WYTYCZNE

WYTYCZNE EUROPEJSKIEGO BANKU CENTRALNEGO (UE) 2021/1759

z dnia 20 lipca 2021 r.

zmieniające wytyczne EBC/2012/27 w sprawie transeuropejskiego zautomatyzowanego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2) (EBC/2021/30)

RADA PREZESÓW EUROPEJSKIEGO BANKU CENTRALNEGO,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności art. 127 ust. 2 tiret pierwsze i czwarte,

uwzględniając Statut Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego, w szczególności art. 3 ust. 1 oraz art. 17, 18 i 22,

a także mając na uwadze, co następuje:

(1) W dniu 26 kwietnia 2007 r. Rada Prezesów Europejskiego Banku Centralnego przyjęła wytyczne EBC/2007/2 ([1]) regulujące działanie systemu TARGET2, który ustanawia pojedynczą platformę techniczną – jednolitą wspólną platformą (Single Shared Platform, SSP). Wytyczne te zostały przekształcone w 2012 r. jako wytyczne Europejskiego Banku Centralnego EBC/2012/27 ([2]).

(2) W celu zapewnienia skuteczności wprowadzanych regulacji konieczne jest doprecyzowanie, że posiadacze rachunków TIPS DCA i posiadacze rachunków T2S DCA będą podłączeni do TARGET2 za pośrednictwem jednolitego punku dostępu do infrastruktur rynkowych Eurosystemu odpowiednio od listopada 2021 r. i czerwca 2022 r.

(3) Aby zapewnić dalszy rozwój systemu TARGET2 w odpowiedzi na zagrożenia dla bezpieczeństwa cybernetycznego, należy doprecyzować i poszerzyć zasady dotyczące przestrzegania wymogów TARGET2 w zakresie ochrony punktów końcowych (endpoint security). Ponadto w celu zapewnienia kompleksowości i zharmonizowania ram prawnych należy dokonać zmian definicji.

(4) Aby zapewnić dostępność płatności natychmiastowych w całej Unii, posiadacze rachunków w PM, ich uczestnicy pośredni i adresowalni posiadacze BIC, którzy przystąpili do schematu SCT Inst poprzez podpisanie porozumienia o zachowaniu zgodności ze schematem polecenia przelewu natychmiastowego SEPA, powinni być stale osiągalni w ramach platformy TIPS za pośrednictwem rachunku TIPS DCA. Na platformie TIPS powinny być świadczone usługi przelewu środków pieniężnych w pieniądzu banku centralnego na potrzeby systemów zewnętrznych dokonujących rozrachunku płatności natychmiastowych we własnych księgach.

(5) Po uruchomieniu Projektu Konsolidacja T2-T2S konieczne będzie zachowanie przejrzystości w zakresie sposobów przenoszenia sald z rachunków uczestników w TARGET2 na odpowiednie rachunki w przyszłym systemie TARGET, tak aby zapewnić pewność prawną.

(6) W celu zapewnienia skutecznego stosowania wytycznych EBC/2012/27 konieczne jest również doprecyzowanie i zaktualizowanie innych ich postanowień.

(7) Wdrożenie Projektu Konsolidacja T2-T2S będzie również wymagało zmian obowiązujących zasad dotyczących umów zawartych z dostawcami usług sieciowych T2S, które powinny mieć zastosowanie od 13 czerwca 2022 r.

(8) Wytyczne EBC/2012/27 powinny zatem zostać odpowiednio zmienione,

([1]) Wytyczne Europejskiego Banku Centralnego EBC/2007/2 z dnia 26 kwietnia 2007 r. w sprawie transeuropejskiego zautomatyzowanego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2) (Dz.U. L 237 z 8.9.2007, s. 1).

([2]) Wytyczne Europejskiego Banku Centralnego EBC/2012/27 z dnia 5 grudnia 2012 r. w sprawie transeuropejskiego zautomatyzowanego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2) (Dz.U. L 30 z 30.1.2013, s. 1).

PRZYJMUJE NINIEJSZE WYTYCZNE:

Artykuł 1

Zmiany

W wytycznych EBC/2012/27 wprowadza się następujące zmiany:

1) w art. 1 ust. 1 otrzymuje brzmienie:

„1. TARGET2 umożliwia rozrachunek brutto w czasie rzeczywistym płatności w euro, przeprowadzany w pieniądzu banku centralnego na rachunkach w PM, rachunkach T2S DCA i rachunkach TIPS DCA. TARGET2 został stworzony i funkcjonuje w oparciu o SSP, za pośrednictwem której na tych samych zasadach technicznych następuje składanie i przetwarzanie zleceń płatniczych oraz otrzymywanie płatności. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków T2S DCA, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę T2S. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków TIPS DCA i rachunków technicznych TIPS AS, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę TIPS.";

2) w art. 2 wprowadza się następujące zmiany:

a) skreśla się pkt 58;

b) pkt 62 otrzymuje brzmienie:

„62) »zlecenie płatnicze« (payment order) – polecenie przelewu, zlecenie przekazania płynności, instrukcję polecenia zapłaty, zlecenie przekazania płynności z PM do T2S DCA, zlecenie przekazania płynności z T2S DCA do PM, zlecenie przekazania płynności z T2S DCA do T2S DCA, zlecenie przekazania płynności z PM do TIPS DCA, zlecenie przekazania płynności z TIPS DCA do PM, zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA, zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS, zlecenie płatnicze dotyczące płatności natychmiastowej lub pozytywną odpowiedź na żądanie zwrotu płatności;";

c) skreśla się pkt 78;

d) pkt 81 otrzymuje brzmienie:

„81) »zlecenie płatnicze dotyczące płatności natychmiastowej« (instant payment order) – zgodnie ze schematem polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności – zlecenie płatnicze, które może być realizowane 24 godziny na dobę w dowolnym dniu kalendarzowym przez cały rok, przy przetwarzaniu natychmiastowym lub bliskim natychmiastowemu oraz przy powiadomieniu płatnika, obejmujące: (i) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA do TIPS DCA; (ii) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA na rachunek techniczny TIPS AS; (iii) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS do TIPS DCA; oraz (iv) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS na rachunek techniczny TIPS AS;";

e) dodaje się pkt 87–90 w brzmieniu:

„87) »schemat polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności« (European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme) lub »schemat SCT Inst« (SCT Inst scheme) – zautomatyzowany schemat oparty na otwartych standardach, określający zbiór zasad międzybankowych obowiązujących uczestników schematu SCT Inst, umożliwiający dostawcom usług płatniczych w ramach SEPA oferowanie zautomatyzowanego, obejmującego cały obszar SEPA produktu w postaci polecenia przelewu natychmiastowego w euro;

88) »rachunek techniczny TIPS systemu zewnętrznego (rachunek techniczny TIPS AS)« (TIPS ancillary system technical account (TIPS AS technical account)) – rachunek utrzymywany przez system zewnętrzny lub BC w imieniu systemu zewnętrznego, w systemie danego BC będącym komponentem TARGET2, wykorzystywany przez system zewnętrzny na potrzeby rozrachunku płatności natychmiastowych we własnych księgach;

89) »zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS« (TIPS DCA to TIPS AS technical account liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku TIPS DCA na rachunek techniczny TIPS AS w celu zasilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

90) »zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA« (TIPS AS technical account to TIPS DCA liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku technicznego TIPS AS na rachunek TIPS DCA w celu odsilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego.";

3) art. 13 otrzymuje brzmienie:

„*Artykuł 13*

Systemy zewnętrzne

1. BC Eurosystemu świadczą na rzecz systemów zewnętrznych usługi przelewu środków w pieniądzu banku centralnego w PM, z dostępem za pośrednictwem dostawcy usług sieciowych TARGET2. Usługi takie podlegają porozumieniom dwustronnym między BC Eurosystemu a danymi systemami zewnętrznymi.

2. Porozumienia dwustronne z systemami zewnętrznymi stosującymi ASI muszą być zgodne z załącznikiem IV. BC Eurosystemu zapewniają ponadto odpowiednie stosowanie w takich porozumieniach dwustronnych następujących postanowień załącznika II:

a) art. 8 ust. 1 (wymagania techniczne i prawne),

b) art. 8 ust. 2–5 (procedura ubiegania się o uczestnictwo), przy czym zamiast wymogu spełnienia kryteriów dostępu określonych w art. 4 do systemu zewnętrznego stosuje się wymóg spełnienia kryteriów dostępu ustalonych w definicji systemu zewnętrznego w art. 1 załącznika II,

c) harmonogramu operacyjnego określonego w dodatku V,

d) art. 11 (wymagania dotyczące współpracy i wymiany informacji), z wyjątkiem ust. 8,

e) art. 27 i 28 (procedury zapewniania ciągłości działania i postępowania w sytuacjach awaryjnych oraz wymogi bezpieczeństwa i procedury kontroli), zgodnie z którymi opłata stosowana jako podstawa obliczania kar pieniężnych za nieprzestrzeganie wymogów bezpieczeństwa na podstawie art. 28 załącznika II stanowi opłatę, o której mowa w załączniku IV pkt 18 ppkt 1 lit. a),

f) art. 31 (zasady dotyczące odpowiedzialności),

g) art. 32 (reguły dowodowe),

h) art. 33 i 34 (okres obowiązywania, wypowiedzenie i zawieszenie uczestnictwa), z wyjątkiem art. 34 ust. 1 lit. b),

i) art. 35, o ile ma zastosowanie (zamknięcie rachunków w PM),

j) art. 38 (zasady dotyczące poufności),

k) art. 39 (wymagania Unii związane z ochroną danych, zapobieganiem praniu brudnych pieniędzy i podobne kwestie),

l) art. 40 (wymagania dotyczące zawiadomień),

m) art. 41 (stosunek umowny z dostawcą usług sieciowych TARGET2),

n) art. 44 (zasady dotyczące prawa właściwego, właściwości sądów i miejsca wykonania świadczenia),

o) art. 45a ust. 1 (klauzula przejściowa).

3. Porozumienia dwustronne z systemami zewnętrznymi stosującymi interfejs użytkownika powinny być zgodne zarówno z:

a) załącznikiem II, z wyjątkiem tytułu V oraz dodatków VI i VII, jak i

b) art. 18 załącznika IV.

Dla celów lit. a) opłata stosowana jako podstawa obliczania kar pieniężnych za nieprzestrzeganie wymogów bezpieczeństwa na podstawie art. 28 załącznika II stanowi opłatę, o której mowa w załączniku IV pkt 18 ppkt 1 lit. a).

4. W drodze wyjątku od postanowień ust. 3 porozumienia dwustronne z systemami zewnętrznymi stosującymi interfejs użytkownika, ale dokonującymi rozrachunku transakcji płatniczych jedynie na rzecz swoich klientów, powinny być zgodne zarówno z:

a) załącznikiem II, z wyjątkiem tytułu V, art. 36 i dodatków VI i VII, jak i

b) art. 18 załącznika IV.

Dla celów lit. a) opłata stosowana jako podstawa obliczania kar pieniężnych za nieprzestrzeganie wymogów bezpieczeństwa na podstawie art. 28 załącznika II stanowi opłatę, o której mowa w załączniku IV pkt 18 ppkt 1 lit. a).

