówno na „dawców", jak i na „biorców" tożsamości, a jedynym ograniczeniem powinny być aspekty biznesowe.

Cyfrowa tożsamość umożliwia rozwój nowoczesnych zdalnych usług zaufania (np. podpisu elektronicznego w chmurze), które wymagają zaadresowania kwestii kompleksowego mechanizmu zdalnego uwierzytelniania. Zgodnie z rozporządzeniem eIDAS rejestracja użytkownika w takiej usłudze może zostać zrealizowana w oparciu o identyfikację elektroniczną o poziomie wiarygodności średnim lub wysokim, o ile pierwotne potwierdzenie tożsamości było bezpośrednie. Dzięki wykorzystaniu mechanizmu identyfikacji elektronicznej użytkownik chcący korzystać z kwalifikowanej usługi nie musi osobiście stawić się w punkcie rejestracji, a całość usługi może zostać wykonana zdalnie. Także inne usługi zaufania, o ile wymagają inicjalnej rejestracji użytkownika, będą korzystały z mechanizmów identyfikacji elektronicznej.

Ekspert raportu

Miłosz Brakoniecki
Partner Obserwatorium.biz

Regulatorzy w Unii Europejskiej szukają rozwiązania, które zapewni jednolity i interoperacyjny model elektronicznej identyfikacji na poziomie wspólnego rynku. „Europejskie eID" może mieć charakter usługi identyfikacji, która będzie dostarczana przez notyfikowane podmioty komercyjne lub przez państwa narodowe. Nowe podejście w tym zakresie musi spełniać najwyższe normy bezpieczeństwa przy jednoczesnej powszechnej dostępności i możliwości działania w e-usługach administracyjnych i komercyjnych wszystkich krajów Unii.

OBSERWATORIUM . BIZ

Firmy ubezpieczeniowe

Polski rynek ubezpieczeń również przyspieszył proces kompleksowej digitalizacji swoich usług. Regulatorzy intensywnie i konsekwentnie wsparli ten trend. Niezależnie od stanowiska UKNF z 5 czerwca 2019 r., ściśle w związku z epidemią COVID-19 KNF wydał Pakiet Impulsów Nadzorczych *(Pakiet Impulsów Nadzorczych na rzecz Bezpieczeństwa i Rozwoju w obszarze rynku ubezpieczeniowego)*, w którym m.in. wprost dopuszcza przeprowadzenie procesu zawarcia umowy ubezpieczenia drogą elektroniczną, po uzyskaniu na to zgody klienta. W takim przypadku należy jednak pamiętać o odpowiednim udokumentowaniu poszczególnych elementów procesu zawierania umowy.

Niezależnie Polska Izba Ubezpieczeń wydała „Rekomendacje działań proklienckich dla rynku ubezpieczeń", w których zaleca m.in. wprowadzenie uproszczonego procesu odnawiania umów, zawierania nowych umów lub, na wniosek klienta, przedłużenia umów, których okres ubezpieczenia kończy się w czasie pandemii. Rekomendacja wspomina również o zdalnych oględzinach i telemedycynie.

Dostawcy usług zaufania

Mówiąc o zdalnej weryfikacji tożsamości, warto też dodać, że podobnie rygorystyczne procedury identyfikacji klientów jak instytucje finansowe muszą stosować dostawcy usług zaufania. Tu również można zaobserwować zmianę podejścia do metod takiej weryfikacji.

Pojawiły się pierwsze procesy zdalnej identyfikacji kontrahentów chcących po raz pierwszy nabyć usługę zaufania u danego dostawcy tych usług.

PRZYKŁAD RYNKOWY!
Szwajcaria:

W Szwajcarii właśnie w związku z zaistniałą sytuacją pandemiczną umożliwiono dostawcom e-podpisów onboarding nowych klientów w procesie e-identyfikacji, opartym o wideokonferencję.

Ekspert raportu

Andrzej Ruciński
doradca prezesa
Asseco Data Systems

Obserwujemy w Polsce bardzo niepokojące zjawisko. Dostawca zagraniczny, podlegając pod nadzór w swoim kraju, może np. stosować zatwierdzoną tam metodę automatycznej wideoweryfikacji tożsamości osoby wnioskującej o certyfikat kwalifikowany podpisu. Tym samym może w ten sposób obsługiwać klientów na terenie m.in. naszego kraju. Z kolei brak jednoznacznych regulacji prawnych dla rozwiązań opartych o wideoweryfikację i ścieżki zdalne na poziomie naszego państwa, powoduje chaos interpretacyjny, co znacznie utrudnia stosowanie tego typu rozwiązań przez polskich dostawców. Stawia to nasze firmy w gorszej sytuacji na rynku usług zaufania nie tylko w Europie, ale nawet we własnym państwie.

asseco DATA SYSTEMS

1.2.6 Edukacja i działania CSR

Poważną barierą utrudniającą wdrożenie opisanych powyżej rozwiązań cyfrowych były często niedostateczne kompetencje cyfrowe lub koszty i niekorzystne uwarunkowania infrastrukturalne korzystania z tego typu usług. Budując i rozwijając usługi kwalifikowane gwarantujące odpowiednie narzędzia i bezpieczeństwo, warto wykorzystać zdobyte doświadczenia przy upowszechnianiu, popularyzacji i zwiększeniu dostępności rozwiązań, które docelowo mają też szansę wprowadzić na wyższy poziom kulturę bezpieczeństwa w korzystaniu z produktów i usług cyfrowych.

1.2.7 Niewykorzystane szanse – zawieranie zdalne umów w branży utilities i telco

Pandemia nie stała się wystarczającym motywatorem do zmian funkcjonalnych na rynku utilities i telco w zakresie wdrażania efektywnych procesów zdalnego pozyskiwania klienta. Zakup usług z kategorii utilities jest domeną, w której od kilku lat niewiele się zmienia, na co wskazywaliśmy już jako Obserwatorium.biz w raporcie *Energia cyfryzacji – stan i kierunki rozwoju cyfrowego kanału obsługi dostawców energii i gazu w Polsce* w 2017r. Spośród czołowych polskich dostawców energii i gazu jedynie dwóch oferuje swoim potencjalnym klientom podpisanie umowy przez internet. Ci dostawcy to Energa, dostawca gazu i prądu koncentrujący się na terenach północnej i centralnej Polski, oraz Lumi – operujący w Warszawie podmiot wywodzący się z marki PGE. W pierwszym przypadku nowy klient może otrzymać umowę na adres email, w drugim – umowa podpisywana jest za pośrednictwem opisywanej wcześniej platformy podpisowej Autenti. Takie rozwiązania nie tylko ułatwiają zmianę dostawcy energii, ale pozwalają też na zwiększenie konwersji – potencjalny klient nie musi zapoznawać się z ofertą w internecie, umawiać na wizytę w biurze i dopiero tam podpisywać umowę. Nowy klient jest obsługiwany całościowo w jednym kanale i może wszystko załatwić bez wstawania od komputera. To rozwiązanie zapewnia również współpracująca z Lumi platforma Rachuneo.

Podpisanie umowy z dostawcą energii elektrycznej	Enea	Tauron	PGE	Energa	Innogy	Lumi PGE
Proces on-line	NIE	NIE	NIE	TAK	NIE	TAK
Wniosek on-line, zakończenie kurierem	NIE	TAK	NIE	TAK	NIE	TAK
Formularz kontaktowy	TAK	TAK	TAK	TAK	TAK	TAK

Podobnie wygląda rynek operatorów komórkowych. Jedynie dwóch z wiodących dostawców posiada w swojej ofercie produkty, które można kupić w całości przez internet, wliczając w to podpisanie umowy – warto w tym miejscu dodać, że nie są to „standardowe" oferty tych dostawców, a raczej produkty skierowane do wybranych segmentów rynkowych. Ci dostawcy to Orange, ze swoją ofertą Orange Flex i T-Mobile (marka Heyah z ofertą Heyah 01). W przypadku Orange Flex aktywacja usługi następuje za pośrednictwem aplikacji mobilnej służącej również do zarządzania usługą i płatnościami, Heyah 01 wykorzystuje w swoim procesie rozwiązanie MojeID KIR. W przypadku pozostałych większych operatorów w Polsce poza osobistym podpisaniem umowy w biurze operatora możliwe jest jedynie podpisanie umowy za pośrednictwem kuriera.

Nowy numer	Play	Plus	Orange	T-Mobile	Heyah 01
Proces on-line	NIE	NIE	TAK	NIE	TAK
Wniosek on-line, zakończenie kurierem	TAK	TAK	TAK	TAK	TAK
Formularz kontaktowy	TAK	TAK	TAK	TAK	NIE

Równie niewielu dostawców oferuje usługę elektronicznego zawarcia umowy na internet lub internet i telewizję. Jednym z większych lokalnych dostawców pozwalających swoim potencjalnym klientom na zdalne zawarcie umowy w kanale elektronicznym jest łódzka Toya, w której proces wygląda bardzo podobnie jak w Enerdze – klient dostaje na adres email umowę, której akceptacja pozwala na kontynuację prac i podłączenie do internetu. Inną praktykę stosuje platforma Canal +, dostarczająca tylko telewizję; nowy klient może zawrzeć umowę przez internet, a uiszczenie opłaty uznawane jest za zawarcie wiążącej umowy (oczywiście z możliwością wypowiedzenia jej w terminie 14 dni).

