



ZWIĄZEK  
BANKÓW  
POLSKICH

# Wymiar prawny eID w Polsce

**r.pr. Piotr Brewiński**

Koordynator Zespołu Prawno-Legislacyjny  
Związek Banków Polskich

Józefów, 31 maja 2016 r.



ZWIĄZEK  
BANKÓW  
POLSKICH

## Stan obecny

Podpis elektroniczny

Ochrona danych  
osobowych

Pranie pieniędzy

Informatyzacja  
działalności podmiotów  
realizujących zadania  
publiczne



## Stan obecny

# Podpis elektroniczny

Art. 3 pkt 1) ustawy z dnia 18 września 2001 r. o podpisie elektronicznym:

*podpis elektroniczny* - dane w postaci *elektronicznej*, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej *podpis elektroniczny*

Każda możliwa elektroniczna forma identyfikacji osoby fizycznej, która ujawnia dane personalne np. e-mail

Hasło jednorazowe wraz z innymi danymi przekazywanymi podczas logowania w systemie bankowości elektronicznej

Kod PIN wraz z kartą posiadającą unikatowym numer



## Stan obecny

# Ochrona danych osobowych

**Art. 1. ust. 1** ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Każdy ma prawo do *ochrony* dotyczących go *danych osobowych*

**Art. 23. ust. 1** Przetwarzanie *danych* jest dopuszczalne tylko wtedy, gdy:

- 1) osoba, której *dane* dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej *danych*;
- 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- 3) jest to konieczne do realizacji umowy, gdy osoba, której *dane* dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której *dane* dotyczą;
- 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów *danych* albo odbiorców *danych*, a przetwarzanie nie narusza praw i wolności osoby, której *dane* dotyczą.

Każdej osobie przysługuje prawo do kontroli przetwarzania *danych*, które jej dotyczą



# Stan obecny

## Pranie pieniędzy

**Art. 8b ust. 1 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu**

1. Instytucje obowiązane stosują wobec swoich klientów środki bezpieczeństwa finansowego.

**Art. 8 b ust. 3** Środki bezpieczeństwa finansowego, o których mowa w ust. 1, polegają na:

1) identyfikacji klienta i weryfikacji jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych;

**Art. 9 ust. 1** Identyfikacja, o której mowa w art. 8b ust. 3 pkt 1, obejmuje:

1) w przypadku osób fizycznych i ich przedstawicieli - ustalenie i zapisanie cech dokumentu stwierdzającego na podstawie odrębnych przepisów tożsamość osoby, a także imienia, nazwiska, obywatelstwa oraz adresu osoby dokonującej transakcji, a ponadto numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, lub numeru dokumentu stwierdzającego tożsamość cudzoziemca, lub kodu kraju w przypadku przedstawienia paszportu;



# Stan obecny

## Informatyzacja działalności podmiotów realizujących zadania publiczne

### Art. 20a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

1. Identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty określone w art. 2 następuje przez zastosowanie kwalifikowanego certyfikatu przy zachowaniu zasad przewidzianych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262), lub **profilu zaufanego ePUAP**.
2. Podmiot publiczny, który używa do realizacji zadań publicznych systemów teleinformatycznych, może umożliwiać użytkownikom identyfikację w tym systemie przez zastosowanie innych technologii, chyba że przepisy odrębne przewidują obowiązek dokonania czynności w siedzibie podmiotu publicznego.

Uwierzytelnienie – 500+

PUE ZUS



ZWIĄZEK  
BANKÓW  
POLSKICH

# Co się zmienia

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

Projekt ustawy o usługach zaufania i  
identyfikacji elektronicznej

ROZPORZĄDZENIE PARLAMENTU  
EUROPEJSKIEGO I RADY (UE) NR 2016/679  
z dnia 27 kwietnia 2016 roku w sprawie  
ochrony osób fizycznych w związku z  
przetwarzaniem danych osobowych i w  
sprawie swobodnego przepływu takich  
danych oraz uchylenia dyrektywy  
95/46/WE

DYREKTYWA PARLAMENTU  
EUROPEJSKIEGO I RADY (UE) 2015/2366 z  
dnia 25 listopada 2015 r. w sprawie usług  
płatniczych w ramach rynku  
wewnętrznego, zmieniająca dyrektywy  
2002/65/WE, 2009/110/WE, 2013/36/UE i  
rozporządzenie (UE) nr 093/2010 oraz  
uchylająca dyrektywę 2007/64/WE

Założenia modelu identyfikacji  
elektronicznej  
oraz usług zaufania w Polsce



## Co się zmienia - eIDAS

Jednym z celów rozporządzenia jest zniesienie, przynajmniej w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uwierzytelniania.

