Uchwała Nr 20 / 2018
Zarządu Narodowego Banku Polskiego
z dnia 25 maja 2018 r.

zmieniająca uchwałę w sprawie wprowadzenia „Regulaminu uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością"

Na podstawie art. 7 ust. 2 pkt 2 i art. 17 ust. 4 pkt 9 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2017 r. poz. 1373) uchwala się, co następuje:

§ 1. W uchwale nr 65/2016 Zarządu Narodowego Banku Polskiego z dnia 24 listopada 2016 r. w sprawie wprowadzenia „Regulaminu uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością" załącznik do uchwały otrzymuje brzmienie określone w załączniku do niniejszej uchwały.

§ 2. Regulamin, w brzmieniu nadanym niniejszą uchwałą, jest udostępniany w dniu podjęcia uchwały na stronie internetowej www.nbp.pl/azu.

§ 3. Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Zarządu
Narodowego Banku Polskiego

Adam Glapiński

Załącznik do uchwały nr 20/2018
Zarządu Narodowego Banku Polskiego
z dnia 25 maja 2018 r.

Regulamin uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością

DZIAŁ I
Postanowienia ogólne

§ 1. Regulamin uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością, zwany dalej „Regulaminem", określa zasady postępowania dotyczące uwierzytelniania i autoryzacji klientów Narodowego Banku Polskiego w systemach informatycznych i zarządzania rolami w tych systemach z wykorzystaniem Zintegrowanego Systemu Zarządzania Tożsamością, zwanego dalej „systemem ZSZT".

§ 2. Użyte w Regulaminie określenia oznaczają:

1) Administrator Uprawnień Instytucji (AUI) – osoba uprawniona przez daną instytucję do zarządzania kontami i uprawnieniami użytkowników instytucji w systemach informatycznych oraz do wnioskowania o certyfikaty w ramach funkcjonalności aplikacji AZU;
2) autoryzacja – proces polegający na potwierdzeniu, czy użytkownik jest uprawniony do uzyskania dostępu do żądanego zasobu w systemie informatycznym;
3) Aplikacja Zarządzania Uprawnieniami (AZU) – aplikacja w ramach systemu ZSZT umożliwiająca zarządzanie prawami dostępu do systemów informatycznych;
4) certyfikat – certyfikat klucza publicznego stanowiący elektroniczne zaświadczenie, za pomocą którego klucz publiczny jest przyporządkowany do użytkownika lub instytucji, umożliwiający ich jednoznaczną identyfikację;
5) dezaktywacja - blokada konta użytkownika w systemie ZSZT połączona z usunięciem posiadanych uprawnień (przynależności do ról) w systemach informatycznych NBP i przeniesienie konta nieaktywnego do archiwum;
6) delegowanie roli – przydzielenie przez gestora systemu informatycznego uprawnień dla instytucji do samodzielnego zarządzania rolami w danym systemie informatycznym przez wyznaczonych AUI;
7) gestor – departament Narodowego Banku Polskiego odpowiedzialny za weryfikację formalną i nadzór merytoryczny nad wskazanym we wniosku systemem informatycznym;

8) instytucja – klient niebędący osobą fizyczną, korzystający z systemów informatycznych w NBP na podstawie umowy lub obowiązującego prawa, który ma założone konto w systemie ZSZT;
9) ID Card – unikalny identyfikator z dokumentu tożsamości ze zdjęciem osoby fizycznej, w którym nie występuje numer PESEL;
10) identyfikator sprawozdawczy – unikalny wyróżnik stosowany w systemach sprawozdawczych Narodowego Banku Polskiego oraz w Internetowej Bazie Ewidencji Numerów Instytucji Finansowych EWIB;
11) klient – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której ustawa przyznaje zdolność prawną, która na mocy umowy lub obowiązującego prawa korzysta z systemu informatycznego;
12) konto – zbiór zasobów i uprawnień (ról) w ramach systemu ZSZT, przypisanych użytkownikowi, posiadający unikalną nazwę logowania (login) i hasło, pozwalający na dostęp do zaawansowanych funkcji w systemach informatycznych;
13) NBP – Narodowy Bank Polski z siedzibą: przy ul. Świętokrzyskiej 11/21, 00-919 Warszawa;
14) RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyleniem dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);
15) umowa – umowa zawarta pomiędzy klientem a NBP lub akt prawny, na podstawie którego NBP świadczy dla klienta usługi uwierzytelniania użytkowników w danym systemie informatycznym, przy wykorzystaniu systemu ZSZT;
16) uwierzytelnienie – proces polegający na potwierdzeniu zadeklarowanej tożsamości użytkownika;
17) użytkownik – osoba upoważniona przez klienta do korzystania z systemu informatycznego , która została zarejestrowana i posiada konto w systemie ZSZT;
18) wniosek – dokument w formie papierowej lub elektronicznej, który po akceptacji przez gestora jest podstawą do zarządzania kontami i uprawnieniami w systemie informatycznym.

