DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2556

z dnia 14 grudnia 2022 r.

w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 53 ust. 1 i art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Banku Centralnego ([1]),

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) Unia musi odpowiednio i kompleksowo uwzględnić ryzyko cyfrowe dla wszystkich podmiotów finansowych w związku ze wzrostem wykorzystania technologii informacyjno-komunikacyjnych (ICT) na potrzeby świadczenia usług finansowych i korzystania z takich usług, przyczyniając się tym samym do wykorzystania potencjału finansów cyfrowych pod względem zwiększenia innowacyjności i promowania konkurencji w bezpiecznym środowisku cyfrowym.

(2) W swojej codziennej działalności podmioty finansowe w dużej mierze wykorzystują technologie cyfrowe. W związku z tym kwestią najwyższej wagi jest zapewnienie odporności operacyjnej ich operacji cyfrowych na ryzyko związane z ICT. Potrzeba zapewnienia odporności operacyjnej stała się jeszcze pilniejsza ze względu na rosnącą obecność przełomowych technologii na rynku, w szczególności technologii umożliwiających cyfrowe przedstawienia wartości lub praw, które można przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii (kryptoaktywa), oraz rosnącą obecność usług związanych z takimi aktywami.

([1]) Dz.U. C 343 z 26.8.2021, s. 1.
([2]) Dz.U. C 155 z 30.4.2021, s. 38.
([3]) Stanowisko Parlamentu Europejskiego z dnia 10 listopada 2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) i decyzja Rady z dnia 28 listopada 2022 r.

(3) Na poziomie Unii wymogi dotyczące zarządzania ryzykiem związanym z ICT w sektorze finansowym są obecnie określone w dyrektywach Parlamentu Europejskiego i Rady 2009/65/WE ([4]), 2009/138/WE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) i (UE) 2016/2341 ([11]).

Wymogi te są różnorodne i czasami niekompletne. W niektórych przypadkach ryzyko związane z ICT uwzględniono wyłącznie w sposób pośredni – w ramach ryzyka operacyjnego, natomiast w innych przypadkach ryzyko takie w ogóle nie zostało uwzględnione. Problemom tym zaradzono, przyjmując rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 ([12]).Należy zatem zmienić powyższe dyrektywy w celu zapewnienia spójności z tym rozporządzeniem. W niniejszej dyrektywie przyjęto szereg zmian, które są niezbędne do zapewnienia jasności prawa i spójności w zakresie stosowania przez podmioty finansowe – upoważnione i nadzorowane zgodnie z powyższymi dyrektywami – różnych wymogów w zakresie operacyjnej odporności cyfrowej, które są konieczne do prowadzenia działalności przez te podmioty i do świadczenia usług, co gwarantuje sprawne funkcjonowanie rynku wewnętrznego. Konieczne jest zapewnienie adekwatności tych wymogów do zmian na rynku, przy jednoczesnym wspieraniu proporcjonalności, w szczególności w odniesieniu do wielkości podmiotów finansowych i szczególnych systemów, którym podlegają, w celu zmniejszenia kosztów przestrzegania przepisów.

(4) W obszarze usług bankowych w dyrektywie 2013/36/UE określa się obecnie wyłącznie ogólne zasady dotyczące zarządzania wewnętrznego i przepisy dotyczące ryzyka operacyjnego, zawierające wymogi w zakresie planów awaryjnych i planów utrzymania ciągłości działania, które w sposób pośredni służą jako podstawa do uwzględniania ryzyka związanego z ICT. Aby jednak uwzględnić ryzyko związane z ICT w sposób bezpośredni i jasny, należy zmienić wymogi dotyczące planów awaryjnych i planów utrzymania ciągłości działania w celu uwzględnienia również planów ciągłości działania oraz planów reagowania i przywracania sprawności w odniesieniu do ryzyka związanego z ICT, zgodnie z wymogami określonymi w rozporządzeniu (UE) 2022/2554. Ponadto ryzyko związane z ICT jest jedynie pośrednio uwzględniane, w ramach ryzyka operacyjnego, w procesie przeglądu i oceny nadzorczej (SREP), przeprowadzanym przez właściwe organy, a kryteria jego oceny są obecnie określone w wytycznych w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych w ramach procesu przeglądu i oceny nadzorczej (SREP), wydanych przez Europejski Urząd Nadzoru (Europejskiego Urzędu Nadzoru Bankowego) (EUNB), ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([13]). W celu zapewnienia jasności prawa i zagwarantowania, że organy nadzoru bankowego skutecznie identyfikują ryzyko związane z ICT i monitorują zarządzanie nim przez podmioty finansowe, zgodnie z nowymi ramami dotyczącymi operacyjnej odporności cyfrowej, należy

([4]) Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) (Dz.U. L 302 z 17.11.2009, s. 32).

