Paweł Pelc*

# Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce

**Streszczenie**

Komisja Europejska przyjęła 24 września 2020 r. pakiet dotyczący finansów cyfrowych, w skład którego wchodzi m.in. strategię oraz szereg projektów aktów normatywnych Unii Europejskiej. W zakresie cyberbezpieczeństwa największe znaczenie ma projekt rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Ma to być element harmonizacji regulacji unijnych w tym zakresie uwzględniający także obawy związane z potencjalnym wpływem cyberataków na poszczególne instytucje finansowe mogących wpływać na zaufanie i płynność także innych instytucji finansowych w pozostałych krajach Unii Europejskiej. Dyskusji wymaga czy proponowane przez Komisję Europejską rozwiązania są rzeczywiście niezbędne zwłaszcza w odniesieniu do polskich instytucji finansowych, których działalność w dużym stopniu ma charakter lokalny a nie transgraniczny, zatem istnieje ryzyko, że poniosą koszty nowych rozwiązań, nie odnosząc korzyści związanych z ich ujednoliceniem na poziomie unijnym.

**Słowa kluczowe:** cyberbezpieczeństwo, instytucje finansowe, harmonizacja, unia bankowa

* Paweł Pelc, Akademia Sztuki Wojennej w Warszawie, Akademickie Centrum Polityki Cyberbezpieczeństwa, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

## Wstęp

Unia Europejska znacząco zwiększa poziom harmonizacji regulacji adresowanych do instytucji finansowych coraz częściej korzystając, zamiast – pozostawiających państwom członkowskim więcej swobody – dyrektyw minimalnej harmonizacji, to z dyrektyw maksymalnej harmonizacji i rozporządzeń. Jest to szczególnie widoczne w działaniach dotyczących tworzenia unii bankowej i unii rynków kapitałowych, ale nie ogranicza się tylko do tej sfery. Szczególnym przedmiotem zainteresowania regulatora unijnego jest także ochrona konsumenta m.in. w relacjach z instytucjami finansowymi[1].

Zderza się to z narastającym znaczeniem sfery szeroko rozumianych usług cyfrowych, w tym finansowych i infrastruktury cyfrowej, ale także i daleko posuniętą ochroną danych osobowych określoną w GPRD (RODO), jak i regulacjami dotyczącymi tożsamości cyfrowej (EIDAS). Elementem tej sfery regulacyjnej jest także rosnące znaczenie regulacji w zakresie cyberbezpieczeństwa.

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[2] w motywie 69 przewidywała, że „obowiązek bezpiecznego przechowywania indywidualnych danych uwierzytelniających ma ogromne znaczenie dla ochrony środków pieniężnych użytkownika usług płatniczych i dla ograniczenia ryzyk związanych z oszustwami i nieuprawnionym dostępem do rachunku płatniczego. Warunki lub inne obowiązki nakładane przez dostawców usług płatniczych na użytkowników usług płatniczych dotyczące bezpiecznego przechowywania indywidualnych danych uwierzytelniających nie powinny jednak być sformułowane w sposób, który uniemożliwia użytkownikom usług płatniczych korzystanie z usług oferowanych przez innych dostawców usług płatniczych, w tym usług inicjowania płatności i usług dostępu do informacji o rachunku. Ponadto warunki takie nie powinny zawierać żadnych postanowień, które w dowolny sposób utrudniałyby korzystanie z usług płatniczych świadczonych

**1** W chwili obecnej m.in. trwają prace związane z przeglądem i ewentualnymi modyfikacjami dyrektywy 2008/48/WE z dnia 23 kwietnia 2008 r. w sprawie umów o kredyt konsumencki (tzw. dyrektywa CCD). Por. Inception Impact Assessment Ref. Ares(2020)3256802-23/06/2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12465-Consumer-Credit-Agreement-review-of-EU-rules.