§ 3. 1. System ZSZT służy do:
1) zapewnienia jednolitego dostępu do systemów informatycznych;
2) zapewnienia pojedynczego punktu logowania dla użytkowników systemów informatycznych, przy zachowaniu restrykcyjnych, jednolitych i scentralizowanych zasad bezpieczeństwa;
3) zarządzania uprawnieniami użytkowników w systemach informatycznych;
4) zapewnienia jednolitego systemu uwierzytelniania i autoryzacji użytkowników systemów informatycznych;

5) monitorowania zgodności posiadanych przez użytkowników uprawnień z założeniami regulacji i polityk bezpieczeństwa w NBP;
6) centralnego zarządzania zbiorem danych osobowych użytkowników systemów informatycznych.

2. Usługi uwierzytelniania użytkowników w systemie ZSZT nie są usługami publicznymi. Podmioty, które podpisały umowę z NBP lub które z mocy obowiązującego prawa są zobowiązane do korzystania co najmniej z jednego systemu informatycznego, mogą wystąpić o założenie kont i nadanie uprawnień w ramach systemu ZSZT.
3. Użytkownikom zakłada się unikalne konta w celu nadania uprawnień w systemie informatycznym.
4. Instytucjom zakłada się unikalne konta w celu wystawienia certyfikatu niezbędnego do korzystania z systemów informatycznych przez użytkowników instytucji, zgodnie z wymaganiami i na zasadach określonych przez gestora danego systemu informatycznego. Certyfikat wydany przez NBP dla instytucji może być wykorzystywany do uwierzytelniania użytkowników danej instytucji w wielu systemach informatycznych.
5. Prawidłowe działanie systemu ZSZT jest zagwarantowane dla użytkowników korzystających z przeglądarek internetowych, realizujących specyfikację HTML5, zgodnie z wymaganiami technicznymi dostępnymi pod adresem: http://www.nbp.pl/azu/ .

DZIAŁ II
Zasady zarządzania uprawnieniami dostępu do systemów informatycznych
Rozdział 1
Rejestracja i zarządzanie uprawnieniami

§ 4. 1. Zarządzanie uprawnieniami dostępu użytkowników do systemów informatycznych jest realizowane przy wykorzystaniu AZU, dostępnej pod adresem: https://azu.nbp.pl.

2. Regulamin, formularze wniosków, wymagania techniczne i instrukcje dla użytkowników AZU są dostępne pod adresem www.nbp.pl/azu.
3. Warunkiem korzystania z AZU jest złożenie wniosku, w wyniku którego po akceptacji przez gestora nastąpi założenie, aktywacja konta, nadanie uprawnień i wydanie certyfikatów, zgodnie z wymaganiami i na zasadach określonych przez gestora systemu informatycznego wskazanego we wniosku.
4. NBP zarządza kontami i uprawnieniami użytkowników w systemach informatycznych, z zastrzeżeniem ust. 7.
5. Konto instytucji w systemie informatycznym jest zakładane na podstawie wniosku o założenie konta instytucji w systemie informatycznym, którego wzór określa załącznik nr 1 do Regulaminu.