Telewizja + internet	Inea	Netia	TOYA	Orange	Canal +	Cyfrowy Polsat
Proces on-line	NIE	NIE	TAK	NIE	TAK	NIE
Wniosek on-line, zakończenie kurierem	NIE	NIE	NIE	NIE	NIE	TAK
Formularz kontaktowy	TAK	TAK	TAK	TAK	TAK	TAK

Z perspektywy użytkownika brakuje jest więc pełnej możliwości zdalnej obsługi klienta w zakresie rejestracji i zdalnego podpisania umowy. Jest to obszerne pole do zagospodarowania przez dostawców rozwiązań bazujących na elektronicznej identyfikacji i usługach zaufania, tym bardziej że w kolejnych miesiącach ograniczenie funkcjonowania oddziałów podmiotów z tej branży oraz niewydolność firm kurierskich może się znowu zwiększyć.

EKSPERT RAPORTU

– RYZYKA ZWIĄZANE Z „NIECHLUJNĄ" CYFRYZACJĄ

Michał Tabor
Partner
Obserwatorium.biz

Przyspieszona cyfryzacja procesów biznesowych w wielu sytuacjach okazała się niezbędna, gdy zaskoczyła nas pandemia i będący jej wynikiem lock-down, a następnie pozostające z nami na dłużej ograniczenia wynikające z zasad dystansu społecznego, wzrostu popularności pracy zdalnej czy ograniczenia funkcjonowania wielu jednostek „naziemnych" podmiotów komercyjnych i administracyjnych. Jednocześnie wdrożenie tzw. prowizorek, czyli rozwiązań na teraz, ze względu na ich niedopracowanie niesie ze sobą całą pulę ryzyk, co jest szczególnie niekorzystne ponieważ wiele tych „szybkich wdrożeń" ze względu na poniesione koszty może być przez wiele lat pozostawione bez zmian. Inne ryzyka związane z „niechlujną" cyfryzacją to:

- zbyt krótki cykl wdrożeniowy, w związku z czym pomija się analizę ryzyka, zgodności, testowanie odporności na błędy;
- wdrożenie rozwiązań z pominięciem analizy ergonomii użytkowania, co może zniechęcić klientów z korzystania z danej funkcjonalności;
- brak analizy rynku oraz analizy prawnej przed wdrożeniem, a co za tym idzie, wybieranie rozwiązań najtańszych lub przypadkowych, które ostatecznie mogą okazać się nieprzydatne, nieskalowalne lub nie spełniać wymogów bezpieczeństwa.

Ważne jest żebyśmy biorąc pod uwagę dotychczasowe doświadczenia, wprowadzali zmiany w procesach w oparciu o analizę biznesową oraz analizę ryzyka, przy uwzględnieniu funkcjonujących i dostępnych usług zaufania.

Rozdział 2
PERSPEKTYWA REGULACYJNA – POLSKA i UE

2.1 Definicje i pojęcia

Jednym z głównych aspektów prawnych cyfryzacji procesów gospodarczych i administracyjnych zawsze była kwestia skutecznego zawierania umów elektronicznie (zdalnie i bez przesyłania papierowych dokumentów).

Zgodnie z Rozporządzeniem eIDAS w obrocie prawnym rozróżniamy trzy poziomy podpisów elektronicznych:

tzw. **zwykły podpis elektroniczny**
najbardziej podstawowy, bez określonych wymogów technicznych

zaawansowany podpis elektroniczny
spełniający określone w eIDAS wymogi technologiczno-prawne

kwalifikowany podpis elektroniczny
oparty o kwalifikowany certyfikat podpisu elektronicznego i utworzony za pomocą kwalifikowanego urządzenia do składania podpisu

Rozporządzenie eIDAS wprowadza jasną zasadę: podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych (art. 25 ust. 1 eIDAS).

Natomiast kluczowe skutki prawne w odniesieniu do KWALIFIKOWANEGO PODPISU ELEKTRONICZNEGO zostały sformułowane w ust. 2 tego samego art. 25 eIDAS. Otóż przepis ten mówi, że ***kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.***

Innymi słowy, kwalifikowany podpis elektroniczny już na mocy unijnego prawa może zastąpić podpis własnoręczny bez konieczności wprowadzania dodatkowych zapisów w krajowych ustawodawstwach. Odróżnia to znacząco jego moc prawną od pozostałych rodzajów podpisów elektronicznych.

Gdy dodamy do tego zgodnie z art. 25.3 jego transgraniczny charakter, oznaczający że *kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich*, uzyskujemy jedno mocne narzędzie do oświadczeń woli w całej UE.

Aby móc przeprowadzać jak najwięcej czynności elektronicznie i korzystać z zapisów zawartych w eIDAS, należy wiedzieć, jaki rodzaj podpisu można zastosować dla danej czynności prawnej.

W pierwszej kolejności należy zaznaczyć, że zarówno w Polsce, jak i w przeważającej większości państw europejskich prawo cywilne wyraża zasadę swobody wyboru formy czynności prawnej. Dopiero jeśli dla konkretnej czynności zastrzeżona jest w przepisach określona forma, wówczas należy ograniczyć dobór narzędzi do dokonania takiej czynności lub rozważyć, czy ewentualne skutki niedochowania zastrzeżonej prawem formy są dla nas akceptowalne (nie zawsze skutkiem będzie nieważność czynności).

Na gruncie polskim wyróżniamy w szczególności:

formę pisemną
- to najbardziej powszechna forma czynności prawnych.
Jest bardzo mocno *wpisana* w naszą kulturę. Do zachowania zwykłej formy pisemnej czynności prawnej wystarczy złożenie **własnoręcznego podpisu** na dokumencie obejmującym jej treść.

formę elektroniczną - równoważną formie pisemnej.
Do zachowania elektronicznej formy czynności prawnej wymagane jest spełnienie dwóch przesłanek: złożenie oświadczenia woli w postaci elektronicznej oraz opatrzenie składanego oświadczenia woli kwalifikowanym podpisem elektronicznym.

formę dokumentową
Do zachowania tej formy wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie. Dokumentem jest natomiast dowolny nośnik informacji, który pozwala zapoznać się z jej treścią. Podstawową różnicą pomiędzy tą formą a formą pisemną (lub formą elektroniczną) jest wobec tego brak konieczności opatrzenia dokumentu własnoręcznym podpisem (lub kwalifikowanym podpisem elektronicznym). Dochowujemy formy dokumentowej w przypadku dokumentu w postaci tekstowej z podpisem powielanym mechanicznie (np. ksero, skan), a także wiadomości elektronicznej (mailowej) zakończonej wpisaniem imienia i nazwiska piszącego lub danymi pozwalającymi ustalić jego tożsamość. Ale będzie to też w pewnych sytuacjach kliknięcie przycisku „Akceptuję" na stronie internetowej. Wszystkie te formy mają na celu powiązanie osoby możliwej do zidentyfikowania z informacjami przechowywanymi w formie elektronicznej. Formą dokumentową będzie wobec tego zastosowanie zarówno zwykłego podpisu elektronicznego, jak i zaawansowanego podpisu elektronicznego.

Najistotniejsze jest zidentyfikowanie, która z wymienionych form czynności prawnych będzie właściwa dla czynności, którą chcemy digitalizować. Posiadając tę wiedzę, możemy odpowiednio dobrać poziom elektronicznego podpisu.

Formy czynności prawnych (Kodeks cywilny)	**Dochowanie formy prawnej w postaci elektronicznej**
Akt notarialny	**Brak postaci elektronicznej**
Forma pisemna (z podpisami poświadczonymi notarialnie)	Brak równoważnej postaci elektronicznej – możliwa **kopia elektroniczna** oryginału papierowego poświadczona za zgodność przez notariusza kwalifikowanym podpisem.
Forma pisemna (z urzędowo poświadczoną datą)	**Forma elektroniczna + kwalifikowany znacznik czasu** dokument opatrzony kwalifikowanym podpisem elektronicznym i oznaczony kwalifikowanym znacznikiem czasu (data pewna).
Forma pisemna	**Forma elektroniczna** – dokument elektroniczny opatrzony kwalifikowanym podpisem elektronicznym - istnieje prawne domniemanie prawdziwości dokumentu i złożonego podpisu.
Forma dokumentowa	**Dowolny sposób zarejestrowania** oświadczenia woli, pozwalający zapoznać się z treścią tego oświadczenia i wskazać osobę składającą to oświadczenie. W przypadku postaci elektronicznej, w zależności od rodzaju użytego podpisu elektronicznego będzie różny poziom mocy dowodowej dokumentu elektronicznego.
Forma bezdokumentowa (np. forma ustna lub domniemana)	**Ważne:** jeśli prawo zastrzega pod rygorem nieważności, dla czynności prawnej formę pisemną dokumentową albo elektroniczną, czynność dokonana bez zachowania zastrzeżonej formy jest nieważna.

Ważne: jeśli dla danej czynności prawnej (np. zawarcia umowy) forma pisemna była wymagana pod rygorem nieważności, to niedochowanie tego wymogu powoduje nieważność tej czynności (np. nieważność umowy).

W praktyce różnych państw UE waga prawna poszczególnych e-podpisów rozkłada się bardzo różnorodnie.

Warto jeszcze wspomnieć o jednej z koncepcji, które legły u podstaw unijnej regulacji związanej z usługami zaufania i elektroniczną identyfikacją. Chodzi o - technologiczną neutralność – która ma być gwarantem tego, że regulacje prawne związane z elektronicznym obrotem nie staną się przestarzałe i niedostosowane do rozwoju nowych technologii. Jest to aspekt uwzględniany powszechnie w regulacjach prawnych związanych z elektroniczną identyfikacją i elektronicznym obrotem. Zasada technologicznej neutralności jest również podstawą dla równego traktowania przez władze publiczne różnych technologii i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania eliminacji technologii konkurencyjnych przy poszerzaniu rynku usług teleinformatycznych.