**2** Dz.U. UE L 335/35.

przez innych dostawców usług płatniczych posiadających zezwolenie lub zarejestrowanych zgodnie z niniejszą dyrektywą". W motywie 91 określała, że „dostawcy usług płatniczych są odpowiedzialni za środki bezpieczeństwa. Środki te muszą być współmierne do odnośnych ryzyk dla bezpieczeństwa. Dostawcy usług płatniczych powinni ustanowić ramy służące ograniczaniu ryzyk oraz utrzymaniu skutecznych procedur zarządzania incydentami. Należy ustanowić mechanizm regularnej sprawozdawczości w celu zapewnienia, by dostawcy usług płatniczych regularnie przekazywali właściwym organom zaktualizowane oceny ryzyk dla bezpieczeństwa, na które są narażeni, oraz informacje o środkach, które podjęli w odpowiedzi na te ryzyka. Ponadto, aby zapewnić ograniczenie do minimum szkód, na jakie narażeni są użytkownicy, inni dostawcy usług płatniczych lub systemy płatności (takich jak poważne zakłócenie funkcjonowania systemu płatności), zasadnicze znaczenie ma to, by dostawcy usług płatniczych mieli obowiązek zgłaszać bez zbędnej zwłoki poważne incydenty związane z bezpieczeństwem właściwym organom. Należy powierzyć rolę koordynacyjną EUNB".

Dyrektywa ta w art. 95 określiła sposób zarządzania ryzykami operacyjnymi oraz ryzykami dla bezpieczeństwa, w art. 96 zgłaszanie incydentów, natomiast jej art. 97 i 98 dotyczą uwierzytelniania i regulacyjnych standardów technicznych dotyczących uwierzytelniania i komunikacji. Dyrektywa do została wprowadzona do polskiego porządku prawnego przez nowelizację ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[3]. Art. 95–98 Dyrektywy zostały zaimplementowane w art. 32f–32i ustawy o usługach płatniczych.

## Pakiet dotyczący finansów cyfrowych

Dnia 24 września 2020 r. Komisja Europejska przyjęła pakiet dotyczący finansów cyfrowych obejmujący strategie w tym zakresie, płatności detalicznych oraz wnioski ustawodawcze w sprawie kryptoaktywów i odporności cyfrowej. Zdaniem Komisji Europejskiej pakiet przyczyni się do zwiększenia konkurencyjności i innowacyjności Europy w sektorze finansowym, torując jej drogę do stania się podmiotem wyznaczającym światowe standardy, ma także zapewnić konsumentom szerszą ofertę i zwiększone możliwości w zakresie usług finansowych i nowoczesnych płatności, jednocześnie gwarantując

3 T.j. Dz.U. 2020, poz. 794.

ochronę konsumentów i stabilność finansową[4]. Elementem tego pakietu jest Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24 września 2020 r. w sprawie strategii dla UE w zakresie finansów cyfrowych (COM(2020) 591 final)[5]. Zgodnie ze strategią cyfryzacja jest przyszłością finansów: konsumenci i przedsiębiorstwa w coraz większym stopniu uzyskują dostęp do usług finansowych drogą cyfrową, innowacyjni uczestnicy rynku wprowadzają nowe technologie, a istniejące modele biznesowe ulegają zmianom, a technologie cyfrowe będą miały kluczowe znaczenie dla ożywienia i modernizacji europejskiej gospodarki we wszystkich sektorach. Celem strategicznym ma być upowszechnienie finansów cyfrowych dla dobra konsumentów i przedsiębiorstw. Strategia wprowadza cztery priorytety w zakresie transformacji cyfrowej sektora finansowego UE: 1) wyeliminowanie rozdrobnienia jednolitego rynku cyfrowego usług finansowych, 2) zapewnienie, aby ramy regulacyjne UE ułatwiały innowacje cyfrowe leżące w interesie konsumentów i sprzyjające efektywności rynku, 3) stworzenie europejskiej przestrzeni danych finansowych mającej na celu promowanie innowacji na podstawie danych w oparciu o europejską strategię w zakresie danych, w tym zwiększenie dostępu do danych i ich udostępnianie w obrębie sektora finansowego oraz 4) sprostanie wyzwaniom i zagrożeniom związanym z transformacją cyfrową. W związku z powyższym Komisja Europejska zamierza dążyć m.in. do umożliwienia interoperacyjnego wykorzystania tożsamości cyfrowych w całej UE, ułatwiania zwiększania skali świadczenia cyfrowych usług finansowych na jednolitym rynku, chce się zająć kwestią kryptoaktywów i tokenizowania instrumentów finansowych, a także promować wykorzystanie infrastruktury przetwarzania w chmurze (w tym uruchomienia europejskiej platformy usług w chmurze) czy wykorzystywania narzędzi sztucznej inteligencji, a także znacznego zwiększenia dostępności informacji finansowych i regulacyjnych. Komisja zamierza doprowadzić do stosowania zasady „taka sama działalność, takie samo ryzyko, takie same przepisy". Oznacza to, że w każdym przypadku wdrożenie strategii wiązać się będzie z aktywnością regulacyjną na szczeblu europejskim, mającą na celu harmonizację rozwiązań stosowanych w poszczególnych krajach członkowskich, co zresztą Komisja Europejska wprost zapowiada w strategii, wskazując, że zamierza wprowadzić szereg istotnych środków. Komisja Europejska zachęca