6. Z zastrzeżeniem ust. 7 i 8, założenie, aktywacja konta użytkownika, przedłużenie ważności konta oraz nadanie uprawnień dla użytkownika w systemie informatycznym są realizowane przez NBP na podstawie wniosku o założenie, aktywację, przedłużenie ważności lub nadanie uprawnień dla konta użytkownika w systemie informatycznym, którego wzór określa załącznik nr 2 do Regulaminu.
7. Instytucja może wystąpić do gestora z wnioskiem o wyznaczenie AUI w Zintegrowanym Systemie Zarządzania Tożsamością na potrzeby wskazanego we wniosku systemu informatycznego. Po nadaniu przez NBP uprawnienia dla AUI i pierwszej autoryzacji AUI w AZU, instytucja przejmie odpowiedzialność za zarządzanie kontami i uprawnieniami użytkowników instytucji oraz za działania AUI we wszystkich systemach informatycznych udostępnionych instytucji przez NBP w ramach Zintegrowanego Systemu Zarządzania Tożsamością. Wzór wniosku o wyznaczenie Administratora Uprawnień Instytucji w Zintegrowanym Systemie Zarządzania Tożsamością określa załącznik nr 3 do Regulaminu.
8. Upoważniony przez instytucję AUI, po nadaniu uprawnień na podstawie wniosku, którego wzór określa załącznik nr 3 do Regulaminu, może w AZU wykonywać samodzielnie następujące czynności:
    1) wyświetlać i modyfikować dane teleadresowe instytucji;
    2) wystawiać w AZU wnioski elektroniczne o założenie kont dla nowych użytkowników instytucji na potrzeby wskazanego systemu informatycznego, które będą przekazane do weryfikacji i akceptacji gestora tego systemu;
    3) wystawiać w AZU wnioski elektroniczne o aktywację lub przedłużenie terminu ważności kont użytkowników instytucji;
    4) wystawiać w AZU wnioski elektroniczne o dezaktywację kont użytkowników instytucji;
    5) nadawać i wycofywać uprawnienia (role) użytkownikom instytucji we wskazanym we wniosku systemie informatycznym, zgodnie z wymaganiami i na zasadach określonych przez gestora tego systemu;
    6) weryfikować uprawnienia użytkowników instytucji w delegowanych dla instytucji rolach w systemach informatycznych;
    7) wystawiać w AZU wnioski elektroniczne o wygenerowanie nowych certyfikatów na potrzeby wskazanego systemu informatycznego, które będą przekazane do weryfikacji i akceptacji gestora tego systemu;
    8) wystawić w AZU wniosek elektroniczny o dezaktywację konta instytucji i unieważnienie certyfikatu instytucji;
    9) wygenerować raport z aktywności użytkowników instytucji w AZU lub zapisać go do pliku.
9. Delegowanie roli do zarządzania przez instytucję uprawnieniami lub nadanie uprawnień dla konta instytucji we wskazanym we wniosku systemie informatycznym jest realizowane na podstawie wniosku, którego wzór określa załącznik nr 1 do Regulaminu.

10. Wycofanie uprawnień dla AUI przez instytucję jest realizowane przez NBP bez zbędnej zwłoki natychmiast po przetworzeniu wniosku o wycofanie uprawnień w Zintegrowanym Systemie Zarządzania Tożsamością dla Administratora Uprawnień Instytucji, którego wzór określa załącznik nr 4 do Regulaminu.
11. Z zastrzeżeniem ust. 7 i 8, wycofanie uprawnień dla użytkownika systemu informatycznego jest realizowane na podstawie wniosku o wycofanie uprawnień dla konta użytkownika w systemie informatycznym, którego wzór określa załącznik nr 5 do Regulaminu.
12. Wycofanie uprawnień dla konta instytucji lub delegowania roli do zarządzania przez instytucję uprawnieniami we wskazanym we wniosku systemie informatycznym jest realizowane na podstawie wniosku, którego wzór określa załącznik nr 6 do Regulaminu.
13. W przypadku całkowitej rezygnacji z funkcji AUI przez instytucję, NBP po weryfikacji i akceptacji przez gestora systemu informatycznego przejmie wykonywanie czynności zarządzania uprawnieniami użytkowników instytucji w systemie informatycznym, o których mowa w ust. 8.
14. Warunkiem dostępu do AZU jest weryfikacja poprawności i ważności certyfikatu instytucji oraz uwierzytelnienie użytkownika indywidualnym loginem i unikalnym hasłem. Przy pierwszym zalogowaniu wymagana jest akceptacja w AZU niniejszego Regulaminu oraz Polityki Prywatności NBP przez każdego użytkownika, co stanowi także potwierdzenie realizacji obowiązku informacyjnego, o którym mowa w art. 14 RODO. Brak akceptacji Regulaminu przez użytkownika skutkuje brakiem aktywacji konta oraz nie przypisaniem uprawnień do systemu informatycznego NBP, wskazanego we wniosku przez instytucję.