5. BC Eurosystemu świadczą usługi przelewu środków w pieniądzu banku centralnego na rzecz systemów zewnętrznych dokonujących rozrachunku płatności natychmiastowych we własnych księgach zgodnie ze schematem SCT Inst wyłącznie na platformie TIPS. Porozumienia dwustronne dotyczące świadczenia takich usług przelewu środków muszą być zgodne z załącznikiem IVa i umożliwiać jedynie rozrachunek płatności natychmiastowych zgodnie ze schematem SCT Inst. W takich dwustronnych porozumieniach stosuje się odpowiednio następujące postanowienia załącznika IIb:

a) dodatki I, II i III;

b) art. 4 (ogólna charakterystyka TARGET2);

c) art. 5 (kryteria dostępu), zgodnie z którym system zewnętrzny musi spełniać kryteria dostępu określone w definicji »systemu zewnętrznego« w art. 1 załącznika IIb;

d) art. 6 ust. 1 (wymagania techniczne i prawne), z zastrzeżeniem, że zamiast obowiązku zachowania zgodności ze schematem SCT Inst przez podpisanie porozumienia o zachowaniu zgodności ze schematem polecenia przelewu natychmiastowego SEPA, system zewnętrzny ma obowiązek ogłoszenia swojej zgodności ze schematem SCT Inst;

e) art. 6 ust. 2–5 (procedura ubiegania się o uczestnictwo), z zastrzeżeniem, że: (i) zamiast obowiązku spełnienia kryteriów dostępu określonych w art. 5 system zewnętrzny musi spełniać kryteria dostępu określone w definicji „systemu zewnętrznego" w art. 1 załącznika IIb oraz (ii) zamiast podlegania obowiązkowi przedstawienia dowodów na zachowanie zgodności ze schematem SCT Inst, system zewnętrzny przedstawia dowód ogłoszenia zgodności ze schematem SCT Inst;

f) art. 7 (uzyskiwanie dostępu do platformy TIPS);

g) art. 8 (podmioty osiągalne);

h) art. 9 (dostawca usług sieciowych);

i) art. 11 (TIPS directory);

j) art. 11a (repozytorium MPL);

k) art. 12 (zobowiązania BC i posiadaczy rachunków), z wyjątkiem ust. 4;

l) art. 14 (wymagania dotyczące współpracy i wymiany informacji);

m) art. 16 (typy zleceń płatniczych);

n) art. 17 (przyjmowanie oraz odrzucanie zleceń płatniczych);

o) art. 18 (przetwarzanie zleceń płatniczych);

p) art. 19 (żądanie zwrotu płatności);

q) art. 20 (moment wprowadzenia, moment nieodwołalności);

r) art. 21 (wymogi bezpieczeństwa i zapewnienie ciągłości działania);

s) art. 23 (zasady dotyczące odpowiedzialności);

t) art. 24 (reguły dowodowe);

u) art. 25 i 26 (okres obowiązywania, wypowiedzenie i zawieszenie uczestnictwa), z wyjątkiem art. 26 ust. 1 lit. b) oraz z wyjątkiem art. 26 ust. 4 akapit drugi;

v) art. 27, o ile ma zastosowanie (zamknięcie rachunków);

w) art. 29 (zasady dotyczące poufności);

x) art. 30 (wymagania Unii związane z ochroną danych, zapobieganiem praniu brudnych pieniędzy i podobne kwestie);

y) art. 31 (wymagania dotyczące zawiadomień);

z) art. 34 (zasady dotyczące prawa właściwego, właściwości sądów i miejsca wykonania świadczenia);

aa) art. 35a (klauzula przejściowa).";

4) w art. 17 ust. 4 otrzymuje brzmienie:

„4. Ustępy 1–3a niniejszego artykułu mają także zastosowanie w przypadku zawieszenia lub wypowiedzenia korzystania z interfejsu ASI lub platformy TIPS przez systemy zewnętrzne.";

5) dodaje się art. 27a w brzmieniu:

„*Artykuł 27a*

Przepis przejściowy

BC Eurosystemu mogą świadczyć usługi przelewu środków w pieniądzu banku centralnego na rzecz systemów zewnętrznych dokonujących rozrachunku płatności natychmiastowych we własnych księgach zgodnie ze schematem SCT Inst, korzystając z interfejsu systemów zewnętrznych do dnia 25 lutego 2022 r.";

6) w załączniku II do wytycznych EBC/2012/27 wprowadza się zmiany zgodnie z załącznikiem I do niniejszych wytycznych;

7) w załączniku IIa do wytycznych EBC/2012/27 wprowadza się zmiany zgodnie z załącznikiem II do niniejszych wytycznych;

8) w załączniku IIb do wytycznych EBC/2012/27 wprowadza się zmiany zgodnie z załącznikiem III do niniejszych wytycznych;

9) w załączniku IV do wytycznych EBC/2012/27 wprowadza się zmiany zgodnie z załącznikiem IV do niniejszych wytycznych;

10) do wytycznych EBC/2012/27 dodaje się nowy załącznik IVa, zgodnie z załącznikiem V do niniejszych wytycznych.

Artykuł 2

Skuteczność i implementacja

1. Niniejsze wytyczne stają się skuteczne z dniem zawiadomienia o nich krajowych banków centralnych państw członkowskich, których walutą jest euro.

2. Krajowe banki centralne państw członkowskich, których walutą jest euro, podejmują środki konieczne do zapewnienia zgodności z postanowieniami niniejszych wytycznych od dnia 21 listopada 2021 r., z wyjątkiem pkt 1 lit. c), pkt 7 i 9 załącznika II do niniejszych wytycznych, w przypadku których podejmują one konieczne środki i stosują je od dnia 13 czerwca 2022 r. Najpóźniej do dnia 9 września 2021 r. powiadamiają one EBC o treści aktów prawnych i innych czynnościach związanych z tymi środkami.

Artykuł 3

Adresaci

Niniejsze wytyczne są adresowane do wszystkich banków centralnych Eurosystemu.

Sporządzono we Frankfurcie nad Menem dnia 20 lipca 2021 r.

W imieniu Rady Prezesów EBC
Christine LAGARDE
Prezes EBC

ZAŁĄCZNIK I

W załączniku II do wytycznych EBC/2012/27 wprowadza się następujące zmiany:

1) w art. 1 wprowadza się następujące zmiany:

a) w definicji terminu „grupa" lit. a) otrzymuje brzmienie:

„a) grupę złożoną z instytucji kredytowych objętych skonsolidowanym sprawozdaniem finansowym spółki dominującej, w przypadku gdy spółka taka jest zobowiązana do przedstawiania skonsolidowanego sprawozdania finansowego na podstawie Międzynarodowego Standardu Rachunkowości 27 (IAS 27), przyjętego zgodnie z rozporządzeniem Komisji (WE) nr 1126/2008 (*) oraz przy założeniu, iż grupa taka składa się: (i) ze spółki dominującej oraz jednej lub większej liczby spółek zależnych; (ii) z dwóch lub większej liczby spółek zależnych spółki dominującej; lub

(*) Rozporządzenie Komisji (WE) nr 1126/2008 z dnia 3 listopada 2008 r. przyjmujące określone międzynarodowe standardy rachunkowości zgodnie z rozporządzeniem (WE) nr 1606/2002 Parlamentu Europejskiego i Rady (Dz.U. L 320 z 29.11.2008, s. 1).";

b) definicja terminu „zlecenie płatnicze dotyczące płatności natychmiastowej" otrzymuje brzmienie:

„— »zlecenie płatnicze dotyczące płatności natychmiastowej« (instant payment order) – zgodnie ze schematem polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności – zlecenie płatnicze, które może być realizowane 24 godziny na dobę w dowolnym dniu kalendarzowym przez cały rok, przy przetwarzaniu natychmiastowym lub bliskim natychmiastowemu oraz przy powiadomieniu płatnika, obejmujące: (i) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA do TIPS DCA; (ii) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA na rachunek techniczny TIPS AS; (iii) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS do TIPS DCA; oraz (iv) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS na rachunek techniczny TIPS AS;";

c) dodaje się następujące definicje:

„— »schemat polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności« (European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme) lub »schemat SCT Inst« (SCT Inst scheme) – zautomatyzowany schemat oparty na otwartych standardach, określający zbiór zasad międzybankowych obowiązujących uczestników schematu SCT Inst, umożliwiający dostawcom usług płatniczych w ramach SEPA oferowanie zautomatyzowanego, obejmującego cały obszar SEPA produktu w postaci polecenia przelewu natychmiastowego w euro;

— »rachunek techniczny TIPS systemu zewnętrznego (rachunek techniczny TIPS AS)« (TIPS ancillary system technical account (TIPS AS technical account)) – rachunek utrzymywany przez system zewnętrzny lub BC w imieniu systemu zewnętrznego w systemie danego BC będącym komponentem TARGET2, wykorzystywany przez system zewnętrzny na potrzeby rozrachunku płatności natychmiastowych we własnych księgach;

— »zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS« (TIPS DCA to TIPS AS technical account liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku TIPS DCA na rachunek techniczny TIPS AS w celu zasilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

— »zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA« (TIPS AS technical account to TIPS DCA liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku technicznego TIPS AS na rachunek TIPS DCA w celu odsilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

— »podmiot osiągalny« (reachable party) – podmiot, który: a) posiada kod BIC; b) jest wyznaczony jako podmiot osiągalny przez posiadacza rachunku TIPS DCA lub przez system zewnętrzny; c) jest korespondentem, klientem lub oddziałem posiadacza rachunku TIPS DCA lub uczestnikiem systemu zewnętrznego, lub też korespondentem, klientem lub oddziałem uczestnika systemu zewnętrznego; oraz d) jest adresowalny za pośrednictwem Platformy TIPS i może składać zlecenia płatnicze dotyczące płatności natychmiastowej oraz otrzymywać zlecenia płatnicze dotyczące płatności natychmiastowej albo za pośrednictwem posiadacza rachunku TIPS DCA lub systemu zewnętrznego, albo – jeżeli posiadacz rachunku TIPS DCA lub system zewnętrzny wyrazi na to zgodę – bezpośrednio.";

d) skreśla się definicję „dostawcy usług sieciowych TIPS";

2) w art. 3 wprowadza się następujące zmiany:

a) w ust 2 lit. fc) otrzymuje brzmienie:

„fc) zlecenia przekazania płynności z TIPS DCA do PM i zlecenia przekazania płynności z PM do TIPS DCA;";

b) w ust. 2 dodaje się lit. fd) w brzmieniu:

„fd) zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS oraz zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA; oraz";

c) ust. 3 otrzymuje brzmienie:

„3. TARGET2 umożliwia rozrachunek brutto w czasie rzeczywistym płatności w euro, przeprowadzany w pieniądzu banku centralnego na rachunkach w PM, rachunkach T2S DCA i rachunkach TIPS DCA. TARGET2 został stworzony i funkcjonuje w oparciu o SSP, za pośrednictwem której na tych samych zasadach technicznych następuje składanie i przetwarzanie zleceń płatniczych oraz otrzymywanie płatności. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków T2S DCA, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę T2S. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków TIPS DCA i rachunków technicznych TIPS AS, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę TIPS.";

3) art. 5 otrzymuje brzmienie:

„*Artykuł 5*

Uczestnicy bezpośredni

1. Posiadacze rachunków w PM w TARGET2-[oznaczenie BC/kraju] są uczestnikami bezpośrednimi i mają obowiązek spełniać wymogi określone w art. 8 ust. 1 i 2. Uczestnicy ci posiadają co najmniej jeden rachunek w PM w [nazwa BC]. Posiadacze rachunków w PM, którzy zobowiązali się do zachowania zgodności ze schematem SCT Inst przez podpisanie porozumienia o zachowaniu zgodności ze schematem polecenia przelewu natychmiastowego SEPA, mają obowiązek być stale osiągalni na platformie TIPS, albo jako posiadacze rachunku TIPS DCA, albo jako podmioty osiągalne za pośrednictwem posiadacza rachunku TIPS DCA.