2.2 Bariery w digitalizacji a praktyka działania w różnych krajach

Świat biznesu prowadzonego cyfrowo należy już chyba dzielić na ten sprzed pandemii COVID-19 i ten po rozprzestrzenieniu się COVID-19. W świecie sprzed pandemii jasne było, co wielokrotnie podnoszono na różnych forach, że możliwość prowadzenia biznesu w sposób w pełni elektroniczny w relacji z klientami, administracją publiczną i zasobami wewnętrznymi była w wielu krajach mocno ograniczona.

„Nie we wszystkich państwach europejskich dochowanie formy pisemnej jest główną przyczyną opóźniania transformacji cyfrowej”.

To, co wówczas stanowiło barierę dla digitalizacji, pozostało do pewnego stopnia aktualne, choć z oczywistych względów straciło na doniosłości w obliczu palącej potrzeby uwzględnienia w całej gospodarczej działalności społecznego dystansowania. Wciąż głównym problemem pozostaje konieczność dochowania formy pisemnej dla różnego rodzaju czynności. Nie można jednak zapominać, że akurat na gruncie prawa polskiego dla ogromnej większości czynności taka forma nie będzie konieczna. Natomiast te czynności, które mają zastrzeżoną formę pisemną, można swobodnie zastąpić kwalifikowanym podpisem elektronicznym.

PRZYKŁAD RYNKOWY

Anglia:
W Anglii koncepcja „na piśmie" i „w dokumencie" zdaje się nie budzić już kontrowersji. W 2001 roku Komisja Prawna (the Law Commission) opublikowała opinię skierowaną do rządu brytyjskiego, w której wyjaśniła powyższe pojęcia, stwierdzając, że oba oznaczają treści mogące występować również w postaci elektronicznej.

[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/

Polska:
Chcąc uzyskać informację o kontrahencie poprzez Biuro Informacji Gospodarczej, należy złożyć stosowne upoważnienie podpisane własnoręcznie przez konsumenta. Jest to wymóg wprost wskazany w przygotowanej przez BIG instrukcji wypełniania tych upoważnień. Powoduje to konieczność składania ich w formie pisemnej, choć podobnego wymogu nie znajdziemy w przepisach ustawowych.

W praktyce przedsiębiorców brakuje jednak rzetelnej weryfikacji wymogów prawnych – najczęściej po prostu zakładamy, że konieczny będzie własnoręczny podpis na papierze nawet tam, gdzie prawo nie zastrzega żadnej określonej formy prawnej danej czynności. Brakuje też zaufania do prawnej skuteczności elektronicznych podpisów.

PRZYKŁAD RYNKOWY

Rumunia:
W Rumunii sytuacja prawna jest o tyle szczególna, że ustawa, która miała dostosować prawo krajowe do eIDAS, nie została jeszcze uchwalona. Natomiast samo eIDAS pozostawia pewną swobodę w kształtowaniu wymogów szczególnych co do formy prawnej wybranych czynności.

O ile kwalifikowany podpis elektroniczny jest generalnie honorowany w obrocie, o tyle nie jest do końca jasna prawna skuteczność zwykłego oraz zaawansowanego podpisu elektronicznego.

Kontrowersje związane są głównie z praktyką podpisywania umowy o pracę podpisami elektronicznymi niebędącymi kwalifikowanymi. Problem sprowadza się do praktyki Terytorialnej Inspekcji Pracy (Territorial Labor Inspectorate), która niechętnie uznaje tak podpisane umowy za ważne, co z kolei może narazić pracodawcę na grzywny w związku z potencjalnym zaniedbaniem obowiązku doręczenia pracownikowi „oryginału" umowy o pracę.

Niejednokrotnie barierą nie jest sama forma czynności przewidziana w przepisach, ale forma, w jakiej dokument może być zaakceptowany przez dany organ państwowy, publiczny rejestr, czy to ze względu na specyficzne przepisy wykonawcze, czy z uwagi na przyjętą praktykę. Chociaż stanowisko rejestru nie musi mieć wpływu na ważność dokumentu, może być wymagane zarejestrowanie dokumentu, aby był on wykonalny w kraju lub za granicą. To, czy rejestr może przyjąć lub będzie przyjmował podpis w określonej formie, ma zatem rzeczywiste znaczenie dla skuteczności podjętej czynności prawnej.

Wciąż się boimy stosować wersje elektroniczne. Wiele obaw wynika ze słabej znajomości technicznych możliwości elektronicznych podpisów i konsekwencji prawnych ich stosowania. Czy na pewno są poprawnie użyte? Czy dla danej czynności mają moc prawną? Jaką mają wartość dowodową? Gdy schodzimy na poziom konkretnych procesów zaczynają się również pojawiać szczegółowe praktyczne problemy.

Oto przykłady takich trudnych dla odbiorców usług zaufania kwestii prawnych:

- **Czy fakt, że dokument elektroniczny nie ma jednego oryginału czy innej ograniczonej ich liczby, jest wadą czy zaletą?**

Tu oczywiście zależy to od procesu. Na przykład przy wystawianiu elektronicznych faktur warto właśnie z tego względu zadbać o ścisłą kontrolę punktów dostępu do dokumentu, żeby nie dublować czynności zarządczych z nim związanych, takich jak wielokrotne opłacanie jednej faktury. Niemniej jednak „wielość" oryginałów jest właśnie jedną z głównych zalet e-dokumentów, pozwalających optymalizować obieg dokumentacji, w którym nie trzeba czekać, aż jeden papierowy oryginał „obiegnie" wszystkie zainteresowane strony.

- **Czy każda ze stron umowy może ją podpisać w innej formie prawnej?**

Zasadniczo przyjmuje się to za dopuszczalne. Będzie to szczególnie praktyczne w sytuacji, gdy jedna strona będzie chciała podpisać umowę kwalifikowanym podpisem elektronicznym, podczas gdy druga nie będzie chciała złożyć elektronicznego podpisu lub nie będzie miała takiej możliwości. Wówczas możliwe jest zawarcie jednego egzemplarza w zwykłej formie pisemnej, a drugiego w równoważnej formie elektronicznej. Trzeba jednak pamiętać, aby na początek sprawdzić ustawowe wymogi co do formy czynności postanowienia w tym zakresie zawarte w samej umowie. Po podpisaniu umowy trzeba również dopilnować, aby strony wymieniły się egzemplarzami podpisanych umów.

- **Jak wykazać umocowanie danej osoby do działania w imieniu osoby prawnej przy elektronicznym podpisaniu umowy?**

Na gruncie polskim nie jest to łatwe pytanie. Otóż technologicznie zamieszczenie w elektronicznym podpisie opisu stanowiska i firmy, którą się reprezentuje, jest jak najbardziej wykonalne. Taką możliwość przewidują np. podpisy elektroniczne wydawane przez Asseco.

Podobnie na platformach do e-podpisów znajdują się niekiedy pola obejmujące dane dotyczące firmy, którą reprezentuje podpisujący, i funkcji tej osoby w ramach firmy.

Dla zwiększenia wagi dowodowej można również rozważyć umieszczenie obok osobistego podpisu elektronicznego, dodatkowo kwalifikowanej pieczęci podmiotu, w imieniu którego ma być zawarta umowa.

Wymienione powyżej dodatkowe elementy w e-podpisie, a nawet dodanie e-pieczęci reprezentowanego podmiotu, nie mają jednak zasadniczo żadnego prawnego waloru poza ewentualnym zwiększeniem wartości dowodowej tak dokonanej czynności, gdyby konieczne było wykazanie, że intencją danej strony było działanie nie we własnym imieniu, lecz w imieniu innego podmiotu.

PRZYKŁAD RYNKOWY

Portugalia:

Portugalia oferuje klasyczne narzędzia do identyfikacji i składania podpisów

- krajowe eID (Cartão de Cidadão [Citizen's Card] – CC eID), czyli eID oparte o kartę elektroniczną;
- mobilne eID (Chave Móvel Digital [Digital Mobile Key] – CMD eID), które jest środkiem uwierzytelniania i podpisu cyfrowego certyfikowanym przez państwo.

Dodatkowo wprowadziła:

- system certyfikacji uprawnień zawodowych [the Professional Attributes Certification System] (Sistema de Certificação de Atributos Profissionais – SCAP).

SCAP służy do uwierzytelniania funkcji, którą właściciel (osoba fizyczna) portugalskiej CC eID lub mobilnej CMD eID pełni w społeczeństwie jako wykwalifikowany specjalista, lub uprawnienia i zakresu umocowania, jakie posiada w spółce publicznej lub prywatnej.

Zarówno CC eID, jak i CMD eID mogą zostać powiązane z kwalifikowanym podpisem elektronicznym. Natomiast łącząc te wszystkie funkcje w ramach SCAP, uzyskujemy niezwykle ciekawe rozwiązanie, pozwalające na powiązanie uprawnień zawodowych lub funkcji w ramach organizacji danej osoby fizycznej korzystającej z kwalifikowanego podpisu elektronicznego z czynnnością posiadania określonego dokumentu elektronicznego.

Korzystanie ze SCAP eID jest opcjonalnym rozwiązaniem dla posiadaczy ważnej portugalskiej karty CC eID lub CMD eID w wieku co najmniej 16 lat.

Ograniczone ramy niniejszego raportu nie pozwalają na pochylenie się nad każdym z problemów i kontrowersji (nawet tylko spośród tych najczęstszych), z jakimi muszą się mierzyć użytkownicy usług zaufania. Nie są to jednak kwestie nie do rozstrzygnięcia. Warto więc niezależnie zadbać o rozsądne i kompleksowe podejście do wdrażania rozwiązań cyfrowych w firmie, a w razie wątpliwości konsultować się.

2.3 Bezpieczeństwo obrotu dokumentów elektronicznych

Wartość dowodowa

Jeśli żaden przepis prawa nie zastrzega dla danej czynności określonej formy, nie musimy w ogóle rozważać ważności bądź nieważności czynności podpisanej elektronicznie. Pozostaje jednak nadal zagadnienie wartości dowodowej czynności dokonanej w tej formie.