Rozdział 2
Konto Użytkownika

§ 5. 1. Konto użytkownika zawiera dane podane we wniosku o założenie konta użytkownika w systemie informatycznym.
2. W przypadku zapomnienia hasła, użytkownik może zwrócić się do wsparcia serwisowego NBP HelpDesk o zmianę hasła i odblokowanie konta przy wykorzystaniu AZU.
3. NBP zapewnia dla użytkowników wsparcie serwisowe w zakresie zarządzania tożsamością dostępne:
    a) drogą telefoniczną: **+48 801 111 000** całodobowo, z wyłączeniem przerwy od godz. 7.00 w sobotę do godz. 19.00 w niedzielę.
    b) drogą mailową: **helpdesk@nbp.pl**.
4. NBP zastrzega sobie prawo do zablokowania konta użytkownika, który łamie postanowienia Regulaminu lub którego działania zostaną uznane przez NBP za szkodliwe dla systemu informatycznego.
5. Użytkownik, którego konto zostało zablokowane przez NBP nie może ponownie aktywować konta bez uprzedniej zgody NBP. Ponowna aktywacja konta dla użytkownika systemu informatycznego jest realizowana na podstawie wniosku

o aktywację konta użytkownika w systemie informatycznym, o którym mowa w § 4 ust. 6.

DZIAŁ III
Ochrona danych osobowych

§ 6.1. Dane osobowe użytkowników systemu ZSZT są przetwarzane przez NBP na podstawie art. 6 ust. 1 lit. b i c RODO.

2. Źródłem danych osobowych użytkownika jest wniosek instytucji, o którym mowa w § 4 ust. 3.
3. NBP przetwarza następujące kategorie danych osobowych:: imię, nazwisko, kraj, numer PESEL lub ID Card, numer dowodu tożsamości ze zdjęciem, nazwa i dane teleadresowe instytucji, którą reprezentuje użytkownik, wizerunek elektroniczny, numer telefonu, fax, adres poczty elektronicznej, hasło do identyfikacji telefonicznej użytkownika, podpis, rodzaj certyfikatu.
4. Z chwilą udostępnienia danych osobowych przez instytucję, administratorem tych danych staje się Narodowy Bank Polski z siedzibą w Warszawie przy ul. Świętokrzyskiej 11/21.
5. Dane inspektora ochrony danych w Narodowym Banku Polskim są publikowane na stronie www.nbp.pl/RODO.
6. NBP przetwarza dane osobowe w systemie ZSZT w celu uwierzytelniania i autoryzacji użytkownika w systemach informatycznych NBP, zintegrowanych z systemem ZSZT.
7. Dane osobowe użytkownika są przechowywane w systemie ZSZT przez okres 10 lat od daty wycofania jego uprawnień do ostatniego systemu informatycznego NBP, zintegrowanego z ZSZT, chyba, że przepisy prawa stanowią inaczej.
8. Dane osobowe nie będą przekazywane do innego państwa (poza terytorium Rzeczypospolitej Polskiej) lub do organizacji międzynarodowej w rozumieniu art. 4 ust. 26 RODO.
9. Dostęp do danych osobowych udostępnionych NBP posiadają wyłącznie osoby upoważnione do przetwarzania tych danych na zasadach obowiązujących w NBP.
10. NBP zobowiązuje osoby, o których mowa w ust. 9, do zachowania poufności udostępnionych danych osobowych; osoby takie mogą podlegać także ustawowemu obowiązkowi zachowania tajemnicy, stosownie do art. 28 ust. 3 lit. b RODO.
11. Osobom, których dane osobowe zostały udostępnione NBP, przysługuje prawo żądania od NBP, jako ich administratora, dostępu do danych osobowych, sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do przenoszenia danych.
12. Osobom, o których mowa w ust. 11 przysługuje możliwość wniesienia skargi do organu nadzorczego, którym jest : Prezes Urzędu Ochrony Danych Osobowych z siedzibą przy ul. Stawki 2, 00-193 Warszawa.
13. Przetwarzane dane osobowe nie będą wykorzystywane przez NBP do podejmowania zautomatyzowanych decyzji w indywidualnych przypadkach, w tym do profilowania.
14. Realizacja praw osób, o których mowa w ust. 11, z wyłączeniem prawa dostępu do swoich danych osobowych, jest realizowana za pośrednictwem instytucji.