2. Posiadacze rachunku w PM są uprawnieni do wyznaczania adresowalnych posiadaczy BIC, bez względu na ich siedzibę. Posiadacze rachunków w PM są uprawnieni do wyznaczania adresowalnych posiadaczy BIC, którzy zobowiązali się do zachowania zgodności ze schematem SCT Inst przez podpisanie porozumienia o zachowaniu zgodności ze schematem polecenia przelewu natychmiastowego SEPA, tylko jeśli takie podmioty są osiągalne na platformie TIPS, albo jako posiadacze rachunku TIPS DCA, albo jako podmioty osiągalne za pośrednictwem posiadacza rachunku TIPS DCA.

3. Posiadacze rachunku w PM mogą wyznaczać inne podmioty jako uczestników pośrednich w PM, pod warunkiem spełnienia warunków określonych w art. 6. Posiadacze rachunków w PM są uprawnieni do wyznaczania jako uczestników pośrednich podmioty, które zobowiązały się do zachowania zgodności ze schematem SCT Inst przez podpisanie porozumienia o zachowaniu zgodności ze schematem polecenia przelewu natychmiastowego SEPA, tylko jeśli takie podmioty są osiągalne na platformie TIPS, albo jako posiadacze rachunku TIPS DCA w [nazwa BC], albo jako podmioty osiągalne za pośrednictwem posiadacza rachunku TIPS DCA.

4. Do dostępu wieloadresowego przez oddziały stosuje się następujące zasady:

a) instytucja kredytowa w rozumieniu art. 4 ust. 1 lit. a) lub b) niniejszego załącznika, która została przyjęta jako posiadacz rachunku w PM, może udzielić dostępu do swojego rachunku w PM jednemu lub większej liczbie własnych oddziałów mających siedzibę w Unii lub EOG w celu bezpośredniego składania zleceń płatniczych lub otrzymywania płatności, pod warunkiem iż [nazwa BC] został o tym odpowiednio powiadomiony;

b) w sytuacji, gdy oddział instytucji kredytowej został przyjęty jako posiadacz rachunku w PM, inne oddziały tej samej osoby prawnej lub jej centrala, w obu przypadkach pod warunkiem posiadania siedziby w Unii lub EOG, mogą uzyskiwać dostęp do rachunku w PM takiego oddziału, pod warunkiem że odpowiednio powiadomiony został [nazwa BC].";

4) w art 12 ust. 5 otrzymuje brzmienie:

„5. Rachunki w PM oraz subkonta takich rachunków podlegają oprocentowaniu w wysokości niższej z następujących wartości: zera procent lub stopy depozytu w banku centralnym, z wyjątkiem sytuacji, w której rachunki takie są wykorzystywane w celu przechowywania rezerw obowiązkowych lub nadwyżek rezerw.

Obliczanie i wypłata oprocentowania z tytułu utrzymywanych rezerw obowiązkowych podlega przepisom rozporządzenia Rady (WE) nr 2531/98 (*) oraz rozporządzenia Europejskiego Banku Centralnego (UE) 2021/378 (EBC/2021/1) (**).

Obliczanie i wypłata oprocentowania z tytułu utrzymywanych nadwyżek rezerw podlega decyzji (UE) 2019/1743 (EBC/2019/31) (***).

(*) Rozporządzenie Rady (WE) nr 2531/98 z dnia 23 listopada 1998 r. dotyczące stosowania stóp rezerw obowiązkowych przez Europejski Bank Centralny (Dz.U. L 318 z 27.11.1998, s. 1).

(**) Rozporządzenie Europejskiego Banku Centralnego (UE) 2021/378 z dnia 22 stycznia 2021 r. w sprawie stosowania wymogów dotyczących utrzymywania rezerwy obowiązkowej (EBC/2021/1) (Dz.U. L 73 z 3.3.2021, s. 1).

(***) Decyzja Europejskiego Banku Centralnego (UE) 2019/1743 z dnia 15 października 2019 r. w sprawie oprocentowania nadwyżek rezerw oraz niektórych depozytów (EBC/2019/31) (Dz.U. L 267 z 21.10.2019, s. 12).";

5) art. 28 otrzymuje brzmienie:

„*Artykuł 28*

Wymogi bezpieczeństwa i procedury kontroli

1. Obowiązkiem uczestników jest wdrożenie odpowiednich narzędzi kontroli w zakresie bezpieczeństwa, chroniących systemy przed nieuprawnionym dostępem i wykorzystaniem. Uczestnicy ponoszą wyłączną odpowiedzialność za odpowiednią ochronę poufności, integralności i dostępności ich systemów.

2. Uczestnicy informują [nazwa BC] o wszystkich incydentach związanych z bezpieczeństwem w ich infrastrukturze technicznej, jak również, w razie potrzeby, o incydentach związanych z bezpieczeństwem występujących w infrastrukturze technicznej podmiotów zewnętrznych. [Nazwa BC] może żądać dodatkowych informacji dotyczących incydentu, a także, w razie potrzeby, podjęcia przez uczestnika odpowiednich środków w celu zapobieżenia powtórzeniu się takiego incydentu.

3. [Nazwa BC] może nałożyć dodatkowe wymagania w zakresie bezpieczeństwa, w szczególności w zakresie cyberbezpieczeństwa lub zapobiegania oszustwom, na wszystkich uczestników lub też na uczestników uważanych przez niego za krytycznych.

4. Uczestnicy przekazują [nazwa BC]: (i) stały dostęp do swojego potwierdzenia zgodności z wymogami wybranego przez nich dostawcy usług sieciowych w zakresie ochrony punktów końcowych (endpoint security); oraz (ii) corocznie – oświadczenie o samocertyfikacji dotyczącej systemu TARGET2 opublikowane na stronie internetowej [nazwa BC] oraz na stronie internetowej EBC w języku angielskim.

4a. [Nazwa BC] dokonuje oceny oświadczeń o samocertyfikacji uczestników w odniesieniu do stopnia zapewnienia przez nich zgodności z każdym z wymogów samocertyfikacji dotyczącej systemu TARGET2. Wymogi te określono w dodatku VIII, który, wraz z innymi dodatkami wskazanymi w art. 2 ust. 1, stanowi integralną część niniejszych warunków uczestnictwa.

4b. Stopień zapewnienia przez uczestnika zgodności z wymogami samocertyfikacji dotyczącej systemu TARGET2 klasyfikuje się w następujący sposób, przy rosnącym stopniu braku zgodności: »pełna zgodność«, »niewielka niezgodność« lub »poważna niezgodność«. Stosuje się następujące kryteria: pełna zgodność zostaje osiągnięta, gdy uczestnicy spełniają 100% wymogów; niewielka niezgodność ma miejsce, gdy uczestnik spełnia mniej niż 100%, ale co najmniej 66% wymogów, a poważna niezgodność ma miejsce wówczas, gdy uczestnik spełnia mniej niż 66% wymogów. Jeśli uczestnik wykaże, że dany wymóg nie ma do niego zastosowania, dla celów kategoryzacji uznaje się, że taki wymóg jest spełniony. Uczestnik, który nie osiągnie pełnej zgodności, przedkłada plan działania wskazujący, w jaki sposób zamierza ją osiągnąć. [Nazwa BC] informuje odpowiednie organy nadzoru o statusie zgodności takiego uczestnika.

4c. Jeżeli uczestnik odmawia udzielenia stałego dostępu do swojego poświadczenia zgodności z wymogami wybranego przez siebie dostawcy usług sieciowych w zakresie ochrony punktów końcowych (endpoint security) lub nie przedstawi samocertyfikacji dotyczącej systemu TARGET2, poziom zgodności uczestnika klasyfikuje się jako »poważną niezgodność«.

4d. [Nazwa BC] dokonuje ponownych ocen zgodności uczestników z częstotliwością roczną.

4e. [Nazwa BC] może nałożyć na uczestników, których poziom zgodności został oceniony jako »niewielka niezgodność« lub »poważna niezgodność«, następujące środki naprawcze, w porządku rosnącym według stopnia dotkliwości:

(i) wzmożone monitorowanie: zobowiązanie uczestnika do przekazywania [nazwa BC] miesięcznych sprawozdań, podpisanych przez członka kadry kierowniczej wyższego szczebla, dotyczących postępów w usuwaniu niezgodności. Uczestnik ponosi dodatkowo miesięczną karę pieniężną za każdy rachunek, którego dotyczy niezgodność, równą miesięcznej opłacie ponoszonej przez uczestnika określonej w pkt 1 dodatku VI, z wyłączeniem opłat transakcyjnych. Taki środek naprawczy może zostać nałożony w przypadku, gdy wobec uczestnika drugi raz z kolei zostanie wydana ocena stwierdzająca niewielką niezgodność lub gdy zostanie wobec niego wydana ocena stwierdzająca poważną niezgodność;

(ii) zawieszenie: uczestnictwo w TARGET2-[oznaczenie BC/kraju] może zostać zawieszone w okolicznościach opisanych w art. 34 ust. 2 lit. b) i c) niniejszego załącznika. W drodze odstępstwa od art. 34 niniejszego załącznika uczestnik zostaje powiadomiony o takim zawieszeniu z trzymiesięcznym wyprzedzeniem. Uczestnik ponosi miesięczną karę pieniężną za każdy zawieszony rachunek równą podwójnej miesięcznej opłacie ponoszonej przez uczestnika określonej w pkt 1 dodatku VI, z wyłączeniem opłat transakcyjnych. Taki środek naprawczy może zostać nałożony w przypadku, gdy wobec uczestnika drugi raz z kolei zostanie wydana ocena stwierdzająca poważną niezgodność;

(iii) wypowiedzenie: uczestnictwo w TARGET2-[oznaczenie BC/kraju] może zostać wypowiedziane w okolicznościach opisanych w art. 34 ust. 2 lit. b) i c) niniejszego załącznika. W drodze odstępstwa od art. 34 niniejszego załącznika uczestnik zostaje powiadomiony o takim wypowiedzeniu z trzymiesięcznym wyprzedzeniem. Uczestnik ponosi dodatkową karę pieniężną w wysokości 1 000 EUR za każdy zamknięty rachunek. Taki środek naprawczy może zostać nałożony, jeżeli uczestnik nie usunął poważnej niezgodności w sposób zadowalający dla [nazwa BC] w terminie trzech miesięcy od dnia zawieszenia.

5. Uczestnicy, którzy udostępniają swój rachunek w PM osobom trzecim zgodnie z art. 5 ust. 2, 3 i 4, przeciwdziałają ryzyku wynikającemu z takiego udostępniania zgodnie z wymogami bezpieczeństwa określonymi w ust. 1–4e niniejszego artykułu. Samocertyfikacja, o której mowa w ust. 4, wskazuje, że uczestnik nakłada na osoby trzecie, które mają dostęp do rachunku w PM tego uczestnika, wymogi dostawcy usług sieciowych TARGET2 w zakresie ochrony punktów końcowych (endpoint security).";

6) w art. 39 ust. 1 otrzymuje brzmienie:

„1. Przyjmuje się, że uczestnicy są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o ochronie danych, mają oni obowiązek przestrzegania takich obowiązków oraz muszą być w stanie wykazać ich przestrzeganie przed właściwymi organami. Przyjmuje się, że uczestnicy są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu, działalności łączącej się z ryzykiem rozprzestrzeniania broni jądrowej oraz rozwoju środków przenoszenia broni jądrowej. Uczestnicy mają obowiązek wykonywania tych obowiązków w szczególności poprzez podejmowanie odpowiednich środków dotyczących płatności obciążających lub uznających ich rachunki w PM. Przed nawiązaniem stosunku umownego z dostawcą usług sieciowych TARGET2 uczestnicy mają obowiązek upewnić się, że są im znane zasady przechowywania danych stosowane przez tego dostawcę usług sieciowych TARGET2.";

7) dodaje się art. 45a w brzmieniu:

„*Artykuł 45a*

Przepisy przejściowe

1. Po uruchomieniu systemu TARGET i zaprzestaniu działania systemu TARGET2 salda rachunków w PM przekazywane są na odpowiednie rachunki posiadacza rachunku w systemie TARGET.