Zwykły podpis elektroniczny może spełniać wszelkie wymogi, żeby dokument nim podpisany był uznany za „podpisany" w sensie prawnym. Tak podpisany dokument może być następnie dopuszczony jako dowód w postępowaniu sądowym.

Art. 25 ust. 1 eIDAS mówi: *Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.*

Jednakże strony będą musiały również uwzględnić, jaką wartość dowodową będzie mieć tak sporządzony dokument elektroniczny w przypadku sporu na przykład o to, kto w rzeczywistości podpisał dokument, czy wyraża on intencję strony do związania się daną umową, jaka jest treść dokumentu.

Na gruncie polskiego prawa, ze względów dowodowych, najbardziej pożądaną formą elektroniczną dokumentów sporządzanych w relacji z kontrahentami wydaje się być forma elektroniczna opatrzona kwalifikowanym podpisem elektronicznym. Wynika to z tego, że właśnie taka forma stanowi zdefiniowany w Kodeksie Postępowania Cywilnego **dokument prywatny**.

Dokumentem prywatnym jest każdy dokument tekstowy zawierający własnoręczny albo kwalifikowany podpis elektroniczny wystawcy. Użycie zwykłego podpisu elektronicznego nie będzie wystarczające do powstania dokumentu prywatnego (w rozumieniu przepisów procesowych).

Tymczasem ma on tę zaletę, że korzysta z domniemania prawdziwości (autentyczności), a więc domniemania, że dokument pochodzi od osoby pod nim podpisanej. Ponadto korzysta również z domniemania, że osoba podpisana pod dokumentem złożyła zawarte w nim oświadczenie.

Z praktycznego punktu widzenia, jeśli podczas sporu druga strona będzie twierdzić, że dokument prywatny (dokument podpisany kwalifikowanym podpisem elektronicznym) nie jest autentyczny, będzie musiała udowodnić swoją rację.

Tak jak wspomnieliśmy na początku, dokument ważnie podpisany przy użyciu zwykłego podpisu elektronicznego lub zaawansowanego podpisu elektronicznego powinien również być dopuszczony jako dowód w sprawie. Jednakże jego moc dowodowa będzie w znacznie większym stopniu podlegać swobodnej ocenie sędziego.

Korzystając z tej niższej formy elektronicznej, warto zatem zapewnić odpowiedni stopień udokumentowania tego rodzaju czynności na potrzeby ewentualnych postępowań dowodowych. W szczególności należy zadbać o to, by na wypadek sporu można było możliwie łatwo wykazać:

- czy dostęp do elektronicznego dokumentu został uzyskany za pośrednictwem określonego konta e-mail lub komputera oraz w określonej lokalizacji;
- czy dostęp do dokumentu został uzyskany przy użyciu hasła, kodu PIN, klucza szyfrującego i/lub innego procesu uwierzytelniania;
- czy moment złożenia podpisu był określony;
- czy istnieją różnice między wersjami podpisanego dokumentu będącymi w posiadaniu różnych stron.

Pewność obrotu

To, że podpis elektroniczny jest prawnie wiążący, nie wpływa jeszcze na to, jak bardzo jest on bezpieczny i wiarygodny, podobnie jak nie wpływa to na jego wartość dowodową. Tymczasem bezpieczeństwo i wiarygodność stanowią istotną kwestię dla stron.

Niepewność lub nieznajomość regulacji prawnych utrudnia korzystanie z podpisów elektronicznych. Istotną barierą są jednak również kwestie praktyczne, takie jak bezpieczeństwo podpisów elektronicznych, ich dostępność i łatwość w obsłudze (intuicyjność).

Użytkownicy technologii, na której opierają się usługi zaufania, zazwyczaj nie będą rozumieć tworzącego go systemu bazowego i mogą nie być w stanie ocenić jego niezawodności. Dlatego stanowczo warto rozważyć skorzystanie z dodatkowych metod, które pozwolą zwiększyć zaufanie do użytych technologii i wprowadzą niezbędne narzędzia dające większą pewność np. co do prawidłowej identyfikacji stron, ich umocowania do działania w imieniu innej osoby lub podmiotu, właściwej treści (wersji) dokumentu, który ma być podpisany. Właściwie dobrane metody mogą ułatwić postępowanie dowodowe na wypadek sporu.

Jedną z takich metod gwarantujących określony poziom usługi i bezpieczeństwo technologii, jest skorzystanie z tzw. zaufanej trzeciej strony (Trusted Third Party; TTP), podlegającej certyfikacji i stałemu nadzorowi. W zakresie Usług Zaufania rolę takiej zaufanej trzeciej strony pełnią kwalifikowani dostawcy usług zaufania. Standaryzacja Usług Zaufania na poziomie UE oraz certyfikacja dostawców tych usług ma właśnie gwarantować bezpieczeństwo użytkownikom, czyli, zgodnie z terminologią eIDAS – „stronie ufającej".

W kontekście zabezpieczenia procesów elektronicznych ciekawym zjawiskiem są **platformy do podpisów elektronicznych i wymiany e-dokumentów**, również te całkowicie zautomatyzowane, czyli tzw. EDI (electronic data interchange).

Zaletą korzystania z tego rodzaju platform jest to, że są one dostępne z dowolnego miejsca i zapewniają pełną widoczność procesu podpisywania oraz ułatwiają weryfikację i edycję elektronicznych dokumentów.

Inną zaletą jest to, że podczas zawierania transakcji na platformie podpisu elektronicznego generowany jest cyfrowy ślad dokumentujący ten proces. Rejestrowane są osoby, które podpisały dokument (w tym ich adres e-mail i IP), wszelkie dodatkowe kroki podjęte w celu uwierzytelnienia osoby podpisującej (np. kod wysyłany na telefon komórkowy osoby podpisującej), a sam cyfrowy ślad jest zazwyczaj opatrzony elektroniczną pieczęcią lub przynajmniej elektronicznym znacznikiem czasu. Taki cyfrowy ślad będzie można również wykorzystać w razie sporu w postępowaniu dowodowym.

„Odmianą tego rodzaju platform, nabierających zwłaszcza ostatnio znaczenia, są elektroniczne platformy do zdalnego głosowania".

PRZYKŁAD RYNKOWY

Norwegia:
W Norwegii wyjątkowo popularne stały się dla tego celu narzędzia służące odbywaniu standardowych telekonferencji, takie jak Zoom i Teams.

Istnieje już jednak także wiele platform wyspecjalizowanych w organizacji zgromadzeń akcjonariuszy/wspólników, umożliwiających w bezpiecznym środowisku przeprowadzenie np. tajnego głosowania.

Korzystając z tego rodzaju platform, nie należy zapominać o przepisach odnoszących się do gromadzenia i przetwarzania danych osobowych. W szczególności należy zwrócić uwagę, że regulacje te mogą się różnić w zależności od tego, o czyich danych mówimy (obywatelach którego państwa).

Rosja:
Zgodnie z Prawem Miejsca na gruncie rosyjskiej ustawy federalnej o danych osobowych (nr 152-FZ), dane osobowe obywateli rosyjskich, będące w posiadaniu administratorów danych, muszą być przetwarzane na serwerach fizycznie zlokalizowanych w Rosji. Dlatego tak ważne jest określenie i uwzględnienie ryzyka związanego z korzystaniem z platform zagranicznych.

2.4 Transgraniczność usług zaufania

eIDAS potwierdza zasadę, że wszelkie podpisy elektroniczne są z założenia zdolne do wywierania skutków prawnych. Ponadto regulacja unijna dąży do zapewnienia wspólnego standardu podpisu elektronicznego (ze szczególnym naciskiem na jednakowo wysoki standard kwalifikowanego podpisu elektronicznego). Celem takiej standaryzacji jest w pierwszej kolejności zapewnienie uznawania prawnej mocy kwalifikowanego podpisu elektronicznego we wszystkich państwach członkowskich pomimo wydania go tylko w jednym państwie członkowskim. Biorąc pod uwagę wyniki naszego badania, można mówić wyłącznie o formalnej transgraniczności usług zaufania, zapewnionej przepisami unijnymi i respektowanej teoretycznie we wszystkich krajowych porządkach prawnych. W praktyce jednak podmioty z danego państwa członkowskiego wybierają swoich narodowych dostawców usług zaufania, a elektroniczne podpisy zagranicznych dostawców są cały czas rzadko spotykane. Granice państw unijnych przekraczają natomiast platformy do podpisywania elektronicznych dokumentów. Do najbardziej rozpowszechnionych platform należą DocuSign i AdobeSign, obecne praktycznie w każdym państwie członkowskim. Być może więc transgraniczność usług zaufania przyjdzie właśnie tą drogą, tzn. poprzez ich wykorzystanie na międzynarodowych platform do podpisów.

e-Notaryzacja

Problem braku transgraniczności jest jednak szerszy. Otóż sam fakt uznania ważności czynności dokonanej z wykorzystaniem e-podpisu nie gwarantuje jeszcze jej egzekwowalności (wykonalności), a tym bardziej nie zapewnia tej wykonalności w innym państwie.

Transgraniczna wykonalność elektronicznych czynności prawnych łączy się co najmniej z dwoma zagadnieniami, które wciąż czekają na ich zaadresowanie w procesie cyfryzacji obrotu gospodarczego. Mianowicie:

1 nierozwiązane w większości państw europejskich zagadnienie **e-notaryzacji**;

2 brak faktycznej możliwości elektronicznej **legalizacji zagranicznych dokumentów.**

e-notaryzacja

Z naszego badania wynika, że wśród podstawowych obszarów prawnych, które w dalszym ciągu stawiają opór digitalizacji, na pierwszym miejscu można wskazać czynności wymagające uczestnictwa notariusza.