DZIAŁ IV
Certyfikaty

§ 7. Zasady świadczenia przez NBP usług zaufania, w szczególności zasady wystawiania i odbioru certyfikatów dla użytkowników dla potrzeb uwierzytelniania i autoryzacji w systemach informatycznych, zawiera dokument „System DOCert – Polityka certyfikacji dla certyfikatów użytkowych", dostępny na stronie internetowej www.docert.nbp.pl .

Załączniki do Regulaminu

WZÓR

Załącznik nr 1

.....

(miejscowość i data wystawienia

Wniosek o założenie konta/ nadanie uprawnień/ delegowanie roli do zarządzania uprawnieniami[1] dla instytucji

w Zintegrowanym Systemie Zarządzania Tożsamością

na potrzeby systemu informatycznego

.....

(nazwa systemu informatycznego)

Zgodnie z .....

(nazwa umowy lub aktu prawnego)

z dnia.....

1. Dane instytucji:	
Nazwa instytucji	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
Identyfikator instytucji (dla Polski NIP)	
REGON[1]	
Identyfikator sprawozdawczy w NBP[2]	
E-mail	
Telefon 1	
Telefon 2	
Fax	

Certyfikat instytucji	TAK ☐ NIE ☐
Nazwa oddziału okręgowego Narodowego Banku Polskiego [3]	
2. Dane osoby upoważnionej do odbioru certyfikatu dla instytucji[3]	
Imię	
Nazwisko	
Numer dokumentu tożsamości ze zdjęciem	
Numer telefonu do kontaktu w sprawie odbioru certyfikatu	
3. Deklaracja użytkowania	
Oświadczamy, że zobowiązaliśmy użytkowników korzystających z certyfikatu instytucji do zapoznania się z Regulaminem uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością i Polityką Prywatności Narodowego Banku Polskiego, umieszczonych na stronie www.nbp.pl/azu oraz poinformowaliśmy ich, że akceptacja tych dokumentów jest warunkiem koniecznym do korzystania z systemów informatycznych. Oświadczamy, że został spełniony obowiązek informacyjny wobec osoby uprawnionej do odbioru certyfikatu dla instytucji wynikający z przetwarzania jej danych osobowych przez NBP.	
..... (pieczęć firmowa i podpisy osób uprawnionych do złożenia wniosku w systemie informatycznym)	

[1] Niepotrzebne skreślić.

[2] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

[3] Wypełnić w celu wskazania miejsca odbioru certyfikatu, jeśli w polu certyfikat zaznaczono „TAK".

Uwaga! Upoważniony pracownik instytucji może osobiście odebrać wygenerowany dla instytucji certyfikat we wskazanym oddziale okręgowym NBP.

WZÓR

Załącznik nr 2

.....

(miejscowość i data wystawienia)

Wniosek o założenie/aktywowanie/przedłużenie ważności /nadanie uprawnień dla[1] konta użytkownika

w systemie informatycznym

.....

(nazwa systemu informatycznego NBP)

Zgodnie z .....