2. Wymóg, zgodnie z którym posiadacze rachunków w PM, uczestnicy pośredni i adresowalni posiadacze BIC zachowujący zgodność ze schematem SCT Inst muszą być osiągalni na platformie TIPS zgodnie z art. 5, stosuje się od dnia 25 lutego 2022 r.";

8) w dodatku I pkt 8 ppkt 4 lit. b) otrzymuje brzmienie:

„b) tryb użytkownik-aplikacja (user-to-applicaton mode – U2A)

Tryb U2A umożliwia bezpośrednią komunikację pomiędzy uczestnikiem a ICM. Informacje wyświetlane są w przeglądarce działającej na systemie PC (SWIFT Alliance WebStation lub inny interfejs, który może być wymagany przez SWIFT). W celu uzyskania dostępu w trybie U2A infrastruktura informatyczna musi obsługiwać pliki cookies. Dalsze szczegóły zawarte są w podręczniku użytkownika ICM.";

9) w dodatku IV pkt 6 lit. g) otrzymuje brzmienie:

„g) w celu awaryjnego przetwarzania zleceń płatniczych uczestnicy ustanowią kwalifikowane aktywa jako zabezpieczenie. Podczas przetwarzania awaryjnego przychodzące płatności awaryjne mogą zostać wykorzystane do pokrycia wychodzących zapasowych płatności awaryjnych. W ramach przetwarzania awaryjnego [nazwa BC] może nie uwzględniać dostępnej płynności uczestników.";

10) dodaje się nowy dodatek VIII do załącznika II do wytycznych EBC/2012/27 w brzmieniu określonym w załączniku VI do niniejszych wytycznych.

ZAŁĄCZNIK II

W załączniku IIa do wytycznych EBC/2012/27 wprowadza się następujące zmiany:

1) w art. 1 wprowadza się następujące zmiany:

   a) definicja terminu „zlecenie płatnicze dotyczące płatności natychmiastowej" otrzymuje brzmienie:

      „— »zlecenie płatnicze dotyczące płatności natychmiastowej« (instant payment order) – zgodnie ze schematem polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności – zlecenie płatnicze, które może być realizowane 24 godziny na dobę w dowolnym dniu kalendarzowym przez cały rok, przy przetwarzaniu natychmiastowym lub bliskim natychmiastowemu oraz przy powiadomieniu płatnika, obejmujące: (i) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA do TIPS DCA; (ii) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA na rachunek techniczny TIPS AS; (iii) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS do TIPS DCA; oraz (iv) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS na rachunek techniczny TIPS AS;";

   b) dodaje się następujące definicje:

      „— »rachunek techniczny TIPS systemu zewnętrznego (rachunek techniczny TIPS AS)« (TIPS ancillary system technical account (TIPS AS technical account)) – rachunek utrzymywany przez system zewnętrzny lub BC w imieniu systemu zewnętrznego w systemie danego BC będącym komponentem TARGET2, przeznaczony do wykorzystania przez system zewnętrzny na potrzeby rozrachunku płatności natychmiastowych we własnych księgach;

      — »zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS« (TIPS DCA to TIPS AS technical account liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku TIPS DCA na rachunek techniczny TIPS AS w celu zasilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

      — »zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA« (TIPS AS technical account to TIPS DCA liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku technicznego TIPS AS na rachunek TIPS DCA w celu odsilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

      — »dostawca usług sieciowych« (Network Service Provider, NSP) – przedsiębiorstwo, które uzyskało koncesję od Eurosystemu na świadczenie usług łączności za pośrednictwem jednolitego punku dostępu do infrastruktury rynkowej Eurosystemu.";

   c) skreśla się definicję „dostawcy usług sieciowych T2S";

2) w art. 4 ust. 2 lit. fc) otrzymuje brzmienie:

   „fc) zlecenia przekazania płynności z TIPS DCA do PM i zlecenia przekazania płynności z PM do TIPS DCA;";

3) w art. 4 ust. 2 dodaje się lit. fd) w brzmieniu:

   „fd) zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS oraz zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA; oraz";

4) w art. 4 ust. 3 otrzymuje brzmienie:

   „3. TARGET2 umożliwia rozrachunek brutto w czasie rzeczywistym płatności w euro, przeprowadzany w pieniądzu banku centralnego na rachunkach w PM, rachunkach T2S DCA i rachunkach TIPS DCA. TARGET2 został stworzony i funkcjonuje w oparciu o SSP, za pośrednictwem której na tych samych zasadach technicznych następuje składanie i przetwarzanie zleceń płatniczych oraz otrzymywanie płatności. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków T2S DCA, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę T2S. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków TIPS DCA i rachunków technicznych TIPS AS, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę TIPS. Podmiotem świadczącym usługi na podstawie niniejszych warunków uczestnictwa jest [nazwa BC]. Działania i zaniechania KBC dostarczających SSP oraz 4BC są uważane za działania i zaniechania [nazwa BC], za które ponosi on odpowiedzialność zgodnie z art. 21 niniejszego załącznika. Uczestnictwo na podstawie niniejszych warunków uczestnictwa nie prowadzi do powstania stosunków umownych między posiadaczami rachunków T2S DCA a KBC dostarczającymi SSP albo 4BC w zakresie, w jakim KBC działają w tym charakterze. Instrukcje, komunikaty lub informacje otrzymywane przez posiadacza rachunku T2S DCA z SSP albo platformy T2S lub przesyłane przez uczestnika do SSP albo platformy T2S w związku z usługami świadczonymi na podstawie niniejszych warunków uczestnictwa uważa się za otrzymywane od [nazwa BC] lub wysyłane do [nazwa BC].";

5) w art. 8 ust. 3 otrzymuje brzmienie:

   „3. W przypadku gdy [nazwa BC] uwzględnił wniosek posiadacza rachunku T2S DCA zgodnie z ust. 1, uznaje się, że ten posiadacz rachunku T2S DCA upoważnił uczestniczące CSD do obciążenia rachunku T2S DCA kwotami związanymi z transakcjami, których przedmiotem są papiery wartościowe, realizowanymi na tych rachunkach papierów wartościowych.";

6) w art. 28 ust. 1 otrzymuje brzmienie:

„1. Przyjmuje się, że posiadacze rachunków T2S DCA są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o ochronie danych, mają oni obowiązek przestrzegania takich obowiązków oraz muszą być w stanie wykazać ich przestrzeganie przed właściwymi organami. Przyjmuje się, że posiadacze rachunków T2S DCA są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu, działalności łączącej się z ryzykiem rozprzestrzeniania broni jądrowej oraz rozwoju środków przenoszenia broni jądrowej. Posiadacze rachunków T2S DCA mają obowiązek wykonywania tych obowiązków w szczególności poprzez podejmowanie odpowiednich środków dotyczących płatności obciążających lub uznających ich rachunki T2S DCA. Przed nawiązaniem stosunku umownego z dostawcą usług sieciowych T2S posiadacze rachunków T2S DCA mają obowiązek upewnić się, że są im znane stosowane przez tego dostawcę usług sieciowych T2S zasady przechowywania danych.";

7) art. 30 otrzymuje brzmienie:

„Artykuł 30

Stosunek umowny z dostawcą usług sieciowych

1. Posiadacze rachunków T2S DCA mają obowiązek:

a) zawrzeć umowę z dostawcą usług sieciowych w ramach umowy dotyczącej koncesji z tym dostawcą w celu ustanowienia połączenia technicznego do systemu TARGET2-[nazwa BC]; albo

b) połączyć się za pośrednictwem innego podmiotu, który zawarł umowę z dostawcą usług sieciowych w ramach umowy dotyczącej koncesji z tym dostawcą.

2. Stosunek prawny między posiadaczem rachunku T2S DCA a dostawcą usług sieciowych podlega wyłącznie warunkom odrębnej umowy zawartej z dostawcą usług sieciowych, o której mowa w ust. 1 lit. a).

3. Usługi świadczone przez dostawcę usług sieciowych nie stanowią części usług świadczonych przez [nazwa BC] w związku z TARGET2.

4. [Nazwa BC] nie ponosi odpowiedzialności za działania, błędy czy zaniechania dostawcy usług sieciowych (w tym jego kierowników, pracowników i zleceniobiorców) ani za żadne działania, błędy czy zaniechania osób trzecich wybranych przez uczestników w celu uzyskania dostępu do sieci danego dostawcy usług sieciowych.";

8) dodaje się art. 34a w brzmieniu:

„Artykuł 34a

Przepisy przejściowe

Po uruchomieniu systemu TARGET i zaprzestaniu działania systemu TARGET2 posiadacze rachunków T2S DCA stają się posiadaczami rachunków T2S DCA w systemie TARGET.";

9) odniesienia do „dostawcy usług sieciowych T2S" (w liczbie pojedynczej lub mnogiej) w art. 6 ust. 1 lit. a) ppkt (i), art. 9 ust. 5, art. 10 ust. 6, art. 14 ust. 1 lit. a), art. 22 ust. 1, 2 i 3, art. 27 ust. 5, art. 28 ust. 1, art. 29 ust. 1 załącznika IIa oraz w pkt 1 dodatku I zastępuje się odniesieniami do „dostawcy usług sieciowych";

10) w dodatku I pkt 7 ppkt 1 lit. b) otrzymuje brzmienie:

„b) tryb użytkownik-aplikacja (user-to-applicaton mode – U2A)

Tryb U2A umożliwia bezpośrednią komunikację pomiędzy posiadaczem rachunku T2S DCA a T2S GUI. Informacje wyświetlane są w przeglądarce działającej na PC. W celu uzyskania dostępu w trybie U2A infrastruktura informatyczna musi obsługiwać pliki cookies. Dalsze szczegóły zawarte są w podręczniku użytkownika T2S.".