**4** https://ec.europa.eu/poland/news/200924_digital_money_pl.

**5** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0591&from=EN.

także Europejskie Urzędy Nadzoru do kontynuowania i przyspieszenia ich prac w zakresie promowania współpracy i konwergencji praktyk nadzorczych. Komisja będzie także pomagała w podnoszeniu umiejętności technicznych organów nadzoru, utworzy także nową unijną platformę finansów cyfrowych.

Elementem proponowanych przez Komisję Europejską działań jest m.in. ogłoszony równolegle z nią wniosek z 24 września 2020 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937 (COM(2020) 593 final 2020/0265(COD)[6], który, zgodnie z uzasadnieniem Komisji Europejskiej obejmuje kryptoaktywa nieobjęte obowiązującymi unijnymi przepisami dotyczącymi usług finansowych, a także tokeny będące pieniądzem elektronicznym, ma cztery ogólne i powiązane cele. Pierwszy cel dotyczy pewności prawa. Aby rynek kryptoaktywów mógł się rozwijać w UE, konieczne jest zapewnienie solidnych ram prawnych jasno określających, w jaki sposób w świetle regulacji traktowane są wszystkie kryptoaktywa nieobjęte obowiązującymi przepisami dotyczącymi usług finansowych. Drugim celem jest wspieranie innowacyjności. Promowanie rozwoju kryptoaktywów i powszechniejszego wykorzystania technologii rozproszonego rejestru wymaga wprowadzenia bezpiecznych i proporcjonalnych ram wspierających innowacyjność i uczciwą konkurencję. Trzeci cel polega na zapewnieniu odpowiedniego poziomu ochrony konsumentów i inwestorów oraz integralności rynku, biorąc pod uwagę, że kryptoaktywa nieobjęte obowiązującymi przepisami dotyczącymi usług finansowych stwarzają w znacznym stopniu podobne ryzyko, co bardziej znane instrumenty finansowe. Czwartym celem jest zapewnienie stabilności finansowej. Kryptoaktywa stale ewoluują. Choć niektóre z nich mają dość ograniczony zakres i zastosowanie, inne, takie jak powstająca kategoria stabilnych kryptowalut, mają potencjał, by stać się powszechnie akceptowanymi instrumentami o charakterze systemowym. Wniosek zawiera w ocenie Komisji Europejskiej zabezpieczenia mające na celu przeciwdziałanie potencjalnym zagrożeniom dla stabilności finansowej i uporządkowanej polityki pieniężnej, jakie mogą się pojawić w związku ze stabilnymi kryptowalutami[7]. Ze względu na specyfikę materii objętej wnioskiem oraz ograniczenia związane z wdrażanymi rozwiązaniami, wydaje się, że ich wpływ na funkcjonowanie instytucji finansowych w Polsce w krótkiej perspektywie powinien być ograniczony, nie koncentruje

**6** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

**7** Por. Kontekst wniosku.

się on na kwestiach cyberbezpieczeństwa, a raczej konstrukcji poszczególnych regulowanych instrumentów. Równie ograniczony wpływ na polski rynek prawdopodobnie będzie miał wniosek Komisji Europejskiej z 24 września 2020 r. w sprawie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru (COM(2020) 594 final 2020/0267(COD)[8].