(nazwa Umowy lub aktu prawnego)

z dnia.....

1. Dane instytucji:	
Nazwa instytucji	
Identyfikator instytucji (dla Polski NIP)	
REGON[1]	
Identyfikator sprawozdawczy w NBP[2]	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
2. Dane użytkownika systemu	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1])	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Założenie/Aktywowanie[1]) konta	TAK □ NIE □
Nadanie uprawnień w systemie informatycznym[1])	..... Nazwa uprawnienia

Nadanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Data ważności konta	
3. Dane użytkownika systemu[1)]	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)])	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Założenie/Aktywowanie [1)] konta	TAK □ NIE □
Nadanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Nadanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Data ważności konta	
4. Dane użytkownika systemu[1)]	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)])	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Założenie/Aktywowanie konta [1)]	TAK □ NIE □
Nadanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Nadanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Data ważności konta	
5. Deklaracja użytkowania	

Oświadczamy, że zobowiązaliśmy wskazanych we wniosku użytkowników do zapoznania się z Regulaminem uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością i Polityką Prywatności Narodowego Banku Polskiego, umieszczonych na stronie http://www.nbp.pl/azu oraz poinformowaliśmy ich, że akceptacja tych dokumentów jest warunkiem koniecznym do korzystania z systemów informatycznych.
..... (pieczęć firmowa i podpisy osób uprawnionych do złożenia wniosku)

[1] Niepotrzebne skreślić.

[2] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

[3] Wypełnić w celu wskazania miejsca odbioru certyfikatu, jeśli w polu certyfikat zaznaczono „TAK".

Uwaga! Zgłoszeni użytkownicy będą osobiście odbierali wygenerowane dla nich certyfikaty we wskazanym oddziale okręgowym NBP.

WZÓR

Załącznik nr 3

.....

(miejscowość i data wystawienia)

Wniosek o wyznaczenie

Administratora Uprawnień Instytucji w Zintegrowanym Systemie Zarządzania Tożsamością

na potrzeby systemu informatycznego.....

(nazwa systemu informatycznego)

Zgodnie z .....

(nazwa Umowy lub aktu prawnego)

z dnia.....

1. Dane instytucji:	
Nazwa instytucji	
Identyfikator instytucji (dla Polski NIP)	
REGON[1)]	
Identyfikator sprawozdawczy w NBP[2)]	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
2. Dane AUI	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)]	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Uprawnienia w AZU	Administrator Uprawnień Instytucji
3. Dane AUI [1)]	
Imię	
Nazwisko	
Kraj	

ID (Pesel/ID Card[1)])	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Uprawnienia w AZU	Administrator Uprawnień Instytucji
4. Dane AUI [1)]	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)])	
E-mail	
Telefon 1	
Telefon 2	
Fax	
Uprawnienia w AZU	Administrator Uprawnień Instytucji
5. Deklaracja użytkowania	
Oświadczamy, że zobowiązaliśmy wskazanych we wniosku Administratorów Uprawnień Instytucji do zapoznania się z Regulaminem uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością i Polityką Prywatności Narodowego Banku Polskiego, umieszczonych na stronie www.nbp.pl/azu oraz poinformowaliśmy ich, że akceptacja tych dokumentów jest warunkiem koniecznym do korzystania z systemów informatycznych NBP. **Oświadczamy, że z chwilą delegowania przez NBP uprawnień dla AUI przejmujemy odpowiedzialność za konta, uprawnienia i działania użytkowników w systemach informatycznych udostępnionych naszej instytucji przez NBP w ramach Zintegrowanego Systemu Zarządzania Tożsamością.**	
..... (pieczęć firmowa i podpisy osób uprawnionych do złożenia wniosku)	

[1)] Niepotrzebne skreślić.

[2)] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

WZÓR

Załącznik nr 4

.....