([5]) Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010 (Dz.U. L 174 z 1.7.2011, s. 1).

([7]) Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

([8]) Dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r. ustanawiająca ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniająca dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady 2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/UE oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 190).

([9]) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).

([10]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

([11]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2341 z dnia 14 grudnia 2016 r. w sprawie działalności instytucji pracowniczych programów emerytalnych oraz nadzoru nad takimi instytucjami (IORP) (Dz.U. L 354 z 23.12.2016, s. 37).

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (zob. s. 1 niniejszego Dziennika Urzędowego).

([13]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

również zmienić zakres SREP, poprzez wyraźne odesłanie do wymogów określonych w rozporządzeniu (UE) 2022/2554 i objęcie nim w szczególności ryzyka ujawnionego w zgłoszeniach dotyczących poważnych incydentów związanych z ICT oraz w wynikach testowania operacyjnej odporności cyfrowej przeprowadzanego przez podmioty finansowe zgodnie z tym rozporządzeniem.

(5) Operacyjna odporność cyfrowa jest niezbędna do zachowania krytycznych funkcji i głównych linii biznesowych podmiotu finansowego w przypadku jego restrukturyzacji i uporządkowanej likwidacji, a tym samym uniknięcia zakłóceń w gospodarce realnej i systemie finansowym. Poważne incydenty operacyjne mogą ograniczyć zdolność podmiotu finansowego do kontynuowania działalności i mogą zagrozić realizacji celów restrukturyzacji i uporządkowanej likwidacji. Niektóre ustalenia umowne dotyczące korzystania z usług ICT mają zasadnicze znaczenie dla zapewnienia ciągłości operacyjnej i dostarczenia niezbędnych danych w przypadku restrukturyzacji i uporządkowanej likwidacji. Aby dostosować się do celów unijnych ram odporności operacyjnej, należy odpowiednio zmienić dyrektywę 2014/59/UE w celu zapewnienia, by informacje dotyczące odporności operacyjnej były uwzględniane w kontekście planowania i oceny możliwości przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji podmiotów finansowych.

(6) W dyrektywie 2014/65/UE określono bardziej rygorystyczne zasady dotyczące ryzyka związanego z ICT w odniesieniu do firm inwestycyjnych i systemów obrotu, które prowadzą handel algorytmiczny. Mniej szczegółowe wymogi mają zastosowanie do usług w zakresie udostępniania informacji i repozytoriów transakcji. Dyrektywa 2014/65/UE zawiera ponadto jedynie ograniczone odniesienia do mechanizmów kontroli i zabezpieczenia dotyczących systemów przetwarzania informacji oraz do wykorzystania odpowiednich systemów, zasobów i procedur w celu zapewnienia ciągłości i regularności świadczenia usług biznesowych. Ponadto dyrektywę tę należy dostosować do rozporządzenia (UE) 2022/2554 w odniesieniu do ciągłości i regularności świadczenia usług inwestycyjnych i prowadzenia działalności inwestycyjnych, odporności operacyjnej, zdolności systemów obrotu oraz skuteczności rozwiązań w zakresie ciągłości działania i zarządzania ryzykiem.

(7) W dyrektywie (UE) 2015/2366 określono zasady szczególne dotyczące elementów kontroli bezpieczeństwa i ograniczania ryzyka w zakresie ICT na potrzeby uzyskania zezwolenia na świadczenie usług płatniczych. Te zasady dotyczące zezwoleń należy zmienić, aby dostosować je do rozporządzenia (UE) 2022/2554. Ponadto, aby zmniejszyć obciążenia administracyjne oraz uniknąć złożoności i powielania wymogów w zakresie sprawozdawczości, zawarte w tej dyrektywie przepisy dotyczące zgłaszania incydentów powinny przestać mieć zastosowanie do dostawców usług płatniczych, którzy są uregulowani w tej dyrektywie, i którzy także podlegają rozporządzeniu (UE) 2022/2554, umożliwiając tym samym tym dostawcom usług płatniczych korzystanie z jednolitego, w pełni zharmonizowanego mechanizmu zgłaszania incydentów w odniesieniu do wszystkich incydentów operacyjnych lub incydentów w zakresie bezpieczeństwa związanych z płatnościami, niezależnie od tego, czy takie incydenty są związane z ICT.