Pakiet uzupełnia także wniosek Komisji Europejskiej z 24 września 2020 r. w sprawie Dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy 2006/43/WE[9], 2009/65/WE[10], 2009/138/WE[11], 2011/61/UE[12], 2013/36/UE[13], 2014/65/UE[14], (UE) 2015/2366[15] i (UE) 2016/2341[16] (COM(2020) 596 final, 2020/0268(COD)[17]. Komisja Europejska uważa, że zaproponowany przez nią

**8** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0594&from=EN.

**9** Dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca dyrektywę Rady 84/253/EWG, Dz.U. L 157 z 9.6.2006, s. 87.

**10** 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.

**11** 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.

**12** 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.

**13** 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 i firmami inwestycyjnymi, 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.

**14** 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.

**15** 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.

**16** 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.

**17** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0596&from=EN.

projekt dyrektywy zawiera zestaw zmian, które wydają się niezbędne do zapewnienia jasności prawa i spójności w zakresie sposobu, w jaki podmioty finansowe – upoważnione i nadzorowane zgodnie ze zmienianymi dyrektywami – stosują poszczególne wymogi w zakresie operacyjnej odporności cyfrowej, które są konieczne do prowadzenia działalności przez te podmioty, co gwarantuje sprawne funkcjonowanie rynku wewnętrznego[18]. Transpozycja powinna nastąpić w ciągu roku od dnia przyjęcia projektu dyrektywy[19]. Zmiany te jednak będą miały znacznie bardziej ograniczony charakter niż wynikające z omówionego kluczowego w tym zestawie projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego, który zasługuje na odrębne omówienie.

## DORA

Wydaje się, że znacznie większy wpływ na funkcjonowanie instytucji finansowych w Polsce będzie miał kolejny z ogłoszonych wraz ze strategią wniosków – wniosek z 24 września 2020 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (COM(2020) 595 final, 2020/0266(COD)[20] (DORA).

DORA jest szczególnie interesująca w kontekście niniejszych rozważań dlatego, że wprost i w szerokim zakresie dotyczy właśnie kwestii cyberbezpieczeństwa instytucji finansowych. W ocenie Komisji Europejskiej konieczne jest wprowadzenie szczegółowych i kompleksowych ram operacyjnej odporności cyfrowej dla unijnych podmiotów finansowych. Ramy te mają wzmocnić wymiar jednolitego zbioru przepisów dotyczących zarządzania ryzykiem cyfrowym. W szczególności przyczynią się one do wzmocnienia i usprawnienia procesu zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi, wprowadzenia dokładnych testów systemów technologii informacyjno-komunikacyjnych, zwiększenia świadomości organów nadzoru na temat ryzyka w cyberprzestrzeni oraz incydentów związanych z technologiami informacyjno-komunikacyjnymi, w obliczu których stają podmioty

**18** Motyw 3 wniosku.
**19** Art. 9 ust. 1 wniosku.
**20** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0595&from=EN.