(miejscowość i data wystawienia)

Wniosek o wycofanie uprawnień w Zintegrowanym Systemie Zarządzania Tożsamością

dla Administratora Uprawnień Instytucji

1. Dane instytucji:	
Nazwa instytucji	
Identyfikator instytucji (dla Polski NIP)	
REGON[1)]	
Identyfikator sprawozdawczy w NBP[2)]	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
2. Dane użytkownika systemu	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)])	

3. Sposób wycofania uprawnień	
Dezaktywacja konta użytkownika	☐
Wycofanie uprawnień AUI	☐
Data wystawienia:	Pieczęć firmowa instytucji i podpisy osób uprawnionych do złożenia wniosku .....

[1)] Niepotrzebne skreślić.

[2)] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

WZÓR

Załącznik nr 5

.....

(miejscowość i data wystawienia)

Wniosek o wycofanie uprawnień dla konta użytkownika

w systemie informatycznym

.....

(nazwa systemu informatycznego)

Zgodnie z .....

(nazwa Umowy lub aktu prawnego)

z dnia.....

I. Dane instytucji:	
Nazwa instytucji	
Identyfikator instytucji (dla Polski NIP)	
REGON[1)]	
Identyfikator sprawozdawczy w NBP[2)]	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
II. Dane użytkownika systemu	
Imię	
Nazwisko	
Kraj	
ID (Pesel/ID Card[1)])	
E-mail	
Telefon 1	
Telefon 2	

Wycofanie uprawnień w systemie informatycznym	..... Nazwa uprawnienia
Wycofanie uprawnień w systemie informatycznym[1)]	..... Nazwa uprawnienia
Dezaktywacja konta	TAK ☐ NIE ☐
	..... (pieczęć firmowa i podpisy osób uprawnionych do złożenia wniosku)

[1)] Niepotrzebne skreślić.

[2)] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

WZÓR

Załącznik nr 6

.....

(miejscowość i data wystawienia)

Wniosek o wycofanie uprawnienia/ delegowania roli do zarządzania uprawnieniami[1] instytucji w systemie informatycznym

.....

(nazwa systemu informatycznego)

Zgodnie z .....

(nazwa Umowy lub aktu prawnego)

z dnia.....

I. Dane instytucji:	
Nazwa instytucji	
Identyfikator instytucji (dla Polski NIP)	
REGON[1]	
Identyfikator sprawozdawczy w NBP[2]	
Ulica	
Kod pocztowy	
Miejscowość	
Kraj	
Wycofanie uprawnienia dla konta instytucji[1]	..... Nazwa uprawnienia
Wycofanie delegacji do zarządzania uprawnieniami przez instytucję	TAK □ NIE □
Dezaktywacja konta	TAK □ NIE □
Unieważnienie Certyfikatu	TAK □ NIE □

.....

(pieczęć firmowa i podpisy osób uprawnionych do złożenia wniosku)

[1] Niepotrzebne skreślić.

[2] Pole opcjonalne wypełniane dla potrzeb systemów sprawozdawczych.

[3] Wypełnić w celu wskazania miejsca zwrotu karty z certyfikatem, jeśli w polu „unieważnienie certyfikatu" zaznaczono „TAK".

Uwaga! Upoważniony pracownik instytucji może zwrócić kartę użytkownika z certyfikatem we wskazanym oddziale okręgowym NBP.

Uzasadnienie

Celem projektowanej uchwały jest wprowadzenie aktualizacji „Regulaminu uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością, stanowiącego załącznik do uchwały nr 65/2016 Zarządu Narodowego Banku Polskiego z dnia 24 listopada 2016 roku", zwanym dalej Regulaminem, w następującym zakresie:

1. Zmiana klauzuli w Dziale III Regulaminu, dotyczącej ochrony danych osobowych na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119/1 z 04. 05. 2016 r.), w uzgodnieniu z Administratorem Bezpieczeństwa Informacji w Narodowym Banku Polskim;
2. Uzupełnienie i rozszerzenie zapisów w Regulaminie w związku z rozbudową funkcjonalności Aplikacji Zarzadzania Użytkownikami (AZU) w ramach Zintegrowanego Systemu Zarządzania Tożsamością.

Projektowana uchwała nie powoduje skutków finansowych dla NBP oraz nie wymaga konsultacji z EBC.