(8) W dyrektywie 2009/138/WE i dyrektywie (UE) 2016/2341 częściowo uwzględniono ryzyko związane z ICT w przepisach ogólnych dotyczących zarządzania i zarządzania ryzykiem oraz przewidziano określenie niektórych wymogów w drodze aktów delegowanych ze szczególnym odniesieniem do ryzyka związanego z ICT albo bez takiego odniesienia. Podobnie jedynie bardzo ogólne zasady mają zastosowanie do zarządzających alternatywnymi funduszami inwestycyjnymi, którzy podlegają dyrektywie 2011/61/UE, oraz do spółek zarządzających, które podlegają dyrektywie 2009/65/WE. Dyrektywy te należy zatem dostosować do wymogów określonych w rozporządzeniu (UE) 2022/2554 w odniesieniu do zarządzania systemami i narzędziami ICT.

(9) W wielu przypadkach dodatkowe wymogi dotyczące ryzyka związanego z ICT zostały już określone w aktach delegowanych i wykonawczych przyjętych na podstawie projektów regulacyjnych standardów technicznych i projektów wykonawczych standardów technicznych opracowanych przez właściwy Europejski Urząd Nadzoru. Ponieważ przepisy rozporządzenia (UE) 2022/2554 stanowią odtąd ramy prawne dotyczące ryzyka związanego z ICT w sektorze finansowym, należy zmienić niektóre umocowania dotyczące uprawnienia do przyjmowania aktów delegowanych i wykonawczych w dyrektywach 2009/65/WE, 2009/138/WE, 2011/61/UE i 2014/65/UE w celu usunięcia przepisów dotyczących ryzyka związanego z ICT z zakresu tych umocowań.

(10) Aby zapewnić spójne wdrożenie nowych ram dotyczących operacyjnej odporności cyfrowej sektora finansowego, państwa członkowskie powinny stosować przepisy prawa krajowego transponujące niniejszą dyrektywę od dnia rozpoczęcia stosowania rozporządzenia (UE) 2022/2554.

(11) Dyrektywy 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 i (UE) 2016/2341 zostały przyjęte na podstawie art. 53 ust. 1 lub art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) lub na obu tych podstawach. Zmiany określone w niniejszej dyrektywie zostały ujęte w jednym akcie ustawodawczym ze względu na wzajemne powiązania przedmiotu i celów tych zmian. W rezultacie niniejszą dyrektywę należy przyjąć na podstawie zarówno art. 53 ust. 1, jak i art. 114 TFUE.

(12) Ponieważ cele niniejszej dyrektywy nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, ponieważ wymagają one harmonizacji wymogów już zawartych w dyrektywach, natomiast ze względu na rozmiary, jak i skutki działania możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(13) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji z dnia 28 września 2011 r. dotyczącą dokumentów wyjaśniających ([14]) państwa członkowskie zobowiązały się do złożenia, w uzasadnionych przypadkach, wraz z powiadomieniem o transpozycji, jednego lub większej liczby dokumentów wyjaśniających związki między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów transpozycyjnych. W odniesieniu do niniejszej dyrektywy prawodawca uznaje, że przekazanie takich dokumentów jest uzasadnione,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

Artykuł 1

Zmiany dyrektywy 2009/65/WE

W art. 12 dyrektywy 2009/65/WE wprowadza się następujące zmiany:

1) ust. 1 akapit drugi lit. a) otrzymuje brzmienie:

„a) stosowała racjonalne procedury administracyjne i procedury księgowe, rozwiązania w zakresie kontroli i bezpieczeństwa na potrzeby elektronicznego przetwarzania danych, w tym w odniesieniu do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*), a także odpowiednie wewnętrzne mechanizmy kontroli, w tym w szczególności zasady dotyczące osobistych transakcji dokonywanych przez jej pracowników lub utrzymania lub zarządzania inwestycjami w instrumenty finansowe w celu inwestowania na rachunek własny, zapewniając przynajmniej, aby każda transakcja, w którą zaangażowane są te UCITS, mogła być odtworzona, dostarczając informacji o jej pochodzeniu, stronach biorących w niej udział, jej charakterze oraz czasie i miejscu jej zawarcia, i aby aktywa UCITS zarządzanych przez spółkę zarządzającą były inwestowane zgodnie z regulaminami funduszy lub dokumentami założycielskimi oraz obowiązującymi przepisami prawnymi;

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L333, z 27.12.2022, s. 1).";

2) ust. 3 otrzymuje brzmienie:

„3. Bez uszczerbku dla art. 116 Komisja przyjmuje, w formie aktów delegowanych zgodnie z art. 112a, środki określające:

a) procedury i rozwiązania, o których mowa w ust. 1 akapit drugi lit. a), inne niż procedury i rozwiązania dotyczące sieci i systemów informatycznych;

b) struktury i wymogi organizacyjne w celu zminimalizowania konfliktów interesów, o których mowa w ust. 1 akapit drugi lit. b).".