finansowe, a także wprowadzenia uprawnień dla organów nadzoru finansowego w zakresie nadzorowania ryzyka wynikającego z zależności podmiotów finansowych od zewnętrznych dostawców usług technologii informacyjno-komunikacyjnych. We wniosku Komisja Europejska przewiduje stworzenie spójnego mechanizmu zgłaszania incydentów, który, jej zdaniem, przyczyni się do zmniejszenia obciążeń administracyjnych ciążących na podmiotach finansowych oraz wzmocni skuteczność nadzoru[21]. W motywie 28 do wniosku wskazano, że „brakuje jednorodności i spójności w zakresie ryzyka związanego z zewnętrznymi dostawcami usług ICT oraz zależnością od zewnętrznych dostawców usług ICT. Pomimo pewnych starań na rzecz uwzględnienia obszaru outsourcingu, między innymi w postaci zaleceń z 2017 r. w sprawie outsourcingu zlecanego dostawcom usług w chmurze. 34, kwestii ryzyka systemowego, które może powstać w wyniku kontaktu sektora finansowego z ograniczoną liczbą kluczowych zewnętrznych dostawców usług ICT, poświęcono w unijnych przepisach niewielką uwagę. Ten brak odniesienia do tej kwestii na szczeblu unijnym jest spotęgowany brakiem konkretnych kompetencji i narzędzi umożliwiających krajowym organom nadzoru osiągnięcie właściwego zrozumienia zależności od zewnętrznych dostawców usług ICT i odpowiednie monitorowanie zagrożeń wynikających z koncentracji takich zależności od zewnętrznych dostawców usług ICT”[22]. Wniosek wprowadza definicję operacyjnej odporności cyfrowej, która oznacza zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej integralności operacyjnej z technologicznego punktu widzenia przez zapewnianie, bezpośrednio albo pośrednio (korzystając z usług zewnętrznych dostawców usług ICT), pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość[23]. Rozporządzenie ma nakładać na podmioty finansowe obowiązek posiadania wewnętrznych ram zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z wykorzystaniem technologii informacyjno-komunikacyjnych[24]. Proponowane rozwiązania wymagać będą zarówno rozbudowy infrastruktury technicznej i informatycznej, jak

**21** Por. Kontekst wniosku.
**22** https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0595&from=EN.
**23** Art. 3 pkt 1 wniosku.
**24** Art. 4 ust. 1 wniosku.

i procedur wewnętrznych podmiotów finansowych. Istotnym elementem projektowanej regulacji są także mechanizmy związane ze zgłaszaniem incydentów związanych z technologią informacyjno-komunikacyjną oraz związanych z testowaniem operacyjnej odporności cyfrowej i zarządzaniem ryzykiem ze strony zewnętrznych dostawców usług informacyjno-komunikacyjnych. W ciągu pięciu lat od dnia wejścia w życie projektowanego rozporządzenia Komisja Europejska będzie mogła wydawać akty delegowane. Rozporządzenie będzie miało bardzo szeroki zakres stosowania, bo będzie miało zastosowanie do następujących podmiotów finansowych: 1) instytucji kredytowych; 2) instytucji płatniczych; 3) instytucji pieniądza elektronicznego; 4) firm inwestycyjnych; 5) dostawców usług w zakresie kryptoaktywów, emitentów kryptoaktywów, emitentów tokenów powiązanych z aktywami oraz emitentów znaczących tokenów powiązanych z aktywami; 6) centralnych depozytów papierów wartościowych; 7) kontrahentów centralnych; 8) systemów obrotu; 9) repozytoriów transakcji; 10) zarządzających alternatywnymi funduszami inwestycyjnymi; 11) spółek zarządzających; 12) dostawców usług w zakresie udostępniania informacji; 13) zakładów ubezpieczeń i zakładów reasekuracji; 14) pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające; 15) instytucji pracowniczych programów emerytalnych; 16) agencji ratingowych; 17) biegłych rewidentów i firm audytorskich; 18) administratorów kluczowych wskaźników referencyjnych; 19) dostawców usług finansowania społecznościowego; 20) repozytoriów sekurytyzacji; 21) zewnętrznych dostawców usług ICT[25].