ZAŁĄCZNIK III

W załączniku IIb wytycznych EBC/2012/27 wprowadza się następujące zmiany:

1) Odniesienia do „dostawcy usług sieciowych TIPS" (w liczbie pojedynczej lub mnogiej) w art. 17 ust. 1 lit. a), art. 24 ust. 1 i 2, art. 26 ust. 2 lit. d), art. 29 ust. 6, pkt 1 dodatku I, pkt 6 ppkt 1 dodatku I oraz pkt 3 ppkt 3 lit. b) dodatku II zastępuje się odniesieniami do „dostawcy usług sieciowych";

2) w art. 1 wprowadza się następujące zmiany:

   a) definicja terminu „podmiot osiągalny" otrzymuje brzmienie:

      „— »podmiot osiągalny« (reachable party) – podmiot, który: a) posiada kod BIC; b) jest wyznaczony jako podmiot osiągalny przez posiadacza rachunku TIPS DCA lub przez system zewnętrzny; c) jest korespondentem, klientem lub oddziałem posiadacza rachunku TIPS DCA lub uczestnikiem systemu zewnętrznego, lub też korespondentem, klientem lub oddziałem uczestnika systemu zewnętrznego; oraz d) jest adresowalny za pośrednictwem Platformy TIPS i może składać zlecenia płatnicze dotyczące płatności natychmiastowej oraz otrzymywać zlecenia płatnicze dotyczące płatności natychmiastowej albo za pośrednictwem posiadacza rachunku TIPS DCA lub systemu zewnętrznego, albo – jeżeli posiadacz rachunku TIPS DCA lub system zewnętrzny wyrazi na to zgodę – bezpośrednio;";

   b) definicja terminu „zlecenie płatnicze" otrzymuje brzmienie:

      „— »zlecenie płatnicze« (payment order) – z wyjątkiem użycia w art. 16–18 niniejszego załącznika – zlecenie płatnicze dotyczące płatności natychmiastowej, pozytywną odpowiedź na żądanie zwrotu płatności, zlecenie przekazania płynności z PM do TIPS DCA, zlecenie przekazania płynności z TIPS DCA do PM, zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA, zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS;";

   c) definicja terminu „zlecenie płatnicze dotyczące płatności natychmiastowej" otrzymuje brzmienie:

      „— »zlecenie płatnicze dotyczące płatności natychmiastowej« (instant payment order) – zgodnie ze schematem polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności – zlecenie płatnicze, które może być realizowane 24 godziny na dobę w dowolnym dniu kalendarzowym przez cały rok, przy przetwarzaniu natychmiastowym lub bliskim natychmiastowemu oraz przy powiadomieniu płatnika, obejmujące: (i) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA do TIPS DCA; (ii) zlecenia płatnicze dotyczące płatności natychmiastowej z TIPS DCA na rachunek techniczny TIPS AS; (iii) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS do TIPS DCA; oraz (iv) zlecenia płatnicze dotyczące płatności natychmiastowej z rachunku technicznego TIPS AS na rachunek techniczny TIPS AS;";

   d) dodaje się następujące definicje:

      „— »rachunek techniczny TIPS systemu zewnętrznego (rachunek techniczny TIPS AS)« (TIPS ancillary system technical account (TIPS AS technical account)) – rachunek utrzymywany przez system zewnętrzny lub BC w imieniu systemu zewnętrznego w systemie danego BC będącym komponentem TARGET2, wykorzystywany przez ten system zewnętrzny na potrzeby rozrachunku płatności natychmiastowych we własnych księgach;

      — »zlecenie przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS« (TIPS DCA to TIPS AS technical account liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku TIPS DCA na rachunek techniczny TIPS AS w celu zasilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

      — »zlecenie przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA« (TIPS AS technical account to TIPS DCA liquidity transfer order) – instrukcję przekazania określonej kwoty z rachunku technicznego TIPS AS na rachunek TIPS DCA w celu odsilenia pozycji posiadacza rachunku TIPS DCA (lub pozycji innego uczestnika systemu zewnętrznego) w księgach systemu zewnętrznego;

      — »schemat polecenia przelewu natychmiastowego SEPA (SCT Inst) Europejskiej Rady ds. Płatności« (European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme) lub »schemat SCT Inst« (SCT Inst scheme) – zautomatyzowany schemat oparty na otwartych standardach, określający zbiór zasad międzybankowych obowiązujących uczestników schematu SCT Inst, umożliwiający dostawcom usług płatniczych w ramach SEPA oferowanie zautomatyzowanego, obejmującego cały obszar SEPA produktu w postaci polecenia przelewu natychmiastowego w euro;

      — »usługa sprawdzania adresów proxy dla urządzeń przenośnych (MPL)« (mobile proxy look-up (MPL) service) – usługę, która umożliwia posiadaczom rachunku TIPS DCA, systemom zewnętrznym korzystającym z rachunków technicznych TIPS AS i podmiotom osiągalnym, którzy otrzymują od swoich klientów wniosek o wykonanie zlecenia płatniczego dotyczącego płatności natychmiastowej na rzecz beneficjenta identyfikowanego za pomocą adresu proxy (np. numeru telefonu komórkowego), uzyskanie z centralnego repozytorium MPL odpowiedniego numeru IBAN beneficjenta i kodu BIC, które mają być wykorzystane do uznania odpowiedniego rachunku w TIPS;

      — »dostawca usług sieciowych« (Network Service Provider, NSP) – przedsiębiorstwo, które uzyskało koncesję od Eurosystemu na świadczenie usług łączności za pośrednictwem jednolitego punku dostępu do infrastruktury rynkowej Eurosystemu;

— »IBAN« (IBAN) – międzynarodowy numer rachunku bankowego, który jednoznacznie identyfikuje indywidualny rachunek w określonej instytucji finansowej w określonym państwie.";

e) skreśla się definicję „dostawcy usług sieciowych TIPS";

3) w art. 3 ust. 1 skreśla się odniesienie do „Dodatku V: Wymagania techniczne dotyczące łączności w odniesieniu do TIPS";

4) w art. 4 wprowadza się następujące zmiany:

a) w ust. 2 dodaje się lit. ia) w brzmieniu:

„ia) zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS oraz zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA; oraz";

b) ust. 3 otrzymuje brzmienie:

„3. TARGET2 umożliwia rozrachunek brutto w czasie rzeczywistym płatności w euro, przeprowadzany w pieniądzu banku centralnego na rachunkach w PM, rachunkach T2S DCA i rachunkach TIPS DCA. TARGET2 został stworzony i funkcjonuje w oparciu o SSP, za pośrednictwem której na tych samych zasadach technicznych następuje składanie i przetwarzanie zleceń płatniczych oraz otrzymywanie płatności. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków TIPS DCA i rachunków technicznych TIPS AS, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę TIPS. W zakresie, w jakim dotyczy to technicznych aspektów funkcjonowania rachunków T2S DCA, TARGET2 został techniczne stworzony i funkcjonuje w oparciu o platformę T2S.";

5) w art. 6 ust. 1 lit. a) ppkt (i) otrzymuje brzmienie:

„(i) zapewnić instalację, zarządzanie, obsługę, monitorowanie i bezpieczeństwo infrastruktury informatycznej niezbędnej do przyłączenia do platformy TIPS oraz do składania w nim zleceń płatniczych. Spełniając te wymagania, podmioty ubiegające się o rachunek TIPS DCA mogą korzystać z usług osób trzecich, ponoszą jednak wyłączną odpowiedzialność w tym zakresie. W szczególności, o ile nie korzysta się z usług podmiotu przekazującego, podmioty ubiegające się o rachunek TIPS DCA zawierają umowę z jednym lub wieloma dostawcami usług sieciowych w celu uzyskania niezbędnego połączenia oraz dostępów, zgodnie ze specyfikacjami technicznymi zawartymi w dodatku I; oraz";

6) art. 9 otrzymuje brzmienie:

„Artykuł 9

Stosunek umowny z dostawcą usług sieciowych

1. Uczestnicy mają obowiązek:

a) zawrzeć umowę z dostawcą usług sieciowych w ramach umowy dotyczącej koncesji z tym dostawcą w celu ustanowienia połączenia technicznego do systemu TARGET2-[nazwa BC/oznaczenie kraju]; albo

b) połączyć się za pośrednictwem innego podmiotu, który zawarł umowę z dostawcą usług sieciowych w ramach umowy dotyczącej koncesji z tym dostawcą.

2. Stosunek prawny między uczestnikiem a dostawcą usług sieciowych podlega wyłącznie warunkom odrębnej umowy zawartej między nimi, o której mowa w ust. 1 lit. a).

3. Usługi świadczone przez dostawcę usług sieciowych nie stanowią części usług świadczonych przez [nazwa BC] w związku z TARGET2.

4. [Nazwa BC] nie ponosi odpowiedzialności za działania, błędy czy zaniechania dostawcy usług sieciowych (w tym jego kierowników, pracowników i zleceniobiorców) ani za żadne działania, błędy czy zaniechania osób trzecich wybranych przez uczestników w celu uzyskania dostępu do sieci danego dostawcy usług sieciowych.";

7) skreśla się art. 10;

8) dodaje się art. 11a w brzmieniu:

„Artykuł 11a

Repozytorium MPL

1. Centralne repozytorium MPL zawiera tabelę mapowania proxy–IBAN na potrzeby usługi MPL.

2. Każdy adres proxy może być powiązany tylko z jednym numerem IBAN. Numer IBAN może być powiązany z jednym lub wieloma adresami proxy.

3. Do danych zawartych w repozytorium MPL stosuje się art. 29.";

9) skreśla się art. 12 ust. 9;

10) w art. 15 ust. 5 otrzymuje brzmienie:

„5. Rachunki TIPS DCA podlegają oprocentowaniu w wysokości niższej z następujących wartości: zera procent lub stopy depozytu w banku centralnym, z wyjątkiem sytuacji, w której rachunki takie są wykorzystywane w celu przechowywania rezerw obowiązkowych lub nadwyżek rezerw.

Obliczanie i wypłata oprocentowania z tytułu utrzymywanych rezerw obowiązkowych podlega przepisom rozporządzenia Rady (WE) nr 2531/98 (*) oraz rozporządzenia Europejskiego Banku Centralnego (UE) 2021/378 (EBC/2021/1) (**).

Obliczanie i wypłata oprocentowania z tytułu utrzymywanych nadwyżek rezerw podlega decyzji (UE) 2019/1743 (EBC/2019/31) (***).

_____

(*) Rozporządzenie Rady (WE) nr 2531/98 z dnia 23 listopada 1998 r. dotyczące stosowania stóp rezerw obowiązkowych przez Europejski Bank Centralny (Dz.U. L 318 z 27.11.1998, s. 1).

(**) Rozporządzenie Europejskiego Banku Centralnego (UE) nr 2021/378 z dnia 22 stycznia 2021 r. w sprawie stosowania wymogów dotyczących utrzymywania rezerwy obowiązkowej (EBC/2021/1) (Dz.U. L 73 z 3.3.2021, s. 1).