([14]) Dz.U. C 369 z 17.12.2011, s. 14.

Artykuł 2

Zmiany dyrektywy 2009/138/WE

W dyrektywie 2009/138/WE wprowadza się następujące zmiany:

1) art. 41 ust. 4 otrzymuje brzmienie:

„4. Zakłady ubezpieczeń i zakłady reasekuracji podejmują rozsądne działania w celu zapewnienia ciągłości i regularności wykonywania swojej działalności, co obejmuje opracowanie planów awaryjnych. W tym celu zakład stosuje odpowiednie i współmierne systemy, zasoby i procedury oraz w szczególności ustanawia sieci i systemy informatyczne oraz zarządza nimi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

2) art. 50 ust. 1 lit. a) i b) otrzymują brzmienie:

„a) elementów systemów, o których mowa w art. 41, art. 44 – w szczególności obszarów wymienionych w art. 44 ust. 2 – oraz art. 46 i 47, innych niż elementy dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi;

b) funkcji, o których mowa w art. 44, 46, 47 i 48, innych niż funkcje dotyczące zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi.".

Artykuł 3

Zmiany dyrektywy 2011/61/UE

Art. 18 dyrektywy 2011/61/UE otrzymuje brzmienie:

„*Artykuł 18*

Zasady ogólne

1. Państwa członkowskie wymagają, aby ZAFI stale korzystali z właściwych i odpowiednich zasobów ludzkich i technicznych, które są niezbędne do właściwego zarządzania AFI.

W szczególności właściwe organy rodzimego państwa członkowskiego ZAFI, uwzględniając również charakter AFI zarządzanego przez ZAFI, wymagają, aby ZAFI stosował racjonalne procedury administracyjne i księgowe, rozwiązania w zakresie kontroli i bezpieczeństwa na potrzeby elektronicznego przetwarzania danych, w tym w odniesieniu do sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*), a także odpowiednie wewnętrzne mechanizmy kontroli, w tym w szczególności zasady dotyczące osobistych transakcji dokonywanych przez ich pracowników, lub posiadania inwestycji lub zarządzania nimi w celu inwestowania na własny rachunek, zapewniając przynajmniej, aby każda transakcja, w którą zaangażowane są AFI, mogła być odtworzona z dostarczeniem informacji o jej pochodzeniu, stronach biorących w niej udział, jej charakterze oraz czasie i miejscu jej zawarcia, oraz aby aktywa AFI zarządzanych przez ZAFI były inwestowane zgodnie z regulaminami lub dokumentami założycielskimi oraz obowiązującymi przepisami.

2. Komisja przyjmuje, w drodze aktów delegowanych zgodnie z art. 56 i z zastrzeżeniem warunków art. 57 i 58, środki określające procedury i rozwiązania, o których mowa w ust. 1 niniejszego artykułu, inne niż procedury i rozwiązania dotyczące sieci i systemów informatycznych.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).".

Artykuł 4

Zmiany dyrektywy 2013/36/UE

W dyrektywie 2013/36/UE wprowadza się następujące zmiany:

1) art. 65 ust. 3 lit. a) pkt (vi) otrzymuje brzmienie:

„(vi) osoby trzecie, którym podmioty, o których mowa w ppkt (i)–(iv), zleciły na zasadzie outsourcingu funkcje lub działalność, w tym zewnętrzni dostawcy usług ICT, o których mowa w rozdziale V rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 (*);

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

2) art. 74 ust. 1 akapit pierwszy otrzymuje brzmienie:

„Instytucje muszą posiadać solidne zasady zarządzania obejmujące jasną strukturę organizacyjną z dobrze określonymi, przejrzystymi i spójnymi zakresami odpowiedzialności, skuteczne procedury służące identyfikacji ryzyka, na które te instytucje są lub mogą być narażone, zarządzania tym ryzykiem, monitorowania i zgłaszania go, odpowiednie mechanizmy kontroli wewnętrznej obejmujące należyte procedury administracyjne i księgowe, sieci i systemy informatyczne utworzone i zarządzane zgodnie z rozporządzeniem (UE) 2022/2554 oraz politykę i praktyki wynagrodzeń zgodne z zasadami należytego i skutecznego zarządzania ryzykiem i sprzyjające takiemu zarządzaniu.";

3) art. 85 ust. 2 otrzymuje brzmienie:

„2. Właściwe organy zapewniają, by instytucje posiadały odpowiednie strategie i plany awaryjne oraz strategie i plany ciągłości działania, w tym strategie i plany na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT w odniesieniu do technologii, którą wykorzystują do przekazywania informacji, oraz by plany te były ustanawiane, zarządzane i testowane zgodnie z art. 11 rozporządzenia (UE) 2022/2554, aby instytucje te mogły nadal prowadzić działalność w przypadku poważnego zakłócenia działalności gospodarczej i ograniczyć straty ponoszone w wyniku takiego zakłócenia.";

4) w art. 97 ust. 1 dodaje się literę w brzmieniu:

„d) ryzyka ujawnione podczas testowania operacyjnej odporności cyfrowej zgodnie z rozdziałem IV rozporządzenia (UE) 2022/2554.".

Artykuł 5

Zmiany dyrektywy 2014/59/UE

W dyrektywie 2014/59/UE wprowadza się następujące zmiany:

1) w art. 10 wprowadza się następujące zmiany:

a) ust. 7 lit. c) otrzymuje brzmienie:

„c) wskazanie, w jaki sposób można w niezbędnym zakresie oddzielić prawnie i gospodarczo funkcje krytyczne i główne linie biznesowe od innych funkcji, tak aby zapewnić ciągłość i operacyjną odporność cyfrową z chwilą upadłości instytucji;";

b) ust. 7 lit. q) otrzymuje brzmienie:

„q) opis podstawowych operacji i systemów zapewniających ciągłość funkcjonowania procesów operacyjnych instytucji, w tym sieci i systemów informatycznych, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554 (*);

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

c) w ust. 9 dodaje się akapit w brzmieniu:

„Zgodnie z art. 10 rozporządzenia (UE) nr 1093/2010 EUNB prowadzi przegląd regulacyjnych standardów technicznych i w stosownych przypadkach aktualizuje je, między innymi w celu uwzględnienia przepisów rozdziału II rozporządzenia (UE) 2022/2554.";

2) w załączniku wprowadza się następujące zmiany:

a) w sekcji A pkt 16 otrzymuje brzmienie:

„16) uzgodnienia i środki niezbędne do utrzymania ciągłości funkcjonowania procedur operacyjnych instytucji, w tym sieci i systemów informatycznych utworzonych i zarządzanych zgodnie z rozporządzeniem (UE) 2022/2554;";

b) w sekcji B wprowadza się następujące zmiany:

(i) pkt 14 otrzymuje brzmienie:

„14) wskazanie właścicieli systemów wymienionych w pkt 13, związanych z nimi umów o gwarantowanym poziomie usług, a także oprogramowania i systemów lub licencji, wraz ze schematem ich przyporządkowania do poszczególnych osób prawnych oraz powiązań z ich operacjami krytycznymi i głównymi liniami biznesowymi, jak również ze wskazaniem kluczowych zewnętrznych dostawców usług ICT zdefiniowanych w art. 3 pkt 23 rozporządzenia (UE) 2022/2554;";

(ii) dodaje się punkt w brzmieniu:

„14a) wyniki testowania operacyjnej odporności cyfrowej przeprowadzanego przez instytucje na podstawie rozporządzenia (UE) 2022/2554;";

c) w sekcji C wprowadza się następujące zmiany:

(i) pkt 4) otrzymuje brzmienie:

„4) stopień, w jakim zawarte przez instytucję umowy dotyczące świadczenia usług, w tym ustalenia umowne dotyczące korzystania z usług ICT, są solidne i w pełni egzekwowalne w razie restrukturyzacji i uporządkowanej likwidacji instytucji;";

(ii) dodaje się punkt w brzmieniu:

„4a) operacyjną odporność cyfrową sieci i systemów informatycznych wspierających funkcje krytyczne i główne linie biznesowe instytucji, z uwzględnieniem zgłoszeń dotyczących poważnych incydentów związanych z ICT oraz wyników testowania operacyjnej odporności cyfrowej na podstawie rozporządzenia (UE) 2022/2554;".

Artykuł 6

Zmiany dyrektywy 2014/65/UE

W dyrektywie 2014/65/UE wprowadza się następujące zmiany:

1) w art. 16 wprowadza się następujące zmiany:

a) ust. 4 otrzymuje brzmienie:

„4. Firma inwestycyjna podejmuje rozsądne działania mające na celu zapewnienie ciągłości i regularności świadczenia usług inwestycyjnych i prowadzenia działalności inwestycyjnej. W związku z tym firma inwestycyjna wprowadza odpowiednie i proporcjonalne systemy, w tym systemy oparte na technologiach informacyjno-komunikacyjnych (ICT) ustanowione i zarządzane zgodnie z art. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 (*), a także odpowiednie i proporcjonalne zasoby i procedury.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

b) ust. 5 akapity drugi i trzeci otrzymuje brzmienie:

„Firma inwestycyjna musi posiadać należyte procedury administracyjne i rachunkowe, mechanizmy kontroli wewnętrznej i skuteczne procedury oceny ryzyka.