## DORA a otoczenie regulacyjne polskich instytucji finansowych

W 2020 r. podmioty nadzorowane przez KNF obowiązane były do dostosowania się do tzw. komunikatu chmurowego wydanego w Polsce przez KNF. Po wejściu w życie projektowanego rozporządzenia niezbędne będzie dostosowanie ich działalności także w zakresie korzystania z przetwarzania danych w chmurze do nowych rozwiązań unijnych. To samo dotyczyć będzie kwestii uregulowanych obecnie w innych rekomendacjach KNF (w tym bankowej

25 Art. 2 wniosku.

rekomendacji D[26] czy rekomendacji D-SKOK[27]). Wdrażanie proponowanych przez Komisję Europejską rozwiązań wiązać się będzie z koniecznością poniesienia dodatkowych kosztów przez podmioty finansowe w rozumieniu projektowanego rozporządzenia, ale także do dostosowania do tych regulacji praktyk nadzorczych Komisji Nadzoru Finansowego. Wszystkie te działania będą musiały być prowadzone w sytuacji niskich stóp procentowych, rosnących kosztów regulacyjnych i związanych z ochroną konsumentów (w tym związanych z orzeczeniami TSUE dotyczącymi tzw. kredytów frankowych – tzw. duże TSUE[28] oraz zwrotu opłat w przypadku wcześniejszej spłaty kredytu – tzw. małe TSUE[29]). Dodatkowo projekt rozporządzenia jedynie w ograniczonym zakresie realizuje zasadę proporcjonalności[30]. Jest to szczególnie istotne w przypadku podmiotów nieprowadzących w istotnym zakresie działalności transgranicznej, gdyż nie odniosą korzyści związanych z harmonizacja regulacji w tym zakresie na szczeblu unijnym, za to poniosą koszty tej harmonizacji związane z wdrożeniem rozwiązań przewidzianych w projekcie rozporządzenia i zastąpienia nimi dotychczas stosowanych zgodnie z regulacjami krajowymi rozwiązań.

## Zakończenie

Komisja Europejska w uzasadnieniu nie wskazała w sposób przekonujący dlaczego rozwiązania krajowe oparte na dyrektywach w sprawie minimalnej harmonizacji lub rozporządzeniach opartych na zasadach są mniej skuteczne w zapewnieniu operacyjnej odporności cyfrowej. Nieprzekonujący jest także

**26** Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa, styczeń 2013 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.

**27** Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych, Warszawa, sierpień 2016 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Reko_SKOK_D_47953.pdf.

**28** Wyrok Trybunału Sprawiedliwości UE z 3 października 2019 r. w sprawie o sygn.akt C-260/18, https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A1125D505F11AEA0BA83B34687757F8?text =&docid=221367&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=247910.

**29** Wyrok Trybunału Sprawiedliwości UE z dnia 11 września 2019 roku wydany w sprawie o sygn. akt C-383/18 https://curia.europa.eu/juris/document/document.jsf?text=&docid=217625&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=247910.

**30** Por. art. 3 pkt 50.

argument o transgranicznym charakterze ryzyka związanego z technologiami informacyjno-komunikacyjnymi, gdyż ryzyko to nie jest także ograniczone do terytorium państw członkowskich, a za licznymi atakami stoją aktorzy spoza terytorium państw członkowskich Unii Europejskiej (odpowiedzialność za ataki, za którymi mają stać aktorzy państwowi przypisywana jest m.in. hakerom z Federacji Rosyjskiej, Chin czy Korei Północnej). Wydaje się zaś, że dla promowania konwergencji podejść nadzorczych do ryzyka ze strony zewnętrznych dostawców usług informatyczno-komunikacyjnych konstrukcja rozporządzenia jest nadmiarowa i w tym zakresie wystarczyłaby forma dyrektywy. Zapewne dalszych analiz, szczególnie w odniesieniu do państw spoza strefy euro, wymaga także teza Europejskiej Rady ds. Ryzyka Systemowego przytoczona w tezie 3 projektu rozporządzenia, zgodnie z którą naruszania związane z technologiami informacyjno-komunikacyjnymi zwiększają ryzyko rozpowszechnienia lokalnych słabych stron we wszystkich kanałach transmisji finansowej oraz potencjalnie wywołują niekorzystne konsekwencje dla stabilności unijnego systemu finansowego, powodując utratę płynności i ogólną utratę pewności i zaufania w odniesieniu do rynków finansowych[31]. Tymczasem autorzy tego raportu Europejskiej Rady ds. Ryzyka Systemowego wyraźnie wskazali w nim, że ryzyko to oparte zostało na analizie hipotetycznych scenariuszy w braku historycznych precedensów[32].