Rozporządzenie określa warunki uznawania i akceptowania przez państwa członkowskie środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych zgłoszonym systemem identyfikacji elektronicznej innego państwa członkowskiego. Państwa członkowskie mogą zgłaszać systemy identyfikacji elektronicznej, które akceptują zgodnie ze swoją jurysdykcją w przypadkach, w których identyfikacja elektroniczna jest wymagana na potrzeby usług publicznych. Zgodnie z dodatkowym wymaganie odpowiednie środki identyfikacji elektronicznej muszą być wydawane przez państwo członkowskie zgłaszające system, w jego imieniu lub co najmniej na jego odpowiedzialność.





## Co się zmienia - eIDAS

„identyfikacja elektroniczna” oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą osobę prawną

„uwierzytelnianie” oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej

„podpis elektroniczny” oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis

„pieczęć elektroniczna” oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych



# Co się zmienia

## Projekt ustawy o usługach zaufania i identyfikacji elektronicznej

Celem regulacji zawartych w projekcie ustawy *o usługach zaufania, identyfikacji elektronicznej i zmianie niektórych ustaw* jest wydanie przepisów w odniesieniu do kwestii wskazanych przez eIDAS jako pozostające w kompetencji państw członkowskich oraz dokonanie koniecznych do prawidłowej realizacji rozporządzenia eIDAS zmian w aktach rangi ustawowej.

Kwestie dotyczące nadzoru usług zaufania oraz notyfikacji systemów elektronicznej identyfikacji stanowią najważniejszą treść nowej krajowej regulacji.

Ważną funkcją ustawy jest usunięcie istniejących w krajowych przepisach odwołań do ustawy o podpisie elektronicznym, która zostanie uchylona, dostosowanie terminologii oraz wprowadzenie niezbędnych odwołań do rozporządzenia eIDAS, w tym stworzenie warunków dla zapewnienia zgodności usługodawców z wymaganiami określonymi przez rozporządzenie eIDAS



# Co się zmienia

## Projekt ustawy o usługach zaufania i identyfikacji elektronicznej

Rozporządzenie w zakresie usług zaufania pozostawia w kilku obszarach swobodę dla prawa krajowego

Ustanowienia i notyfikowania nadzoru nad usługami zaufania – minister właściwy ds. informatyzacji

Odpowiedzialność cywilnoprawna dostawców usług zaufania – zasady ogólne Kodeksu cywilnego

Zmiana siatki pojęciowej funkcjonującej w dotychczasowych aktach prawnych

Zastąpienie bezpiecznego podpisu elektronicznego weryfikowanego ważnym certyfikatem przez kwalifikowany podpis elektroniczny oraz znakowanie czasem przez kwalifikowany znacznik czasu



# Co się zmienia

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

**„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

**„dane biometryczne”** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;



# Co się zmienia

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

## Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.



# Co się zmienia

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 093/2010 oraz uchylająca dyrektywę 2007/64/WE

INICJACJA TRANSAKCJI  
PRZEZ PODMIOTY  
TRZECIE (PIS)

**Art. 66**

DOSTĘP DO INFORMACJI  
PRZEZ PODMIOTY  
TRZECIE (AIS)

**Art. 67**

WYDAWANIE  
INSTRUMENTU  
PŁATNICZEGO  
BAZUJĄCEGO NA KARCIE  
PRZEZ PODMIOTY  
TRZECIE (PIIs)

**Art. 65**



# Co się zmienia

## Założenia modelu identyfikacji elektronicznej oraz usług zaufania w Polsce

**Powierzenie państwu roli nadzorcy rynku, a także dostawcy pewnych usług w zakresie eID, ale wyłącznie w zakresie administracji publicznej i sektora finansów publicznych, aby nie naruszać zasad, jakie do chwili obecnej obowiązują.**