(***) Decyzja Europejskiego Banku Centralnego (UE) 2019/1743 z dnia 15 października 2019 r. w sprawie oprocentowania nadwyżek rezerw oraz niektórych depozytów (EBC/2019/31) (Dz.U. L 267 z 21.10.2019, s. 12).";

11) art. 16 otrzymuje brzmienie:

„*Artykuł 16*

Typy zleceń płatniczych na rachunkach TIPS DCA

Na potrzeby usługi TIPS za zlecenia płatnicze uznaje się:

a) zlecenia płatnicze dotyczące płatności natychmiastowej;

b) pozytywne odpowiedzi na żądanie zwrotu płatności;

c) zlecenia przekazania płynności z TIPS DCA do PM;

d) zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS; oraz

e) zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA.";

12) w art. 18 ust. 6 otrzymuje brzmienie:

„6. Po przyjęciu zlecenia przekazania płynności z TIPS DCA do PM, zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS lub zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA, zgodnie z art. 17, TARGET2-[oznaczenie BC/kraju] sprawdza, czy na rachunku płatnika dostępne są wystarczające środki. W przypadku braku wystarczających środków zlecenie przekazania płynności zostaje odrzucone. W przypadku dostępności wystarczających środków rozrachunek zlecenia przekazania płynności następuje natychmiast.";

13) w art. 20 ust. 1 lit. b) otrzymuje brzmienie:

„b) zlecenia przekazania płynności z TIPS DCA do PM, pozytywne odpowiedzi na żądanie zwrotu płatności oraz zlecenia przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS uznaje się za wprowadzone do systemu TARGET2-[oznaczenie BC/kraju] i nieodwołalne w momencie obciążenia odpowiedniego rachunku TIPS DCA. Zlecenia przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA uznaje się za wprowadzone do systemu TARGET2-[oznaczenie BC/kraju] i nieodwołalne w momencie obciążenia odpowiedniego rachunku technicznego TIPS AS.";

14) w art. 30 ust. 1 otrzymuje brzmienie:

„1. Przyjmuje się, że posiadacze rachunków TIPS DCA są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o ochronie danych, mają oni obowiązek przestrzegania takich obowiązków oraz muszą być w stanie wykazać ich przestrzeganie przed właściwymi organami. Przyjmuje się, że posiadacze rachunków TIPS DCA są świadomi wszystkich obowiązków ciążących na nich w związku z przepisami o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu, działalności łączącej się z ryzykiem rozprzestrzeniania broni jądrowej oraz rozwoju środków przenoszenia broni jądrowej. Posiadacze rachunków TIPS DCA mają obowiązek wykonywania tych obowiązków w szczególności poprzez podejmowanie odpowiednich środków dotyczących płatności obciążających lub uznających ich rachunki TIPS DCA. Przed nawiązaniem stosunku umownego z dostawcą usług sieciowych posiadacze rachunków TIPS DCA mają obowiązek upewnić się, że są im znane zasady przechowywania danych stosowane przez takiego dostawcę.";

15) dodaje się art. 35a w brzmieniu:

„*Artykuł 35a*

Przepis przejściowy

Po uruchomieniu systemu TARGET i zaprzestaniu działania systemu TARGET2 posiadacze rachunków TIPS DCA stają się posiadaczami rachunków TIPS DCA w systemie TARGET.";

16) w dodatku I tabela w pkt 2 otrzymuje brzmienie:

„Rodzaj komunikatu	Nazwa komunikatu
Pacs.002	FIToFIPayment Status Report
Pacs.004	PaymentReturn
Pacs.008	FIToFICustomerCreditTransfer
Pacs.028	FIToFIPaymentStatusRequest
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.011	ModifyLimit
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.050	LiquidityCreditTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
acmt.010	AccountRequestAcknowledgement
acmt.011	AccountRequestRejection
acmt.015	AccountExcludedMandateMaintenanceRequest
reda.016	PartyStatusAdviceV01
reda.022	PartyModificationRequestV01"

17) w dodatku I pkt 6 ppkt 1 lit. b) otrzymuje brzmienie:

„b) tryb użytkownik-aplikacja (user-to-applicaton mode – U2A)

Tryb U2A umożliwia bezpośrednią komunikację pomiędzy posiadaczem rachunku TIPS DCA a TIPS GUI. Informacje wyświetlane są w przeglądarce działającej na PC. W celu uzyskania dostępu w trybie U2A infrastruktura informatyczna musi obsługiwać pliki cookies. Dalsze szczegóły zawarte są w podręczniku użytkownika TIPS.";

18) w dodatku IV skreśla się pkt 2;

19) uchyla się dodatek V.

ZAŁĄCZNIK IV

W załączniku IV do wytycznych EBC/2012/27 wprowadza się następujące zmiany:

1) w pkt 14 ppkt 14 lit. d) otrzymuje brzmienie:

„d) zlecenia SWIFT przesyłane komunikatem MT 103 nie mogą być składane.";

2) w pkt 18 ppkt 1 lit. b) wiersz pierwszy tabeli otrzymuje brzmienie:

„Zakres	Od (mln EUR/dzień operacyjny)	Do (mln EUR/dzień operacyjny)	Opłata roczna (EUR)	Opłata miesięczna (EUR)"

3) w pkt 18 ppkt 1 lit. d) skreśla się ostatni akapit.

ZAŁĄCZNIK V

Do wytycznych EBC/2012/27 dodaje się załącznik IVa brzmieniu:

„ZAŁĄCZNIK IVa

USŁUGA TIPS DLA SYSTEMÓW ZEWNĘTRZNYCH DOKONUJĄCYCH ROZRACHUNKU PŁATNOŚCI NATYCHMIASTOWYCH

1. **Definicje**

W uzupełnieniu definicji zawartych w art. 1 załącznika IIb użyte w niniejszym załączniku terminy oznaczają:

1) »bank centralny systemu zewnętrznego« (ancillary system central bank, ASCB) – BC Eurosystemu, z którym dany system zewnętrzny dokonujący rozrachunku płatności natychmiastowych we własnych księgach zawarł porozumienie dwustronne w sprawie rozrachunku płatności natychmiastowych systemu zewnętrznego;

2) »wolumen bazowy brutto« (underlying gross volume) – liczbę płatności natychmiastowych poddanych rozrachunkowi we własnych księgach systemu zewnętrznego i zrealizowanych ze środków utrzymywanych na rachunku technicznym TIPS AS. Nie obejmuje on płatności natychmiastowych na rachunki techniczne TIPS DCA lub inne rachunki techniczne TIPS AS ani dokonywanych z takich rachunków;

3) »podmiot przekazujący« (instructing party) – podmiot, który został wskazany jako taki przez system zewnętrzny i który ma prawo wysyłać zlecenia płatnicze na platformę TIPS lub otrzymywać zlecenia płatnicze z platformy TIPS w imieniu tego systemu zewnętrznego lub podmiotu osiągalnego tego systemu zewnętrznego.

2. **Wprowadzenie zleceń płatniczych do sytemu i ich nieodwołalność**

Stosowanie postanowień art. 20 załącznika IIb w odniesieniu do chwili wprowadzenia do odpowiedniego systemu będącego komponentem systemu TARGET2 zleceń płatniczych dotyczących płatności natychmiastowych, pozytywnych odpowiedzi na żądanie zwrotu płatności, zleceń przekazania płynności z TIPS DCA na rachunek techniczny TIPS AS oraz zleceń przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA nie uchybia regulaminom systemów zewnętrznych przewidującym jako chwilę wprowadzenia poleceń przelewu do systemu lub chwilę ich nieodwołalności moment wcześniejszy niż chwila wprowadzenia odpowiedniego zlecenia płatniczego do odpowiedniego systemu będącego komponentem systemu TARGET2.

3. **Rachunki wspierające rozrachunek płatności natychmiastowych we własnych księgach systemów zewnętrznych**

1) W celu wspierania rozrachunku płatności natychmiastowych związanych z systemami zewnętrznymi w TIPS, otwiera się jeden rachunek techniczny TIPS AS.

2) Rachunek techniczny TIPS AS jest identyfikowalny za pomocą niepowtarzalnego numeru rachunku o długości do 34 znaków i ma strukturę określoną w tabeli:

	Nazwa	Format	Treść
Część A	Rodzaj rachunku	Dokładnie 1 znak	»A« dla rachunku technicznego systemu zewnętrznego
	Kod kraju banku centralnego	Dokładnie 2 znaki	Kod ISO kraju 3166-1
	Kod waluty	Dokładnie 3 znaki	EUR
Część B	Posiadacz rachunku	Dokładnie 11 znaków	BIC
Część C	Podklasyfikacja rachunku	Do 17 znaków	Dowolny tekst (alfanumeryczny) dostarczony przez posiadacza rachunku.

3) Saldo rachunków technicznych TIPS AS może w czasie dnia wynosić zero lub być dodatnie oraz może być dodatnie do następnego dnia. Saldo pozostające na rachunku do kolejnego dnia podlega zasadom w zakresie oprocentowania mającym zastosowanie do środków gwarancyjnych zgodnie z art. 11 niniejszych wytycznych.

4. **Procedura rozrachunkowa**

1) System zewnętrzny korzysta z rachunku technicznego TIPS AS do gromadzenia niezbędnej płynności przez jego członków rozliczających na potrzeby zasilenia ich pozycji.

2) Na żądanie system zewnętrzny otrzymuje informację o uznaniu i obciążeniu jego rachunku technicznego TIPS AS.

3) System zewnętrzny może wysyłać zlecenia płatnicze dotyczące płatności natychmiastowych i pozytywne odpowiedzi na żądanie zwrotu płatności do każdego posiadacza rachunku TIPS DCA lub systemu zewnętrznego TIPS. System zewnętrzny odbiera i przetwarza zlecenia płatnicze dotyczące płatności natychmiastowych, żądania zwrotu płatności i pozytywne odpowiedzi na żądanie zwrotu płatności od każdego posiadacza rachunku TIPS DCA lub systemu zewnętrznego TIPS.

5. **Interfejs użytkownika**

1) Posiadacz rachunku technicznego TIPS AS ma dostęp do platformy TIPS w trybie A2A i może również połączyć się w trybie U2A bezpośrednio lub za pośrednictwem jednego lub większej liczby podmiotów przekazujących.

2) Dostęp do platformy TIPS umożliwia posiadaczom rachunków technicznych TIPS AS:

a) dostęp do informacji dotyczących ich rachunków oraz zarządzanie limitem wykorzystania salda;

b) inicjowanie zleceń przekazania płynności z rachunku technicznego TIPS AS do TIPS DCA; oraz

c) zarządzanie określonymi danymi statycznymi.

6. **Taryfa opłat i fakturowanie**

1) System zewnętrzny w TIPS podlega łącznie:

a) opłacie za transakcje, obliczonej na tej samej podstawie, co zestawienie opłat dla posiadaczy rachunków TIPS DCA zawarte w dodatku IV do załącznika IIb;

b) opłacie opartej na wolumenie bazowym brutto płatności natychmiastowych poddawanych rozrachunkowi na własnej platformie systemu zewnętrznego i realizowanych z zasilonych wcześniej pozycji na rachunku technicznym TIPS AS. Opłata wynosi 0,0005 EUR za płatność natychmiastową.

2) Wolumen bazowy brutto płatności natychmiastowych systemu zewnętrznego jest obliczany przez bank centralny systemu zewnętrznego każdego miesiąca na podstawie wolumenu bazowego brutto w poprzednim miesiącu, zaokrąglonego w dół do najbliższych dziesięciu tysięcy i zgłoszonego przez system zewnętrzny najpóźniej do trzeciego dnia operacyjnego następnego miesiąca. Obliczony wolumen brutto stosuje się do obliczenia opłaty w następnym miesiącu.

3) Systemy zewnętrzne otrzymują od swoich banków centralnych systemów zewnętrznych faktury za poprzedni miesiąc obliczone na podstawie opłat określonych w ppkt 1 niniejszego punktu nie później niż dziewiątego dnia operacyjnego kolejnego miesiąca. Płatności realizowane są nie później niż czternastego dnia operacyjnego miesiąca, w którym wystawiona została faktura, na rachunek wskazany przez bank centralny systemu zewnętrznego, albo kwotami takich opłat obciąża się rachunek wskazany przez system zewnętrzny.

4) Do celów taryf opłat i fakturowania na podstawie niniejszego załącznika:

a) system zewnętrzny, który został wskazany jako system na mocy dyrektywy 98/26/WE, traktuje się jako oddzielny system zewnętrzny, niezależnie od tego, czy jest on prowadzony przez podmiot prawny, który jest operatorem innego systemu zewnętrznego;

b) system zewnętrzny, który nie został wskazany jako system na mocy dyrektywy 98/26/WE, traktuje się jako oddzielny system zewnętrzny, jeżeli spełnia on następujące kryteria:

(i) jest to formalne porozumienie w formie umowy lub aktu prawnego;

(ii) posiada więcej niż jednego [członka] [uczestnika] [z wyłączeniem operatora tego systemu];

(iii) jest on ustanowiony dla celów działalności polegającej na rozliczaniu, nettingu lub rozrachunku płatności lub transakcji papierami wartościowymi między uczestnikami; oraz

(iv) stosuje on wspólne zasady i standardowe umowy w odniesieniu do rozliczania, nettingu i rozrachunku płatności i papierów wartościowych między uczestnikami.