Wśród badanych przez nas państw udział notariusza jest powszechnie wymagany przy:

- **czynnościach prawnych odnoszących się do nieruchomości;**
- **czynnościach dokonywanych w obszarze prawa rodzinnego lub spadkowego;**
- **sporządzaniu aktów założycielskich spółek handlowych;**
- **niekiedy również przy przeniesieniu własności udziałów w spółce.**

W odniesieniu do procesu zakładania spółek handlowych warto wspomnieć, że ma on szansę być wkrótce w pełni cyfrowy w poszczególnych państwach członkowskich. Najpóźniej do 1 sierpnia 2021 roku państwa członkowskie są zobowiązane implementować dyrektywę PE i Rady (UE) 2019/1151 z 20 czerwca 2019 r. zmieniającej dyrektywę (UE) 2017/1132 w odniesieniu do stosowania narzędzi i procesów cyfrowych w prawie spółek. Dyrektywa m.in. wymaga zagwarantowania możliwości całkowicie zdalnego tworzenia spółek, bez konieczności osobistego stawiennictwa.

W tym kontekście należy się spodziewać, że przynajmniej część krajowych ustawodawców będzie musiała wprowadzić jakiegoś rodzaju zdalną formę notaryzacji.

W Polsce trwają już prace nad stworzeniem przepisów umożliwiających zakładanie on-line spółki z ograniczoną odpowiedzialnością, za pomocą wzorca przygotowanego przez notariusza, lecz bez fizycznej obecności w kancelarii notarialnej.
https://www.gov.pl/web/aktywa-panstwowe/nowe-technologie-w-funkcjonowaniu-prawa-handlowego

PRZYKŁAD RYNKOWY

Niemcy:
Podobne prace zostały też podjęte w Niemczech, gdzie już teraz notariusze mogą poświadczać urzędowo niektóre dokumenty i wydawać proste zaświadczenia w formie elektronicznej.

Czechy:
Czechy również rozważają wprowadzenie zmian, które pozwolą całkowicie online zakładać spółki przy wykorzystaniu zdalnej komunikacji z notariuszem.

Istnieją również państwa, które w obliczu pandemii podjęły od razu dalej idące kroki w kierunku pełnej cyfryzacji czynności notarialnych.

Belgia:
W Belgii od kilku miesięcy możliwe jest podpisywanie aktów notarialnych za pomocą elektronicznego pełnomocnictwa.

Austria:
Jeżeli czynność prawna, oświadczenie lub istotna z prawnego punktu widzenia okoliczność faktyczna wymaga dla skuteczności formy aktu notarialnego lub innego publicznego lub publicznie poświadczonego aktu, wówczas, aby zapobiec rozprzestrzenianiu się COVID-19, czynności notarialne wymagane do sporządzenia aktu mogą być również dokonywane przy użyciu środków komunikacji elektronicznej.

Legalizacja zagranicznych dokumentów

Przy korzystaniu w innym państwie z zagranicznych dokumentów, aby wykazać ich pochodzenie od oficjalnych organów państwowych, konieczna jest niejednokrotnie ich legalizacja. W odniesieniu do państw, które ratyfikowały Konwencję Haską z 1961 roku, oznacza to dołączenie oficjalnej klauzuli *apostille* na dokumencie. Obecnie nie ma możliwości uzyskania elektronicznej *apostille* na dokumencie elektronicznym. Powoduje to, że dokumenty, które potencjalnie mogłyby wymagać legalizacji, należałoby sporządzać zapobiegawczo w tradycyjnej formie papierowej.

2.5 Rozwój usług zaufania w Europie

Europejski rynek dostawców kwalifikowanych usług zaufania w ciągu ostatnich miesięcy znacznie urósł. Między majem 2019 a czerwcem 2020 roku na rynku pojawiło się 58 nowych dostawców. Poszerzenie rynku wynika przede wszystkim z dostępności oraz umocnienia się narzędzi identyfikacji elektronicznej (np. wideoweryfikacji), które wspierają procesy rejestracji oraz identyfikacji podmiotów do nowych usług zaufania w skali międzynarodowej.

Liczba dostawców usług zaufania w Europie i wybranych rynkach krajowych

Kwalifikowana usługa zaufania	Europa	Polska	Niemcy	Włochy	Hiszpania	Francja
Razem usługodawców	249[1]	6	12	39	33	22
Wydawanie certyfikatów	208	6	10	40	26	13
Znakowanie czasem	110	5	5	18	21	10
Konserwacja	12	1 (w trakcie)			2	1
Rejestrowane doręczenie elektroniczne	18		2		5	7
Walidacja podpisów i pieczęci	15	1			2	1

Zestawienie kwalifikowanych usług zaufania – stan na wrzesień 2020 r.

W analizowanym okresie w szczególności zauważalny jest wzrost usług wydawania certyfikatów (+48), znakowania czasem (+18), konserwacji podpisów i pieczęci (+11) oraz rejestrowanego doręczenia elektronicznego (+7). W zakresie usług walidacji podpisów i pieczęci rynek poszerzył się o dwóch nowych dostawców. Wyjątkowo pozytywnie odnotowujemy rozwój usług rejestrowanego doręczenia elektronicznego (Francja +3, Hiszpania +2), które posiadają duży potencjał dla obszaru cyfryzacji procesów na styku klient – administracja publiczna.

Jeżeli chodzi o polski rynek, nie pojawili się na nim nowi dostawcy kwalifikowani. W poprzednim raporcie *Biznes bez papieru* wskazywaliśmy na potencjał certyfikatów jednorazowych. Obecnie na rynku polskim jeden z dostawców (KIR) oferuje usługę certyfikatu do jednorazowego kwalifikowanego podpisu, a drugi dostawca Asseco Data System wdrożył jednorazowy podpis zaawansowany w Santander Consumer Banku.

2.6 Rozwój notyfikowanych schematów identyfikacji w Europie

W poprzednim raporcie, z roku 2019, jako Obserwatorium.biz wskazywaliśmy na znaczenie umiędzynarodowienia usług zaufania dzięki wykorzystaniu środków identyfikacji elektronicznej pomiędzy krajami Unii Europejskiej. Zgodnie z eIDAS, państwa członkowskie są zobowiązane do uznawania w usługach on-line notyfikowanych środków identyfikacji elektronicznej, o ile spełniają one wymogi co do ustalonego poziomu wiarygodności (bezpieczeństwa). Notyfikacja oznacza wskazanie krajowego środka identyfikacji jako dostępnego w całej UE.

Na dzień 14 września 2020 roku opublikowano 20 schematów identyfikacji elektronicznej notyfikowanych i prenotyfikowanych (+3 względem roku 2019) – obejmujących różne środki identyfikacji. Za nowe schematy identyfikacji elektronicznej uznajemy schemat z Holandii, Litwy oraz Danii.

W poprzednim raporcie 9 z 17 schematów było w trakcie procedury notyfikacyjnej. Obecnie 19 systemów zostało notyfikowanych, a tylko jeden (portugalski system profesjonalistów) pozostaje w fazie prenotyfikacyjnej.

Najczęściej notyfikowanym środkiem jest karta identyfikacyjna (dowód tożsamości); zauważalny jest również rozwój usług mobilnych (aplikacje mobilne).

Rozdział 3
KOMERCJALIZACJA – PERSPEKTYWA USŁUGOBIORCÓW

3.1 Wykorzystanie usług zaufania i eID do praktyki rynkowej

W ramach badań przeprowadzonych na rzecz niniejszego raportu wśród przedstawicieli biznesu jedynie 3 (7%) z grupy 41 wskazało, że w okresie ostatnich sześciu miesięcy, na który przypadła pandemia COVID-19, ich przedsiębiorstwo nie wdrożyło projektu przenoszącego do kanałów cyfrowych ważne obszary biznesowe.

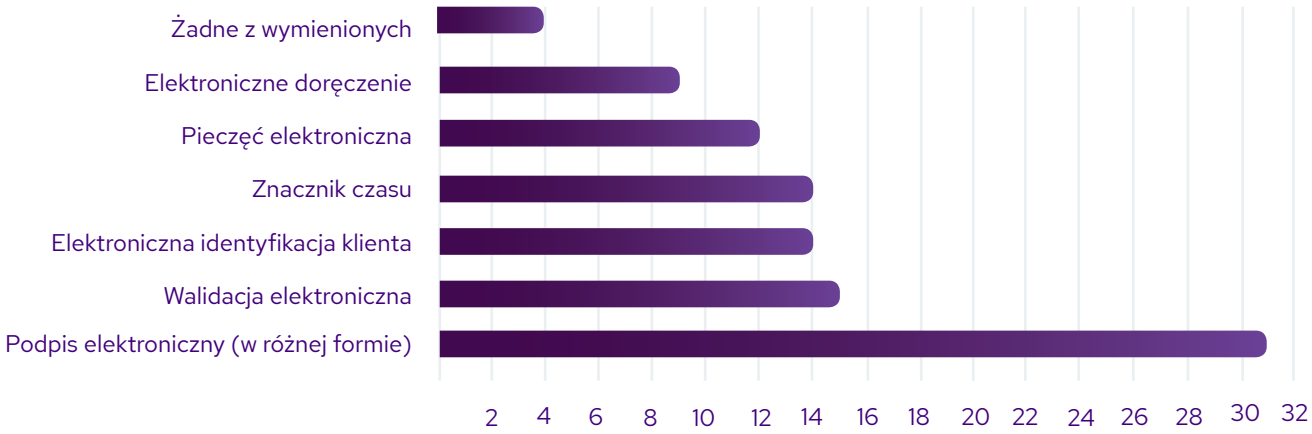
„Zdecydowana większość firm wdrożyła w czasie pandemii rozwiązania przenoszące wybrane obszary swojej działalności do sfery cyfrowej".