Bez uszczerbku dla możliwości uzyskania przez właściwe organy dostępu do komunikacji zgodnie z niniejszą dyrektywą i rozporządzeniem (UE) nr 600/2014 firma inwestycyjna musi posiadać należyte mechanizmy bezpieczeństwa służące zapewnieniu – zgodnie z wymogami określonymi w rozporządzeniu (UE) 2022/2554 – bezpieczeństwa środków przekazu informacji i ich uwierzytelnianiu, minimalizowaniu ryzyka uszkodzenia danych oraz nieuprawnionego dostępu i zapobieganiu wyciekowi informacji, zapewniając w ten sposób poufność danych przez cały czas.";

2) w art. 17 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Firma inwestycyjna prowadząca handel algorytmiczny musi posiadać skuteczne systemy i mechanizmy kontroli ryzyka odpowiednie dla prowadzonej działalności, aby zapewnić odporność i wystarczającą wydajność swoich systemów transakcyjnych zgodnie z wymogami określonymi w rozdziale II rozporządzenia (UE) 2022/2554 oraz zapewnić, aby podlegały one odpowiednim progom i limitom transakcyjnym oraz uniemożliwiały wysyłanie błędnych zleceń, a także aby nie dopuścić do sytuacji, w której sposób funkcjonowania systemu mógłby doprowadzić lub przyczynić się do powstania zaburzeń rynkowych.

Taka firma musi posiadać również skuteczne systemy i mechanizmy kontroli ryzyka, aby zapewnić uniemożliwienie wykorzystania systemów transakcyjnych do celów sprzecznych z rozporządzeniem (UE) nr 596/2014 lub regulaminem systemu obrotu, do którego jest podłączona.

Firma inwestycyjna musi posiadać skuteczne rozwiązania w zakresie ciągłości działania, aby sprostać wszelkim awariom swoich systemów transakcyjnych, w tym strategie i plany na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT ustanowione zgodnie z art. 11 rozporządzenia (UE) 2022/2554, oraz zapewnia kompleksowe testowanie i właściwe monitorowanie swoich systemów, aby zapewnić spełnianie przez nie ogólnych wymogów określonych w niniejszym ustępie oraz wszelkich wymogów szczególnych określonych w rozdziałach II i IV rozporządzenia (UE) 2022/2554.";

b) ust. 7 lit. a) otrzymuje brzmienie:

„a) szczegółowych wymogów organizacyjnych określonych w ust. 1–6, innych niż wymogi organizacyjne dotyczące zarządzania ryzykiem związanym z ICT, którym powinny podlegać firmy inwestycyjne świadczące różne usługi inwestycyjne, prowadzące różną działalność inwestycyjną, świadczące usługi dodatkowe lub ich kombinację, poprzez które szczegółowe uregulowania wymogów organizacyjnych z ust. 5 ustanawiają wymogi szczególne dla bezpośredniego dostępu do rynku oraz dla dostępu sponsorowanego w taki sposób, aby zapewnić przynajmniej równoważność kontroli stosowanych do dostępu sponsorowanego z kontrolami stosowanymi do bezpośredniego dostępu do rynku;";

3) w art. 47 ust. 1 wprowadza się następujące zmiany:

a) lit. b) otrzymuje brzmienie:

„b) odpowiednich zdolności do zarządzania ryzykiem, na które jest narażony, w tym do zarządzania ryzykiem związanym z ICT zgodnie z rozdziałem II rozporządzenia (UE) 2022/2554, do wdrażania odpowiednich mechanizmów i systemów na potrzeby ustalania istotnego ryzyka dla swojej działalności oraz wprowadzenia skutecznych środków ograniczania tego ryzyka;";

b) uchyla się lit. c);