5) Opłaty do celów fakturowania na podstawie niniejszego artykułu za okres od dnia 1 grudnia 2021 r. do dnia 28 lutego 2022 r., są równe średniej całkowitej kwoty opłat uwzględnionych w fakturach za wrzesień, październik i listopad 2021 r.”.

ZAŁĄCZNIK VI

Do załącznika II do wytycznych EBC/2012/27 dodaje się dodatek VIII w brzmieniu:

„Dodatek VIII

Wymogi dotyczące zarządzania bezpieczeństwem informacji i zarządzania ciągłością działania

Zarządzanie bezpieczeństwem informacji

Niniejsze wymogi mają zastosowanie do każdego uczestnika, chyba że uczestnik wykaże, że dany wymóg nie ma do niego zastosowania. Określając zakres stosowania niniejszych wymogów w ramach swojej infrastruktury, uczestnik powinien zidentyfikować elementy wchodzące w skład łańcucha transakcji płatniczych (Payment Transaction Chain, PTC). W szczególności łańcuch transakcji płatniczych rozpoczyna się w punkcie wejścia (Point of Entry, PoE), tj. w systemie odpowiedzialnym za tworzenie transakcji (np. stacje robocze, aplikacje związane z obsługą klienta, aplikacje związane z zapleczem administracyjnym, oprogramowanie pośredniczące), a kończy się w systemie odpowiedzialnym za wysyłanie wiadomości do SWIFT (np. SWIFT VPN Box) lub do internetu (w przypadku dostępu za pośrednictwem internetu).

Wymóg 1.1: Polityka bezpieczeństwa informacji

Kadra kierownicza określa jasny kierunek polityki zgodny z celami biznesowymi oraz wykazuje wsparcie i zaangażowanie na rzecz bezpieczeństwa informacji poprzez stanowienie, zatwierdzenie i utrzymywanie polityki bezpieczeństwa informacji mającej na celu zarządzanie bezpieczeństwem informacji i odpornością cybernetyczną w całej organizacji w zakresie identyfikacji, oceny i ograniczania zagrożeń dla bezpieczeństwa informacji i cyberodporności. Polityka ta powinna obejmować co najmniej następujące sekcje: cele, zakres (w tym takie obszary jak organizacja, kadry, zarządzanie aktywami itp.) oraz zasady i podział obowiązków.

Wymóg 1.2: Organizacja wewnętrzna

W celu wdrożenia polityki bezpieczeństwa informacji w ramach organizacji należy ustanowić zasady dotyczące bezpieczeństwa informacji. Kadra kierownicza koordynuje proces ustanawiania zasad dotyczących bezpieczeństwa informacji oraz dokonuje przeglądu tego procesu w celu zapewnienia wdrożenia polityki bezpieczeństwa informacji w całej organizacji (zgodnie z wymogiem 1.1), w tym przeznaczenia na ten cel wystarczających zasobów i rozdzielenia w tym celu obowiązków w zakresie bezpieczeństwa.

Wymóg 1.3: Podmioty zewnętrzne

Bezpieczeństwo informacji i infrastruktury przetwarzania informacji w organizacji nie powinno być ograniczone przez wprowadzanie podmiotu zewnętrznego/podmiotów zewnętrznych lub dostarczanych przez nie produktów lub usług, ani też przez poleganie na takich podmiotach, produktach lub usługach. Dostęp podmiotów zewnętrznych do infrastruktury przetwarzania informacji w organizacji musi podlegać kontroli. W przypadku gdy podmioty zewnętrzne albo produkty lub usługi osób trzecich wymagają dostępu do infrastruktury przetwarzania informacji w organizacji, przeprowadza się ocenę ryzyka w celu określenia skutków dla bezpieczeństwa i wymogów w zakresie kontroli. Kontrole uzgadnia się i określa w umowie z każdym odpowiednim podmiotem zewnętrznym.

Wymóg 1.4: Zarządzanie aktywami

Wszystkie aktywa informacyjne, procesy biznesowe i bazowe systemy informacyjne, takie jak systemy operacyjne, infrastruktura, aplikacje biznesowe, gotowe produkty, usługi i aplikacje opracowane przez użytkownika, wchodzące w zakres łańcucha transakcji płatniczych, muszą być ewidencjonowane i mieć wyznaczonego właściciela. Wyznacza się podmioty odpowiedzialne za utrzymanie i funkcjonowanie odpowiednich kontroli procesów biznesowych i powiązanych komponentów informatycznych w celu zabezpieczenia zasobów informacyjnych. Uwaga: właściciel może w stosownych przypadkach zalecać prowadzenie konkretnych kontroli, ale pozostaje odpowiedzialny za właściwą ochronę aktywów.

Wymóg 1.5: Klasyfikacja aktywów informacyjnych

Aktywa informacyjne klasyfikuje się pod względem ich znaczenia dla sprawnego świadczenia usługi przez uczestnika. Klasyfikacja wskazuje potrzebę, priorytety oraz stopień ochrony wymagane przy posługiwaniu się aktywami informacyjnymi w odpowiednich procesach biznesowych, a także uwzględnia bazowe komponenty informatyczne. Schemat klasyfikacji aktywów informacyjnych zatwierdzony przez kadrę kierowniczą stosuje się w celu określenia odpowiedniego zestawu ochronnych środków kontroli przez cały cykl istnienia aktywów informacyjnych (w tym w odniesieniu do usuwania i niszczenia aktywów informacyjnych) oraz w celu informowania o potrzebie przyjęcia konkretnych sposobów postępowania.

Wymóg 1.6: Bezpieczeństwo kadrowe

Obowiązki w zakresie bezpieczeństwa określa się przed zatrudnieniem w odpowiednim opisie stanowiska pracy oraz w warunkach zatrudnienia. Wszyscy kandydaci na pracowników, wykonawcy i użytkownicy będący osobami trzecimi podlegają odpowiedniemu sprawdzeniu, zwłaszcza w przypadku stanowisk pracy o newralgicznym charakterze. Pracownicy, wykonawcy i osoby trzecie korzystające z infrastruktury przetwarzania informacji podpisują umowę dotyczącą ich roli i obowiązków w zakresie bezpieczeństwa. Zapewnia się, aby wszyscy pracownicy, wykonawcy i użytkownicy będący osobami trzecimi mieli odpowiedni poziom świadomości, a także zapewnia się im kształcenie i szkolenia w zakresie procedur bezpieczeństwa oraz właściwego korzystania z infrastruktury przetwarzania informacji w celu zminimalizowania ewentualnych zagrożeń dla bezpieczeństwa. W odniesieniu do pracowników ustanawia się formalną procedurę dyscyplinarną dotyczącą postępowania w przypadku naruszenia zasad bezpieczeństwa. Należy wprowadzić wymogi gwarantujące zarządzanie procesem odejścia z organizacji lub przeniesienia w ramach organizacji pracownika, wykonawcy lub użytkownika będącego osobą trzecią, a także zapewniające kompletny zwrot całego sprzętu i odebranie wszystkich praw dostępu.

Wymóg 1.7: Bezpieczeństwo fizyczne i środowiskowe

Infrastruktura służąca przetwarzaniu informacji krytycznych lub wrażliwych musi być zlokalizowana w strefach bezpiecznych, chronionych środkami bezpieczeństwa o określonych parametrach, z odpowiednimi zabezpieczeniami i kontrolą dostępu. Infrastruktura taka musi być fizycznie zabezpieczona przed nieuprawnionym dostępem, uszkodzeniem i nieuprawnioną ingerencją. Dostęp do niej może być przyznawany wyłącznie osobom objętych zakresem wymogu 1.6. Należy ustanowić procedury i normy w celu ochrony fizycznych nośników zawierających zasoby informacyjne w trakcie ich przenoszenia.

Sprzęt musi być chroniony przed zagrożeniami fizycznymi i środowiskowymi. Ochrona sprzętu (w tym sprzętu używanego poza obiektem) oraz ochrona przed usunięciem mienia jest konieczna w celu zmniejszenia ryzyka nieuprawnionego dostępu do informacji oraz zabezpieczenia informacji lub sprzętu przed utratą lub uszkodzeniem. Szczególne środki mogą być wymagane w celu ochrony przed zagrożeniami fizycznymi oraz zabezpieczenia urządzeń pomocniczych, takich jak infrastruktura zasilania elektrycznego i okablowanie.

Wymóg 1.8: Zarządzanie operacyjne

Ustanawia się obowiązki i procedury dotyczące zarządzania infrastrukturą przetwarzania informacji i korzystania z niej obejmujące wszystkie systemy bazowe w każdym ogniwie łańcucha transakcji płatniczych.

W odniesieniu do procedur operacyjnych, w tym technicznego zarządzania systemami informatycznymi, w stosownych przypadkach wprowadza się podział obowiązków w celu zmniejszenia ryzyka niewłaściwego wykorzystania systemu w wyniku niedbalstwa lub działania umyślnego. W przypadku gdy podział obowiązków nie może zostać wprowadzony z powodu udokumentowanych obiektywnych przyczyn, po przeprowadzeniu formalnej analizy ryzyka przeprowadza się dodatkowe kontrole. Należy wprowadzić kontrole w celu zapobiegania wprowadzaniu oraz wykrywania złośliwych kodów dla systemów w ramach łańcucha transakcji płatniczych. Należy również wprowadzić kontrole (w tym uświadamiać użytkowników) mające na celu zapobieganie złośliwym kodom, ich wykrywanie i usuwanie. Stosowane mogą być wyłącznie kody przenośne pochodzące z zaufanych źródeł (np. podpisane komponenty Microsoft COM i aplety Java). Konfiguracja przeglądarki (np. stosowanie rozszerzeń i wtyczek) podlega ścisłej kontroli.

Kadra kierownicza wdraża politykę tworzenia kopii zapasowych i odzyskiwania danych; polityka odzyskiwania danych obejmuje plan procesu przywracania danych, który podlega testowaniu w regularnych odstępach czasu, co najmniej raz w roku.

Monitoruje się systemy, które mają kluczowe znaczenie dla bezpieczeństwa płatności, a zdarzenia istotne dla bezpieczeństwa informacji są rejestrowane. W celu zapewnienia identyfikacji problemów z systemem informatycznym wykorzystuje się rejestry operatora. Rejestry operatora są poddawane regularnym przeglądom na zasadzie próby, w oparciu o znaczenie operacji. Monitorowanie systemu stosuje się w celu sprawdzania skuteczności kontroli, które zostały zidentyfikowane jako kluczowe dla bezpieczeństwa płatności, oraz w celu weryfikacji zgodności z modelem polityki dostępu.

Wymiana informacji między organizacjami opiera się na formalnej polityce wymiany informacji, odbywa się zgodnie z porozumieniami o wymianie informacji między zaangażowanymi stronami i musi być zgodna z mającymi zastosowanie przepisami prawa. Komponenty oprogramowania osób trzecich wykorzystywane do wymiany informacji z systemem TARGET2 (takie jak oprogramowanie otrzymane z biura serwisowego (Service Bureau) w scenariuszu 2 sekcji określającej zakres dokumentu zawierającego ustalenia w sprawie samocertyfikacji dotyczącej systemu TARGET2) mogą być wykorzystywane tylko na podstawie formalnej umowy z osobą trzecią.