Po wyłączeniu trzech respondentów, którzy nie wdrożyli rozwiązania digitalizującego ich działalność, 35 (85% z całej grupy respondentów) z pozostałych 38 respondentów, którzy dokonali takiego wdrożenia odpowiedziało „tak" na uzupełniające pytanie: „Czy pandemia koronawirusa i związana z tym sytuacja wpłynęła na przyspieszenie wdrożenia tych projektów?". Trzech respondentów odpowiedziało „nie". Można więc te wyniki interpretować w taki sposób, że pandemia i wynikające z niej ograniczenia, zdecydowanie przyczyniły się do uruchomienia lub przyspieszenia projektów tego typu.

Wcześniej wpominaliśmy, że telepraca (23 respondentów) oraz procesy wewnętrzne (21), a także HR (18) były najczęściej wskazywanymi obszarami zmian. Rzadziej projektów digitalizujących procesy biznesowe dokonywano w obszarach obsługi klienta (13) oraz sprzedaży (12), co wskazuje na istniejący cały czas potencjał w tych dziedzinach, jeśli uwzględnimy utrzymującą się sytuację związaną z rekomendowanym dystansem społecznym i zmieniające się preferencje społeczne.

Kolejne pytanie dotyczyło wskazania konkretnych rozwiązań organizacyjno -technicznych, które zostały wykorzystane we wdrażanych procesach cyfryzacyjnych z zakresu elektronicznej identyfikacji (eID) oraz poszczególnych usług zaufania. Największą popularnością cieszył się podpis elektroniczny – 31 wskazań (76 %), następnie walidacja elektroniczna – 15 wskazań (37%). Elektroniczna identyfikacja, znacznik czasu, pieczęć elektroniczna oraz elektroniczne doręczenie były wskazywane rzadziej.

Popularność wykorzystania narzędzi eID i usług zaufania w projektach cyfryzacyjnych



Następnie chcieliśmy zweryfikować ważność poszczególnych aspektów prowadzenia inicjatyw i projektów cyfryzacyjnych w kontekście planów firm na kolejne sześć miesięcy. Okazało się, że świadomość narzędzi eID i usług zaufania jest na tyle wysoka, że planuje je uwzględnić 17 respondentów, czyli 41% badanych.. Bardzo istotna okazała się również możliwość łatwej integracji z istniejącymi w firmie procesami i systemami IT – 16 (39%), a także ergonomia i doświadczenie użytkowników (UX) – 12 (29%) oraz zarządzanie ryzykiem operacyjnym i cyberbezpieczeństwo – 10 (24%).

„Firmy są świadome usług zaufania, ale nadal mniej niż połowa z nich bierze je pod uwagę w planowaniu projektów i inicjatyw mających na celu cyfryzację procesów biznesowych”.

„TOP 3 tematów istotnych dla menedżerów realizujących projekty cyfryzacyjne w kontekście narzędzi eID i usług zaufania to:

- **integracja rozwiązań z istniejącymi systemami iT,**
- **ergonomia i doświadczenie użytkowników,**
- **Zarządzanie ryzykiem operacyjnym i cyberbezpieczeństwo”.**

Co Cię najbardziej niepokoi w procesie cyfrowej transformacji?

Przy pytaniu „Co Cię najbardziej niepokoi w procesie cyfrowej transformacji?” respondenci mogli wskazań maksymalnie dwie odpowiedzi. Najczęściej wskazywano brak „know-how” w organizacji – 18 odpowiedzi (44% respondentów), zaraz po nim wysokie koszty bez gwarancji sukcesu – 14 wskazań (34%) oraz konieczność zarządzania zmianą (a więc podnoszenie kwalifikacji personelu, wdrażania procesów, zmiany struktur itp.) – 13 wskazań (31%), a także brak zgodności z przepisami prawa – 12 wskazań (29%).

3.2 Scenariusze rozwoju rynku

Powyżej podjęliśmy próbę scharakteryzowania bieżącej sytuacji na rynku usług zaufania i elektronicznej identyfikacji w kontekście sytuacji biznesowej, w której przedsiębiorcy i kluczowa kadra zarządzająca poszukują – często bardzo pilnie – rozwiązań z zakresu transformacji do środowiska cyfrowego. Oczekują tego od nich klienci – ze względu na zmieniające się preferencje zachowań, akcjonariusze, ze względu na większą efektywność biznesową procesów realizowanych zdalnie, współpracownicy i pracownicy, gdyż w świecie cyfrowym bez problemów realizują inne aktywności życiowe. Sytuacja pandemii tylko pogłębiła i przyspieszyła te zjawiska.

Przyjrzyjmy się teraz scenariuszom rozwoju rynku usług, które z definicji miały stać się narzędziem realizacji tej transformacji w sposób bezpieczny, dzięki wdrożeniu zaufanej trzeciej strony jako naturalnego arbitra w procesie realizowanym realizowanym między dwoma podmiotami elektronicznego kontaktu – ze względów ergonomicznych często pozostającego „w cieniu" całej transakcji. Co musi wydarzyć się na rynku, aby usługi zaufania i eID stały się rzeczywistym gwarantem bezpieczeństwa postępujących zmian w życiu gospodarczym Polski i Europy w aspekcie procesów „paperless"?

Wykorzystanie potencjału e-pieczęci

Kwalifikowana elektroniczna pieczęć w zamierzeniu ma pozwalać osobom prawnym (a więc w szczególności spółkom) autoryzować i zabezpieczać elektronicznie dokumenty. Zgodnie z nazwą ma to być odpowiednik tradycyjnej firmowej pieczątki, tyle że w odniesieniu do danych elektronicznych.

Kwalifikowana pieczęć elektroniczna na gruncie eIDAS nie pozwala na zastąpienie podpisu składanego zgodnie z reprezentacją osoby prawnej, natomiast przynosi szereg możliwości zabezpieczania zobowiązań osób prawnych, takich jak zaświadczenia, zamówienia lub dokumenty, które powstały na podstawie wcześniej zawartych umów.

Przyszłość e-pieczęci jest szeroko dyskutowana zarówno wśród prawników, jak i na poziomie technologii. Jednak w zakresie potencjalnego wykorzystania e-pieczęci do składania oświadczeń woli przez osoby prawne nie ma, jak się wydaje, prostych rozwiązań legislacyjnych.

E-pieczęć jest natomiast świetnym narzędziem, do zastosowania w kontekście dowodowym. Złożona na danym dokumencie elektronicznym, jest gwarantem jego integralności i autentyczności. Jeśli treść e-dokumentu zostanie zmieniona po nałożeniu e-pieczęci, wówczas na etapie weryfikacji otrzymamy komunikat o uznaniu e-pieczęci za wadliwą.

Oczywiście podobny efekt można uzyskać, stosując również inne rozwiązania technologiczne. Jednak przewagą kwalifikowanej e-pieczęci (certyfikowanej zgodnie z eIDAS) jest fakt, że podobnie jak w przypadku kwalifikowanego podpisu elektronicznego, ważność kwalifikowanej e-pieczęci jest domniemana, a po jej wydaniu w jednym państwie członkowskim nie można jej odrzucić w innym państwie członkowskim.

Ciekawym przykładem wykorzystania tych właściwości e-pieczęci jest zabezpieczenie e-pieczęcią opartą o kwalifikowany certyfikat dokumentów podpisywanych zwykłym podpisem elektronicznym (tam gdzie dla ważności transakcji nie jest wymagany KWALIFIKOWANY PODPIS ELEKTRONICZNY). Na takiej zasadzie oparta jest na przykład platforma Autenti. Autentyczność i nienaruszalność treści podpisywanych na platformie dokumentów zabezpieczona jest e-pieczęciami firmy Autenti.

Trudno przewidzieć, jaka przyszłość czeka e-pieczęć. Jest to mimo wszystko narzędzie z ogromnym potencjałem, gdy uwzględnić jego specyficzne cechy. W szczególności może się sprawdzić w obszarach, które:

- wymagają zapewnienia integralności i autentyczności dokumentów na wysokim poziomie;
- preferują automatyzację wydawania dokumentów;
- przenoszą odpowiedzialność za wystawiony dokument na organizację, firmę składającą e-pieczęć (nie ma konieczności poszukiwania osoby odpowiedzialnej indywidualnie za wystawiony e-dokument).

Być może e-pieczęć znajdzie jeszcze szersze zastosowanie, gdy w procesy związane z dokumentacją określonych czynności lub zdarzeń zostanie w szerszym zakresie zaangażowane AI lub IoT.

To jest czas na e-tożsamość, czyli eID

Pandemia pokazała, jak istotne znaczenie dla kompleksowej digitalizacji ma identyfikacja stron. Potrzeba było tej motywacji, żeby zacząć szukać innych, zdalnych rozwiązań dla identyfikacji, wykraczających poza komfortowy mechanizm porównania fizycznie obecnego człowieka z jego tradycyjnym dowodem osobistym.

Zdalny onboarding jest tylko pierwszym krokiem do e-tożsamości. Kluczem jest upowszechnienie środków identyfikacji elektronicznej oraz takie ich uwierzytelnianie, by mogły być stosowane na co dzień w cyfrowym obrocie, również transgranicznym. Obecnie zakres wykorzystania eID jest w nadal niezadowalający.

Jaka jest zatem przyszłość eID w Polsce i w całej Unii Europejskiej?

Latem rozpoczęły się publiczne konsultacje związane z planowaną rewizją eIDAS. Bez wątpienia jednym z motywatorów rozpoczęcia takich działań jest kryzys związany z COVID-19. Osią dyskusji nad koniecznymi zmianami jest w szczególności dążenie do zapewnienia wszystkim obywatelom i przedsiębiorcom europejskim powszechnie akceptowanej, godnej zaufania tożsamości cyfrowej.