4) w art. 48 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Państwa członkowskie wymagają, aby rynek regulowany uzyskał i utrzymywał swoją odporność operacyjną zgodnie z wymogami określonymi w rozdziale II rozporządzenia (UE) 2022/2554 zapewniającą odporność jego systemów transakcyjnych, ich wystarczającą wydajność, aby móc obsłużyć znaczny wolumen zleceń i komunikatów w szczytowych okresach, zdolność zapewnienia prawidłowego obrotu w warunkach dużych napięć rynkowych, pełne przetestowanie mające zapewnić spełnienie tych warunków, a także objęcie skutecznymi rozwiązaniami w zakresie ciągłości działania, w tym strategią i planami na rzecz ciągłości działania w zakresie ICT oraz planami reagowania i przywracania sprawności ICT ustanowionymi zgodnie z art. 11 rozporządzenia (UE) 2022/2554, celem zapewnienia ciągłości świadczenia usług w przypadku wystąpienia jakichkolwiek awarii systemów transakcyjnych.";

b) ust. 6 otrzymuje brzmienie:

„6. Państwa członkowskie wymagają, aby rynek regulowany posiadał skuteczne systemy, procedury i mechanizmy, w tym nakładające na członków lub uczestników obowiązek przeprowadzania odpowiednich testów algorytmów i zapewnienia warunków ułatwiających prowadzenie takich testów – zgodnie z wymogami określonymi w rozdziałach II i IV rozporządzenia (UE) 2022/2554 – w celu zapewnienia, aby systemy handlu algorytmicznego nie mogły doprowadzić lub przyczynić się do powstania na rynku zakłóceń obrotu oraz w celu eliminowania wszelkich warunków powodujących zakłócenia obrotu, spowodowanych takimi systemami handlu algorytmicznego, w tym systemy umożliwiające ograniczenie wielkości wskaźnika niewykonanych zleceń do liczby transakcji, które członek lub uczestnik rynku może wprowadzić do systemu, spowolnienie napływu zleceń w przypadku ryzyka osiągnięcia przez system maksymalnej wydajności oraz ograniczenie i egzekwowanie minimalnej wielkości zmiany ceny, jakiej można dokonywać na rynku.";

c) w ust. 12 wprowadza się następujące zmiany:

(i) lit. a) otrzymuje brzmienie:

„a) wymogi mające na celu zapewnienie odporności systemów transakcyjnych rynków regulowanych oraz ich odpowiedniej wydajności, z wyjątkiem wymogów związanych z operacyjną odpornością cyfrową;";

(ii) lit. g) otrzymuje brzmienie:

„g) wymogi mające zapewniać przeprowadzanie odpowiednich testów algorytmów, innych niż testowanie operacyjnej odporności cyfrowej, w celu zapewnienia, aby systemy handlu algorytmicznego obejmujące systemy handlu algorytmicznego o wysokiej częstotliwości nie mogły doprowadzić lub przyczynić się do powstania na rynku zakłóceń obrotu.".

Artykuł 7

Zmiany dyrektywy (UE) 2015/2366

W dyrektywie (UE) 2015/2366 wprowadza się następujące zmiany:

1) art. 3 lit. j) otrzymuje brzmienie:

„j) usług świadczonych przez dostawców usług technicznych, które wspierają świadczenie usług płatniczych, nie wchodząc jednak na żadnym etapie w posiadanie transferowanych środków pieniężnych; usługi te obejmują m.in. przetwarzanie i przechowywanie danych, usługi powiernicze i ochrony prywatności, uwierzytelnianie danych i podmiotów, technologie informacyjno-komunikacyjne (ICT), dostarczanie sieci informatycznych i komunikacyjnych, dostarczanie i konserwacja terminali i urządzeń wykorzystywanych na potrzeby usług płatniczych, z wyjątkiem usług inicjowania płatności i usług dostępu do informacji o rachunku;";

2) w art. 5 ust. 1 wprowadza się następujące zmiany

a) w akapicie pierwszym wprowadza się następujące zmiany:

(i) lit. e) otrzymuje brzmienie:

„e) opis stosowanych przez wnioskodawcę zasad zarządzania i mechanizmów kontroli wewnętrznej, w tym procedur administracyjnych, procedur zarządzania ryzykiem i procedur księgowych, jak również ustaleń dotyczących korzystania z usług ICT zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*), wykazujący, że te zasady zarządzania i mechanizmy kontroli wewnętrznej są proporcjonalne, właściwe, rzetelne i adekwatne;

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

(ii) lit. f) otrzymuje brzmienie:

„f) opis procedury wprowadzonej w celu monitorowania incydentów związanych z bezpieczeństwem i skarg klientów dotyczących bezpieczeństwa oraz postępowania i działań następczych w przypadku wystąpienia takich incydentów i skarg, łącznie z mechanizmem zgłaszania incydentów uwzględniającym obowiązki instytucji płatniczej dotyczące zgłaszania określone w rozdziale III rozporządzenia (UE) 2022/2554;";