Wymóg 1.9: Kontrola dostępu

Dostęp do aktywów informacyjnych musi być uzasadniony potrzebami biznesowymi (na zasadzie wiedzy koniecznej ([1])) oraz być zgodny z ustanowionymi ramami polityki korporacyjnej (w tym polityką bezpieczeństwa informacji). Określa się jasne zasady kontroli dostępu w oparciu o zasadę najmniejszego uprzywilejowania ([2]), w celu dokładnego odzwierciedlenia potrzeb wynikających z odpowiednich procesów biznesowych i informatycznych. W stosownych przypadkach (np. w przypadku zarządzania kopiami zapasowymi) logiczna kontrola dostępu powinna być spójna z fizyczną kontrolą dostępu, chyba że stosowane są odpowiednie kontrole dodatkowe (np. szyfrowanie, anonimizacja danych osobowych).

Należy wprowadzić formalne i udokumentowane procedury kontroli przyznawania praw dostępu do systemów i usług informatycznych, które wchodzą w zakres łańcucha transakcji płatniczych. Procedury te muszą obejmować wszystkie etapy przyznawania dostępu, od pierwszej rejestracji nowych użytkowników po końcowe wyrejestrowanie użytkowników, którym dostęp nie jest już potrzebny.

W szczególny sposób należy traktować przypadki, w których udzielane są prawa dostępu o znaczeniu na tyle krytycznym, że ich nadużycie może mieć poważny niekorzystny wpływ na działalność uczestnika (np. prawa dostępu umożliwiające administrowanie systemem, obchodzenie kontroli systemu lub bezpośredni dostęp do danych biznesowych).

Należy wprowadzić odpowiednie kontrole w celu identyfikacji, uwierzytelniania i upoważniania użytkowników w określonych punktach w ramach sieci danej organizacji, np. w odniesieniu do stacjonarnego i zdalnego dostępu do systemów w ramach łańcucha transakcji płatniczych. W celu zapewnienia możliwości pociągania do odpowiedzialności niedozwolone jest udostępnianie innym kont osobistych.

W odniesieniu do haseł ustanawia się i wdraża szczególne kontrole mające na celu zapewnienie, aby hasła nie mogły być łatwo odgadnięte, np. zasady dotyczące ich złożoności i ograniczonego okresu, przez który pozostają one ważne. Należy wprowadzić protokół bezpiecznego odzyskiwania lub resetowania hasła.

Należy opracować i wdrożyć politykę stosowania kontroli kryptograficznych w celu ochrony poufności, autentyczności i integralności informacji. Należy ustanowić politykę zarządzania kluczami w celu umożliwienia stosowania kontroli kryptograficznych.

Należy stosować zasady wyświetlania informacji poufnych na ekranie lub w druku (np. politykę „czystego ekranu" i „czysczystego biurka") w celu ograniczenia ryzyka nieuprawnionego dostępu do nich.

Należy uwzględniać ryzyko pracy w środowisku niezabezpieczonym w ramach pracy zdalnej i stosować odpowiednie kontrole techniczne i organizacyjne.

Wymóg 1.10: Zakup, rozwój i utrzymanie systemów informatycznych

Przed opracowaniem lub wdrożeniem systemów informatycznych należy określić i uzgodnić wymogi bezpieczeństwa.

W aplikacje, w tym aplikacje opracowane przez użytkowników, muszą być wbudowane odpowiednie narzędzia kontroli w celu zapewnienia prawidłowego ich stosowania. Kontrole te muszą obejmować walidację danych wejściowych, przetwarzania wewnętrznego i danych wyjściowych. Dodatkowe kontrole mogą być wymagane w przypadku systemów przetwarzających lub mających wpływ na informacje wrażliwe, informacje o dużej wartości lub informacje krytyczne. Kontrole takie określa się na podstawie wymogów bezpieczeństwa i oceny ryzyka zgodnie z ustalonymi politykami (np. polityką bezpieczeństwa informacji, polityką kontroli kryptograficznych).

([1]) Zasada wiedzy koniecznej (need-to-know principle) odnosi się do identyfikacji zbioru informacji, do których dana osoba potrzebuje mieć dostęp w celu wykonywania swoich obowiązków.

([2]) Zasada najmniejszego uprzywilejowania odnosi się do dostosowania profilu dostępu danego podmiotu do systemu informatycznego do jego roli biznesowej.

Przed akceptacją i użyciem nowych systemów należy ustanowić, udokumentować i przetestować wymogi operacyjne dla tych systemów. Należy wprowadzić odpowiednie kontrole w odniesieniu do bezpieczeństwa sieciowego, w tym segmentację i bezpieczne zarządzanie, w oparciu o stopień krytyczności przepływu danych i poziom ryzyka poszczególnych stref sieci w organizacji. Należy prowadzić specjalne kontrole w celu ochrony informacji szczególnie wrażliwych przekazywanych za pośrednictwem sieci publicznych.

Dostęp do plików systemowych i kodu źródłowego programu musi być kontrolowany, a projekty informatyczne i czynności wspierające należy prowadzić w bezpieczny sposób. Należy zachować ostrożność, aby uniknąć narażenia danych wrażliwych w środowiskach testowych. Środowisko projektowe i wspierające podlegają ścisłej kontroli. Wprowadzanie zmian w produkcji podlega ścisłej kontroli. Przeprowadza się ocenę ryzyka głównych zmian, które mają zostać wprowadzone w produkcji.

Regularne badania bezpieczeństwa systemów będących w produkcji przeprowadza się również zgodnie z wcześniej określonym planem opartym na wynikach oceny ryzyka, a testy bezpieczeństwa obejmują co najmniej oceny podatności na zagrożenia. Wszystkie kwestie problematyczne uwidocznione podczas testów bezpieczeństwa należy poddać ocenie oraz należy przygotować i regularnie monitorować plany działania mające na celu usunięcie wszelkich zidentyfikowanych luk.

Wymóg 1.11: Bezpieczeństwo informacji w relacjach z dostawcami ([3])

Aby zapewnić ochronę wewnętrznych systemów informatycznych uczestnika dostępnych dla dostawców, wymogi w zakresie bezpieczeństwa informacji służące ograniczeniu ryzyka związanego z dostępem udzielonym dostawcom muszą być udokumentowane i formalnie uzgadniane z dostawcami.

Wymóg 1.12: Zarządzanie zdarzeniami związanymi z naruszeniem bezpieczeństwa informacji i usprawnienia w tym zakresie

W celu zapewnienia spójnego i skutecznego podejścia do zarządzania zdarzeniami związanymi z naruszeniem bezpieczeństwa informacji, w tym komunikacji na temat zdarzeń i słabych punktów związanych z bezpieczeństwem, należy ustanowić i testować stanowiska, zadania i procedury, na poziomie biznesowym i technicznym, zapewniające szybką, skuteczną, uporządkowaną i bezpieczną reakcję na zdarzenia związane z naruszeniem bezpieczeństwa informacji, w tym zdarzenia, których przyczyny związane są z cyberprzestrzenią (np. oszustwa popełniane przez podmioty zewnętrzne lub działające w ramach organizacji). Personel zaangażowany w te procedury musi być odpowiednio przeszkolony.

Wymóg 1.13: Przegląd zgodności z wymogami technicznymi

Wewnętrzne systemy informatyczne uczestnika (np. systemy zaplecza administracyjnego, sieci wewnętrzne i zewnętrzne połączenia sieciowe) podlegają regularnej ocenie pod kątem zgodności z polityką ustanowioną przez organizację (np. polityką bezpieczeństwa informacji, polityką kontroli kryptograficznej).

Wymóg 1.14: Wirtualizacja

Maszyny wirtualne w roli gościa (guest virtual machines) muszą spełniać wszystkie kontrole bezpieczeństwa ustanowione dla sprzętu i systemów fizycznych (np. utwardzanie (hardening), logowanie). Procedury kontrolne dotyczące hiperwizorów muszą obejmować: hardening hiperwizora i hosting systemu operacyjnego, regularne dokonywanie poprawek (patching), ścisłe rozdzielenie różnych środowisk (np. produkcji i środowiska rozwojowego). Scentralizowane zarządzanie, logowanie i monitorowanie, a także zarządzanie prawami dostępu, w szczególności w przypadku kont uprzywilejowanych, należy wprowadzać na podstawie oceny ryzyka. Maszyny wirtualne w roli gości zarządzane przez tego samego hiperwizora muszą mieć podobny profil ryzyka.

Wymóg 1.15: Przetwarzanie w chmurze

Wykorzystanie w łańcuchu transakcji płatniczych publicznych lub hybrydowych rozwiązań związanych z przetwarzaniem w chmurze musi opierać się na formalnej ocenie ryzyka, z uwzględnieniem kontroli technicznych i klauzul umownych związanych z przetwarzaniem w chmurze.

W przypadku zastosowania hybrydowych rozwiązań przewidujących przetwarzanie w chmurze, uznaje się, że poziom krytyczności całego systemu jest taki, jak najwyższy poziom krytyczności wśród połączonych systemów. Wszystkie składniki rozwiązań hybrydowych znajdujące się na terenie obiektu muszą być oddzielone od innych systemów znajdujących się na terenie obiektu.

([3]) W bieżącym kontekście przez dostawcę należy rozumieć każdą osobę trzecią (i jej personel), którą łączy z instytucją umowa o świadczenie usług, na mocy której osobie trzeciej (i jej personelowi) przyznaje się dostęp, zdalny lub na terenie obiektu, do informacji, systemów informatycznych lub infrastruktury służącej przetwarzaniu informacji instytucji w zakresie lub w związku z zakresem wynikającym z dokonywania samocertyfikacji dotyczącej systemu TARGET2.

Zarządzanie ciągłością działania (dotyczy tylko krytycznych uczestników)

Poniższe wymogi (2.1–2.6) odnoszą się do zarządzania ciągłością działania. Każdy uczestnik TARGET2 zaklasyfikowany przez Eurosystem jako krytyczny dla sprawnego funkcjonowania systemu TARGET2 ma obowiązek posiadać strategię ciągłości działania obejmującą następujące elementy.

Wymóg 2.1: Opracowane muszą być plany ciągłości działania i wdrożone procedury ich utrzymania.

Wymóg 2.2: Dostępne musi być zastępcze miejsce prowadzenia działalności.

Wymóg 2.3: Profil ryzyka zastępczego miejsca prowadzenia działalności musi różnić się od profilu pierwotnego obiektu, aby uniknąć sytuacji, w której oba obiekty będą dotknięte tym samym zdarzeniem w tym samym czasie. Na przykład zastępcze miejsce prowadzenia działalności musi być podłączone do innej sieci elektroenergetycznej i innego centralnego obwodu telekomunikacyjnego niż obiekt pierwotny.

Wymóg 2.4: W przypadku poważnych zakłóceń operacyjnych powodujących niedostępność głównego obiektu lub kluczowego personelu, krytyczny uczestnik musi mieć możliwość wznowienia normalnej działalności z zastępczego miejsca prowadzenia działalności, gdzie musi istnieć możliwość właściwego zamknięcia dnia operacyjnego i otwarcia następnego dnia operacyjnego (następnych dni operacyjnych).

Wymóg 2.5: Wdrożone muszą być procedury zapewniające ponowne przetwarzanie transakcji z zastępczego miejsca prowadzenia działalności w rozsądnym terminie po początkowym zakłóceniu świadczenia usług i współmiernym do stopnia istotności działań, które zostały zakłócone.

Wymóg 2.6: Zdolność do przeciwdziałania skutkom zakłóceń operacyjnych musi być testowana co najmniej raz w roku, a kluczowy personel musi być odpowiednio przeszkolony. Maksymalny okres między testami nie może przekraczać roku.”

.