Być może zatem w przyszłości należy się spodziewać intensyfikacji działań zmierzających do unifikacji rozwiązań związanych z tożsamością cyfrową, mającą zapewnić szeroki dostęp do kluczowych i wrażliwych usług publicznych w ramach całej Unii Europejskiej.

Cyberbezpieczeństwo - mniej luk i ryzyk

Nieodłączną częścią planowania transformacji cyfryzacji jest zapewnienie bezpieczeństwa nowych rozwiązań. Źle zaprojektowane procesy digitalowe są bardzo podatne na zagrożenia z sieci, co stanowi niejednokrotnie barierę w ich implementacji.

Usługi zaufania odgrywają istotną rolę w zapewnianiu bezpieczeństwa cyfrowego obrotu. Podobnie wprowadzenie powszechnie rozpoznawalnych mechanizmów identyfikacji elektronicznej (eID), umożliwiające jednoznaczną weryfikację tożsamości użytkowników e-usług, ma ogromne znaczenie dla bezpieczeństwa procesów cyfrowych.

EKSPERT RYNKOWY

Marcin Szulga,
Asseco Data Systems Polska

GŁÓWNE TRENDY W USŁUGACH ZAUFANIA

Dynamiczny rozwój usług zaufania następuje od wejścia w życie rozporządzenia eIDAS, tj od 2016 roku. W ostatnim roku aktywny wzrost potęgują cztery trendy oddziałujące na rynek, które niewątpliwie utrzymają się w najbliższych latach:

Pandemia COVID19 przyspieszyła digitalizację klasycznych procesów: rośnie liczba transakcji cyfrowych, które wymagają implementacji zabezpieczeń przy pomocy usług zaufania. Zarysowuje się silny trend odejścia od popularnego modelu subskrypcji w kierunku modelu transakcyjnego wiążącego opłaty za realizację pojedynczych operacji, np. generowania tzw. podpisów w locie (ang. on-the-fly signatures). Izolacja społeczna wymusza kreowanie przez dostawców usług zaufania nowych metod identyfikacji – rośnie popularność wideoidentyfikacji. Uzupełniają ją środki identyfikacji elektronicznej (eID) oraz hybrydowej.

Nowe procesy biznesowe – przemysł 4.0: rozwój usług zaufania wspierać będzie kluczowe właściwości procesów wielkiej skali np. skalowalność, wysoką dostępność, wydajność, rozliczalność lub anonimowość. Tu pojawią się nowe zastosowania usług zaufania i synergie z technologiami wspierającymi procesy przemysłowe tj. IoT, 5G, Blockchain. Rozerwanie światowych łańcuchów dostaw spowoduje konieczność walidacji transakcji pomiędzy poszczególnymi ekosystemami gospodarczymi.

Standaryzacja i zmiany prawne: następuje silny trend wzmacniania warstwy cybersec, czego dowodem jest wdrażanie w życie wymagań dla zdalnych, kwalifikowanych urządzeń do składania podpisu (Remote QSCD's) w postaci załącznika do Decyzji Implementującej KE 650/2016, zgodnie z normami EN 419 241-2 oraz EN 419 221-5. Standaryzacja postępuje także w obszarze API do składania zdalnych podpisów (ETSI TS 119 432, Cloud Signature) i w zakresie formatów podpisów.

Ryzyka cybersec: wzrasta opłacalność ataków na technologie wykorzystywane w usługach zaufania, które najczęściej nakierowane są na elementy niechronione przez kryptografię, w szczególności proces identyfikacji osób fizycznych. Tu z pomocą przychodzi sztuczna inteligencja wspierająca algorytmy wykrywające np. ataki związane z generowaniem w czasie rzeczywistym masek 2D/3D. W obszarze kryptografii także widać ruch (np. ataki na funkcje skrótu, rozwój komputerów kwantowych), co determinuje sposób budowania usług zaufania w kierunku zapewniającym tzw. zwinność kryptograficzną (możliwość szybkiej wymiany algorytmów kryptograficznych).

asseco
DATA SYSTEMS

By zapewnić odpowiedni poziom bezpieczeństwa mechanizmów identyfikacji elektronicznej, wszyscy dostawcy eID powinni podlegać analogicznym wymogom, w szczególności co do gwarantowanego przez nich poziomu bezpieczeństwa i zakresu ich odpowiedzialności. Unifikacja wymogów stawianych dostawcom sprzętu lub oprogramowania następuje na szczeblu unijnym i krajowym.

W ostatnim czasie można było zaobserwować dążenia do przyspieszenia wprowadzenia regulacji związanych z cyberbezpieczeństwem na większą skalę. Zgodnie z tym trendem zapowiedziano niedawno nowelizację ustawy o krajowym systemie cyberbezpieczeństwa w Polsce. Planowane zmiany mają na celu w szczególności wprowadzenie możliwości oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa. Nowelizacja przewiduje również powstanie centr wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa (z angielskiego zwane ISAC, czyli Information Sharing and AnalysisCenter).

PRZYKŁAD RYNKOWY

„W naszej firmie już przed pandemią dość szeroko wdrożyliśmy kwalifikowane podpisy elektroniczne. Związane jest to z obowiązkami podatkowymi, ale też innymi obowiązkami rejestracyjnymi, które obecnie można dopełnić wyłącznie elektronicznie. Ostatnie miesiące wskazały nam jednak pola zastosowania dla podpisów elektronicznych, których wcześniej nawet nie braliśmy pod uwagę.

Wykorzystanie kwalifikowanego podpisu elektronicznego ma jednak więcej zalet. Jedną z nich jest wykorzystanie ich przy jednoznacznej i bezpiecznej identyfikacji w różnego rodzaju procesach. Niezależnie od pandemii, w ostatnim czasie dało się zauważyć powszechne rozluźnienie przy podawaniu danych osobowych w różnego rodzaju sytuacjach. A tymczasem w dzisiejszych czasach jeszcze bardziej trzeba uważać na to jakie informacje są ogólnodostępne, bo niektóre ich kombinacje pozwalają na autoryzację osoby, a to już otwiera drogę do wielu potencjalnych nadużyć, w tym także zagrażających funkcjonowaniu firmy."

Tomasz Budny, CFO firmy agrochemicznej

Walidacja podpisów elektronicznych

Rosnąca popularność podpisów elektronicznych przynosi również konsekwencje w postaci konieczności ich właściwego rozpoznania i to często wśród osób lub podmiotów gospodarczych, które nie są wyspecjalizowane w tym zakresie. To rodzi z kolei wymóg nabycia podstawowych chociażby kompetencji w tym zakresie wśród bardzo szerokiego grona odbiorców. W sukurs przychodzi tu usługa kwalifikowanej walidacji, która zapewnia weryfikację kwalifikowanych podpisów niezależnie od dostawcy rozwiązania – ale również ona jest jeszcze słabo rozpowszechniona i widzimy duży potencjał jej rozwoju.

Elektroniczne doręczenia

Wskazany powyżej przykład z Włoch, gdzie elektroniczne doręczenia sprawdziły się jako narzędzie usprawniające zdalną komunikację i załatwianie spraw biznesowych i administracyjnych w najtrudniejszych okresach pandemii, wskazał na ich niedoceniony do tej pory potencjał. Aktualnie w Unii Europejskiej kwalifikowane e-doręczenia wdrożone są jedynie w pięciu krajach, natomiast ich możliwości jako narzędzia, zarówno jako alternatywy do papierosowych przesyłek poleconych, jak i do zabezpieczania komunikacji biznesowej jest trudny do przecenienia i przy pozytywnym podejściu regulatora na danym rynku elektroniczne doręczenia mogą bardzo mocno przyczynić się do skutecznej cyfryzacji wielu dziedzin życia gospodarczego i administracyjnego na poszczególnych rynkach.

EKSPERT RAPORTU

Marta Gocał
Deloitte Legal

Jednym z aspektów bezpieczeństwa cyfrowego jest troska o to, by skutecznie uniemożliwić udostępnianie wrażliwych danych osobom niepowołanym. Najbardziej chyba obrazowymi przypadkami naruszenia tego bezpieczeństwa są kradzieże e-tożsamości.

Tymczasem, jak pokazuje niedawno przeprowadzone przez Deloitte badanie, konsumenci dzielą się ogromem swoich danych, czasami nie znając warunków, na jakich je udostępniają. W ciągu ostatniego roku wzrosła liczba i waga przypadków związanych z naruszeniem prywatności danych.
Można też powiedzieć, że kraje europejskie mają już za sobą okres niemowlęctwa ogólnego rozporządzenia o ochronie danych (General Data Protection Regulation; GDPR). Jednym z głównych celów GDPR jest ułatwienie obywatelom Europy zrozumienia, w jaki sposób wykorzystywane są ich dane.

Świadomość konsumentów co do treści ogólnych warunków korzystania z aplikacji lub urządzeń elektronicznych jest jednak nadal niewielka: Około 80% dorosłych rzadko, jeśli w ogóle, je czyta.

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 Jak przeprowadzić cyfryzację z sukcesem

1. Poznaj swoje dane i procesy – stwórz mapę dokumentów i czynności, które wiążą się z Twoim biznesem. Zidentyfikuj powiązania między nimi.

2. Oszacuj sensytywność zidentyfikowanych danych – elektroniczne procesy dają pewną swobodę w zarządzaniu ryzykiem biznesowym i prawnym. Aby stosować tylko niezbędne środki, trzeba wiedzieć, z jakimi potencjalnymi ryzykami mamy do czynienia w danym przypadku i przed którymi chcemy (potrzebujemy) się zabezpieczyć w najwyższym możliwym stopniu, a z którymi jesteśmy ewentualnie gotowi się pogodzić.