(iii) lit. h) otrzymuje brzmienie:

„h) opis rozwiązań zapewniających ciągłość działania, w tym jasne określenie operacji krytycznych, skutecznej strategii i planów na rzecz ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT, a także procedury na potrzeby regularnego testowania i przeglądu adekwatności i skuteczności takich planów zgodnie z rozporządzeniem (UE) 2022/2554;";

b) akapit trzeci otrzymuje brzmienie:

„Środki kontroli bezpieczeństwa i ograniczania ryzyka, o których mowa w akapicie pierwszym lit. j), wskazują sposób zapewniania wysokiego poziomu operacyjnej odporności cyfrowej zgodnie z rozdziałem II rozporządzenia (UE) 2022/2554, w szczególności w zakresie bezpieczeństwa technicznego i ochrony danych, w tym w odniesieniu do oprogramowania i systemów ICT stosowanych przez wnioskodawcę lub przedsiębiorstwa, którym zleca on w ramach outsourcingu całość lub część swoich operacji. Środki te obejmują również środki bezpieczeństwa określone w art. 95 ust. 1 niniejszej dyrektywy. Środki te uwzględniają wytyczne EUNB dotyczące środków bezpieczeństwa, o których mowa w art. 95 ust. 3 niniejszej dyrektywy, kiedy zostaną one przyjęte.";

3) art. 19 ust. 6 akapit drugi otrzymuje brzmienie:

„Zlecanie w ramach outsourcingu ważnych funkcji operacyjnych, łącznie z systemami ICT, nie może odbywać się w sposób istotnie obniżający jakość kontroli wewnętrznej instytucji płatniczej oraz zdolność właściwych organów do monitorowania i odtworzenia przestrzegania przez instytucję płatniczą wszystkich obowiązków określonych w niniejszej dyrektywie.";

4) w art. 95 ust. 1 dodaje się akapit w brzmieniu:

„Akapit pierwszy pozostaje bez uszczerbku dla stosowania rozdziału II rozporządzenia (UE) 2022/2554 do:

a) dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. a), b) i d) niniejszej dyrektywy;

b) dostawców świadczących usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 niniejszej dyrektywy;

c) instytucji płatniczych zwolnionych zgodnie z art. 32 ust. 1 niniejszej dyrektywy; oraz

d) instytucji pieniądza elektronicznego korzystających z wyłączenia, o którym mowa w art. 9 ust. 1 dyrektywy 2009/110/WE.";

5) w art. 96 dodaje się ustęp w brzmieniu:

„7. Państwa członkowskie zapewniają, aby ust. 1–5 niniejszego artykułu nie miały zastosowania do:

a) dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. a), b) i d) niniejszej dyrektywy;

b) dostawców świadczących usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 niniejszej dyrektywy;

c) instytucji płatniczych zwolnionych zgodnie z art. 32 ust. 1 niniejszej dyrektywy; oraz

d) instytucji pieniądza elektronicznego korzystających z wyłączenia, o którym mowa w art. 9 ust. 1 dyrektywy 2009/110/WE.";

6) art. 98 ust. 5 otrzymuje brzmienie:

„5. EUNB, zgodnie z art. 10 rozporządzenia (UE) nr 1093/2010, dokonuje regularnego przeglądu i, w stosownych przypadkach, aktualizuje regulacyjne standardy techniczne w celu, między innymi, uwzględnienia innowacji i postępu technologicznego oraz przepisów rozdziału II rozporządzenia (UE) 2022/2554".

Artykuł 8

Zmiany dyrektywy (UE) 2016/2341

Art. 21 ust. 5 dyrektywy (UE) 2016/2341 otrzymuje brzmienie:

„5. Państwa członkowskie zapewniają, aby IORP podejmowały rozsądne działania w celu zapewnienia ciągłości i regularności prowadzenia swojej działalności, co obejmuje opracowanie planów awaryjnych. W tym celu IORP, w sto-

sownych przypadkach, stosują odpowiednie i współmierne systemy, zasoby i procedury oraz w szczególności ustanawiają sieci i systemy informatyczne i zarządzają nimi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).".

Artykuł 9

Transpozycja

1. Państwa członkowskie przyjmują i publikują do dnia 17 stycznia 2025 r. przepisy niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję.

Państwa członkowskie stosują te przepisy od dnia 17 stycznia 2025 r.

Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Sposoby dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji teksty najważniejszych przepisów prawa krajowego w dziedzinie objętej zakresem niniejszej dyrektywy.

Artykuł 10

Wejście w życie

Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 11

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Strasburgu dnia 14 grudnia 2022 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	M. BEK