**Budowa krajowego węzła administracji publicznej, który pełniłby rolę krajowego pośrednika pomiędzy usługodawcami (usługi online), dostawcami tożsamości (eID), oraz dostawcami atrybutów (rejstry), posiadając jednocześnie dostęp do notyfikowanych środków elektronicznej identyfikacji z całego obszaru UE.**

**Utworzenie krajowego rejestru krajowych środków/systemów identyfikacji elektronicznej.**

**Wprowadzenie rekomendacji dla stosowania identyfikacji elektronicznej na poziomie średnim dla większości usług administracji publicznej. Umożliwienie skorzystania z e-usługi (w celu innym, niż tylko informacyjny) posiadaczowi środka identyfikacji elektronicznej powinno być oparte o dodatkowe zabezpieczenie – **jednorazowy kod dostępu do usługi lub sesji**, które może być realizowane w różny sposób – np. poprzez potwierdzenie za pomocą jednorazowego kodu przesłanego SMS-em na numer telefonu przypisany do danego użytkownika.**



# Co się zmienia

## Założenia modelu identyfikacji elektronicznej oraz usług zaufania w Polsce

**Szerokie wykorzystanie zaawansowanej pieczęci elektronicznej przez administrację publiczną do zabezpieczania wszystkich dokumentów pochodzących z urzędów.**

**Wprowadzenie i umocowanie prawne ujednoliczonego, spójnego, niesprzecznego wewnątrznie słownika pojęć prawnych i technicznych, stanowiącego podstawę interpretacji przepisów prawa w zakresie identyfikacji elektronicznej i usługi zaufania.** W chwili obecnej można wskazać istnienie niespójności utrudniających lub nawet uniemożliwiających wprowadzanie e-usług opartych o eID lub o wiarygodne dokumenty elektroniczne. Pojęciem negatywnie wpływającym na stosowalność e-usług jest „pisemność”, mająca w różnych przepisach prawa różne definicje oraz sformułowania z wykorzystaniem alternatyw „pisemnie lub w postaci elektronicznej, „w formie pisemnej lub w formie dokumentu elektronicznego” itd. Umocowanie w 2016 r. w przepisach prawa cywilnego „formy pisemnej”, „formy elektronicznej” i „formy dokumentowej” jak również definicji dokumentu niewystarczająco rozwiązuje te problemy.

**Ustanowienie rozdzielności certyfikatów kwalifikowanych służących do podpisywania i do identyfikacji** (czym innym jest wyrażenie woli, czym innym wiarygodne „przedstawienie się” systemowi).

**Zapewnienie uznawania wizualizacji dokumentu elektronicznego w postępowaniu przed urzędami i sądami jako równorzędnej dokumentowi elektronicznemu**, na podstawie którego została wytworzona, o ile źródłowy dokument elektroniczny jest udostępniany w systemie teleinformatycznym urzędu lub sądu i treść wizualizowana może być zweryfikowana.





# Co się zmienia

## Założenia modelu identyfikacji elektronicznej oraz usług zaufania w Polsce

**Wykorzystanie komercyjnych usług zaufania**, jednak szerokie wykorzystanie takich usług powinno dotyczyć nie tylko podmiotów publicznych i powinno obejmować:

- **wykorzystanie pieczęci elektronicznej i usług konserwacji elektronicznej** dla celów pełnej elektronizacji procesów – nawet w przypadku gdy w ramach ich realizacji występują dokumenty nieelektroniczne,
- **umocowanie kwalifikowanych usług rejestrowanego doręczania elektronicznego** jako zastępujących całkowicie doręczenia na papierze;
- **ustalenie nowych zasad działania elektronicznych skrzynek podawczych (ESP):**
- **umocowanie usługi kwalifikowanej walidacji kwalifikowanego podpisu elektronicznego** jako zaświadczenia o znaczeniu takim jak poświadczenie notarialne.



ZWIĄZEK  
BANKÓW  
POLSKICH

Dziękuję za uwagę.