3. Zidentyfikuj wymogi prawne – pamiętaj, że w dużym stopniu zależą one od państwa, któremu będzie podlegać dana relacja (prawo lokalne, ale też z uwzględnieniem prawa domenowego) i branży, w ramach której działasz.

4. Dostosuj swoje umowy – dodaj odpowiednie postanowienia regulujące prawidłowo formę, jaką chcesz stosować dla danych relacji.

5. Uwzględnij potrzeby swojego biznesu i swoich kontrahentów – niekoniecznie wszyscy twoi pracownicy i twoi kontrahenci będą chętni do zmiany przyzwyczajeń, nie wszyscy będą również mieć odpowiednią technologię i kompetencje, żeby dostosować się do cyfrowego modelu współpracy.

6 Przygotuj wewnętrzną politykę e-podpisywania – powinna ona uwzględniać przede wszystkim wyniki wcześniej przeprowadzonej analizy i wskazywać co najmniej:

- które dokumenty i czynności mogą być sporządzane i podpisywane elektronicznie,
- jaka powinna być zachowana forma elektroniczna (z uwzględnieniem zasady, że korzystamy z możliwie najprostszej formy gwarantującej wystarczający poziom bezpieczeństwa i wiarygodności),
- kto powinien być umocowany (i w jakiej formie) do dokonywania danego rodzaju czynności elektronicznych.

EKSPERT RYNKOWY

Artur Miękina,
Asseco Data Systems Polska

Transformacja cyfrowa to przede wszystkim proces, który powinien być odpowiednio zaplanowany, nadzorowany i prowadzony przez kompetentnego lidera. Holistyczne podejście do jego realizacji to poważne wyzwanie, wymagające zmian w różnych obszarach organizacji, dlatego wsparcie na poziomie zarządczym jest niezbędne do powodzenia transformacji.

Usługi zaufania są bardzo pomocne, o ile traktujemy je jako element większej całości – mają one wspierać tworzenie procesów, a nie same te procesy kreować. Dlatego niezmiernie ważne jest patrzenie na transformację poprzez odpowiednią logikę korzyści, która się za nią kryje. Przy takim postrzeganiu i podejściu do tego zagadnienia elementy bezpieczeństwa same zazębiają się o siebie – puzzle muszą trafić na swoje miejsce.

#podpis elektroniczny
#uslugi zaufania
#elektroniczna identyfikcja
#transformacja cyfrowa
#ergonomia usług cyfrowych

OBSERWATORIUM . BIZ

Informacja o poprzednich raportach dotyczących eID i usług zaufania

1. Raport

Biznes bez Papieru – Komercjalizacja eID i usług zaufania w Polsce i Europie

Raport prezentuje mapę polskich dostawców usług elektronicznej identyfikacji oraz usług zaufania, perspektywę europejską – pokazuję, jak ten rynek rośnie za granicą i jaki będzie miał wpływ na Polskę oraz wskazuje potencjał komercjalizacji eID i usług zaufania dla poszczególnych sektorów rynku – finansowego, telekomunikacyjnego, pocztowego i innych. Przedstawia również konieczne kierunki rozwoju narzędzi, takich jak wideoweryfikacja, użycie identyfikacji od dostawców tożsamości, podpis elektroniczny w locie, platformy do podpisywania, walidacje podpisów, elektroniczne doręczenia, aby stały się one narzędziami powszechnie używanymi przez konsumentów i przedsiębiorstwa.

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

2. Raport

Raport eID 2017 – Elektroniczna identyfikacja w Polsce

Badania zrealizowane na potrzeby raportu udowodniły, jak ważne w oczach ekspertów i poszczególnych uczestników rynku, jest zapewnienie systemowego podejścia do rynku eID. Takie aspekty, jak regulacje, bezpieczeństwo, model biznesowy, świadomość użytkowników muszą być właściwie rozpoznane i zaadresowane przez rynek i regulatora, ponieważ równie dobrze mogą stać się katalizatorami, jak i barierami w rozwoju elektronicznej identyfikacji w Polsce

Link do pobrania raportu:
https://obserwatorium.biz/wp-content/uploads/2019/01/RAPORT_eID2017.pdf

3. Raport

Przełom w usługach online. Rozwój usług zaufania w Polsce

Raport został przygotowany w oparciu o analizy rynku polskiego i zagranicznego w zakresie usług zaufania i elektronicznej identyfikacji oraz ich zastosowania w biznesie i administracji publicznej. Cyfrowa rewolucja, której jesteśmy świadkami, będzie mogła przejść na kolejny etap, gdy jako obywatele, klienci i przedsiębiorcy będziemy mogli w sposób wygodny i bezpieczny w pełni realizować transakcje w środowisku elektronicznym. Usługi zaufania, o których mowa w raporcie, mają stać się odpowiedzią na rosnące zapotrzebowanie wszystkich stron potencjalnej „transakcji" na spójne, przewidywalne i uniwersalne ramy organizacyjne i prawne świadczenia takich usług.

Link do pobrania raportu: https://obserwatorium.biz/wpcontent/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf

AUTORZY RAPORTU

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.

PARTNERZY RAPORTU

PATRON GŁÓWNY

EFPE ON-LINE

PARTNERZY

Deloitte. Legal

asseco DATA SYSTEMS

POLSKA 5.0

WYDAWCA RAPORTU

OBSERWATORIUM . BIZ

Metodologia przygotowania raportu

Raport został przygotowany w oparciu o wiedzę partnerów i ekspertów z dziedziny transformacji cyfrowej. Dodatkowo zrealizowano badania ankietowe poprzez kanał elektroniczny oraz wywiady bezpośrednie. Wszystkie badania z wykorzystaniem wymienionych narzędzi badawczych były zrealizowane w okresie sierpień-wrzesień 2020.
W ramach przygotowania raportu zostały przeprowadzone:

1. Analiza otoczenia prawnego / Analiza prawna – na podstawie dostępnych aktów prawnych zostało zweryfikowane tempo zmian w prawie, spowodowanych pandemią, zbadano, czy takie zmiany zaszły oraz czy istniejące prawo było przygotowane na takie okoliczności.
2. Elektroniczne badania ankietowe (CAWI) – badanie przeprowadzone wśród przedsiębiorców i firm deklarujących realizację projektów transformacji cyfrowej; próba objęła 41 respondentów.
3. Wywiady bezpośrednie z kancelariami prawnymi państw europejskich; próba wyniosła 35 respondentów.
4. Badania metodą desk research – metoda, w ramach której katalogowano zmiany produktowe dostawców usług B2C i B2B w zakresie rozwoju elektronicznych kanałów kontaktów i realizacji transakcji z klientem.
5. Analiza rynku – analiza obszaru rozwoju usług elektronicznej identyfikacj oraz usług zaufania. Analiza skupiała się na weryfikacji postępujących zmiany w kontekście zwiększania dostępności tych usług dla szerokiego grona konsumentów i firm.

Źródła

1. Dyrektywa Cyfrowa – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1151 z dnia 20 czerwca 2019 r. zmieniająca dyrektywę (UE) 2017/1132 w odniesieniu do stosowania narzędzi i procesów cyfrowych w prawie spółek.
2. eIDAS – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
3. Kodeks Cywilny – Ustawa z dnia 23 kwietnia 1964 r. (t.j. Dz. U. z 2019 r. poz. 1145 z późn. zm.).
4. Kodeks Postępowania Cywilnego – Ustawa z dnia 17 listopada 1964 r. (t.j. Dz. U. z 2019 r. poz. 1460 z późn. zm.).
5. Kodeks Pracy – Ustawa z dnia 26 czerwca 1974 r. (t.j. Dz. U. z 2020 r. poz. 1320).

6. Kodeks Spółek Handlowych – Ustawa z dnia 15 września 2000 r. (t.j. Dz. U. z 2020 r. poz. 1526).

7. Konwencja Haska – Konwencja znosząca wymóg legalizacji zagranicznych dokumentów urzędowych, sporządzona w Hadze dnia 5 października 1961 r. (Dz. U. z 2005 r. Nr 112, poz. 938).

8. Tarcza antykryzysowa – Ustawa o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw z dnia 31 marca 2020 r. (Dz. U. poz. 568 z późn. zm.).

9. Ustawa federalna o danych osobowych z dnia 27 lipca 2006 r. Nr 152-FZ (Rosja).

10. Ustawa o interpretacji z dnia 20 lipca 1978 r. (Interpretation Act) (Wielka Brytania)

10. Ustawa o Komitecie Wykonawczym 172/1/29.05.2020 (Executive Committee Act) (Grecja).

11. Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz. U. z 2020 r. poz. 1369).

12. Ustawa o podatku od towarów i usług z dnia 11 marca 2004 r. (Dz. U. z 2020 r. poz. 106 z późn. zm.).

13. Ustawa o przeciwdziałaniu praniu pieniędzy (Geldwäschegesetz, GwG) z dn. 25.101993 r. — (niem. Gesetz über Aufspüren von Gewinnen aus schweren Straftaten, BGB l. cz. I, s. 1770.) (Niemcy).

Nota prawna

Opinie zawarte w raporcie wydane zostały na podstawie wiedzy pozyskanej z badania rynku i doświadczenia autorów Raportu. Autorzy nie biorą odpowiedzialności za decyzje podjęte na podstawie opinii wydanych w ramach Raportu „Raport specjalny 2020 – „TRUSTED ECONOMY w nowej rzeczywistości Ograniczanie ryzyka związanego z szybką cyfryzacją". Odniesienia do dostawców rozwiązań elektronicznych są tylko przykładami i nie stanowią rekomendacji.