Z tych przyczyn należy uznać, że w pakiecie rozwiązań przedstawionych przez Komisję Europejską 24 września 2020 r. kluczowe znaczenie będzie miał projekt DORA, zatem niewątpliwie wymaga on szczególnych analiz i uwagi w toku prac nad nim, ze względu na jego fundamentalne znaczenie dla funkcjonowania podmiotów finansowych w zakresie szeroko rozumianego cyberbezpieczeństwa.

**31** European Systemic Risk Board. Systemic cyber risk. February 2020.

**32** „In the absence of historical precedents, the ESRB has examined whether, and if so how, a cyber incident could cause a systemic crisis. To this end, the ESRB's European Systemic Cyber Group developed a conceptual framework and applied it to a range of historical and hypothetical scenarios. The aim of the analysis was to explore how, in certain circumstances, a cyber incident could lead to a systemic crisis, defined as "disruption in the financial system with the potential to have serious negative consequences for the internal market and the real economy". This report explored how a cyber incident could create widespread disruption in the financial system, s. 40.

## Bibliografia

Cyfryzacja to przyszłość finansów, https://ec.europa.eu/poland/news/200924_digital_money_pl.

Inception Impact Assessment Ref. Ares(2020)3256802-23/06/2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12465-Consumer-Credit-Agreement-review-of-EU-rules.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24 września 2020 w sprawie strategii dla UE w zakresie finansów cyfrowych (COM(2020) 591 final), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0591&from=EN.

Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa, styczeń 2013 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.

Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych, Warszawa, sierpień 2016 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Reko_SKOK_D_47953.pdf.

Wniosek Komisji Europejskiej z 24 września 2020 r. dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (COM(2020) 595 final, 2020/0266(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0595&from=EN.

Wniosek Komisji Europejskiej z 24 września 2020 dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937 (COM(2020) 593 final 2020/0265(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

Wniosek Komisji Europejskiej z 24 września 2020 r. w sprawie Dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy 2006/43/WE, 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 i (UE) 2016/2341 (COM(2020) 596 final, 2020/0268(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0596&from=EN.

Wniosek Komisji Europejskiej z 24 września 2020 r. w sprawie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru (COM(2020) 594 final 2020/0267(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0594&from=EN.

Wyrok Trybunału Sprawiedliwości UE z dnia 11 września 2019 roku wydany w sprawie o sygn. akt C-383/18, https://curia.europa.eu/juris/document/document.jsf?text=&docid=217625&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=247910.

Wyrok Trybunału Sprawiedliwości UE z dnia 3 października 2019 r. w sprawie o sygn.akt C-260/18, https://curia.europa.eu/juris/document/document.jsf;jsessionid=0A1125D505F11AEA0BA83B34687757F8?text=&docid=221367&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=247910.

# Impact of planned EU actions and regulations on financial institutions in Poland

**Abstract**

On 24 September 2020, the European Commission adopted the Digital Finance Package, which includes inter alia strategy and a number of draft legislative acts of the European Union. In the area of cybersecurity, the draft regulation on the operational resilience of the digital financial sector (DORA) is of the greatest importance. This is to be part of the harmonisation of EU regulations in this area, also taking into account concerns about the potential impact of cyber-attacks on individual financial institutions that could affect the confidence and liquidity of other financial institutions in the rest of the European Union. The discussion requires whether the solutions proposed by the European Commission are indeed necessary, in particular for Polish financial institutions, whose activities are largely local rather than cross-border, so there is a risk that they will incurred the costs of new solutions without benefiting from their harmonisation at European Union level.

Key words: cybersecurity, financial institutions, harmonisation, banking union