

Bruksela, 11 marca 2026 r.
(OR. en)

7240/26

EF 66
ECOFIN 329
FSC 6
ESMA
ESRB
ECB
EIOPA
SRB
EBA

PISMO PRZEWODNIE

Od: Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)

Do: Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej

Nr dok. Kom.: COM(2026) 119 final

Dotyczy: SPRAWOZDANIE KOMISJI DLA RADY I PARLAMENTU
EUROPEJSKIEGO
na temat gotowości sektora finansowego UE

Delegacje otrzymują w załączeniu dokument COM(2026) 119 final.

Załącznik: COM(2026) 119 final



Bruksela, dnia 10.3.2026 r.
COM(2026) 119 final

SPRAWOZDANIE KOMISJI DLA RADY I PARLAMENTU EUROPEJSKIEGO

na temat gotowości sektora finansowego UE

1. Wprowadzenie

Unia Europejska stoi w obliczu rosnącego ryzyka i bezprecedensowych zagrożeń w wielu sektorach. Zagrożenia te obejmują zwiększoną niepewność, napięcia i konflikty geopolityczne, ryzyko w cyberprzestrzeni i ryzyko związane z manipulacją informacjami, a także zmianę klimatu i rosnące ryzyko zagrożeń naturalnych. Aby zwiększyć zdolność UE do przewidywania tych zagrożeń, zapobiegania im i reagowania na nie, 26 marca 2025 r. Komisja i Europejska Służba Działań Zewnętrznych (ESDZ) wspólnie przedstawiły strategię na rzecz unii gotowości¹. Kluczową rolę w utrzymaniu niezbędnych funkcji społecznych w każdych okolicznościach odgrywa sektor finansowy UE. Dlatego też w ramach strategii na rzecz unii gotowości i realizując działanie nr 25 określone w załączniku do wspólnego komunikatu, Komisja przeprowadza kompleksową ocenę poziomu gotowości w sektorze finansowym. W szczególności ocenia się zdolność sektora do zapewnienia ciągłości funkcji krytycznych, takich jak dokonywanie płatności i finansowanie gospodarki, w każdych okolicznościach.

Unijne przepisy dotyczące usług finansowych opierają się na solidnej tradycji, którą cechują ostrożność, rozwaga, odporność i zdolność przewidywania. Cele są jasne: zapewnienie stabilności finansowej, zorganizowanego procesu restrukturyzacji i uporządkowanej likwidacji wszelkich instytucji finansowych będących na progu upadłości, zarządzania w sytuacji kryzysowej i gwarantowania depozytów, ochrony inwestorów i integralności rynku. W następstwie wielkiego kryzysu finansowego, który rozpoczął się w 2007 r., UE dokonała kompleksowej przebudowy swoich norm ostrożnościowych i struktury nadzoru bankowego. Reformy te wzmocniły instytucje finansowe i rynki kapitałowe w UE oraz dostawców infrastruktury rynku finansowego w Unii.

Obecnie sektor finansowy UE osiągnął wysoki poziom odporności dzięki konsolidacji trzech filarów: (i) kapitału opartego na analizie ryzyka w przypadku banków i instytucji finansowych, (ii) wymogów w zakresie zarządzania i przejrzystości oraz (iii) mechanizmów współpracy w zakresie nadzoru między państwami członkowskimi i między poszczególnymi segmentami sektora. UE wprowadziła polityki i zasady, które zapewniają ciągłą ocenę ryzyka wystąpienia zdarzeń ekstremalnych w ramach oceny ryzyka operacyjnego oraz w ramach planów utrzymania ciągłości działania i planów awaryjnych.

W ostatnich latach ramy UE zostały poddane próbie w związku z kilkoma sytuacjami kryzysowymi, takimi jak pandemia COVID-19, rosyjska agresja na Ukrainę, amerykański kryzys związany z bankami regionalnymi i kryzys związany z Credit Suisse w 2023 r., przerwy w dostawie energii elektrycznej, cyberataki i incydenty hybrydowe. W obliczu tych kryzysów sektor finansowy UE wykazał solidność i odporność. Organy na szczeblu unijnym i krajowym podejmowały szybkie i skuteczne działania.

Ogólnie rzecz biorąc, gotowość nie jest stanem statycznym, lecz dynamicznym i perspektywicznym. Wymaga ciągłego cyklu planowania, szkolenia, wyposażania, testowania, oceny i doskonalenia. Wymaga ona skupienia uwagi na gotowości do radzenia sobie ze wszystkimi zagrożeniami przez przewidywanie ryzyka, rozwijanie zdolności, koordynację

¹ Komisja i ESDZ wydały [wspólny komunikat](#) w sprawie [strategii na rzecz unii gotowości](#).

między sektorami (rządowym, prywatnym, publicznym) i wyciąganie wniosków z przeszłych wydarzeń w celu budowania odpornych społeczności, które mogą zapobiegać sytuacjom kryzysowym, chronić się przed nimi i przewycięzać ich skutki. Dotyczy to również sektora finansowego.

Niniejsze sprawozdanie zawiera przegląd obecnego stanu gotowości sektora finansowego UE dokonany na podstawie stałych dyskusji z Europejskim Bankiem Centralnym, Europejskimi Urzędami Nadzoru, Europejską Radą ds. Ryzyka Systemowego, Jednolitą Radą ds. Restrukturyzacji i Uporządkowanej Likwidacji, państwami członkowskimi i sektorem usług finansowych.

2. Gotowość na jednolitym rynku europejskim

Na szczeblu UE gotowość w sektorze finansowym poprawiła się w ciągu ostatnich kilku lat dzięki środkom ustawodawczym i utworzeniu struktur zarządzania na szczeblu UE, które odzwierciedlają transgraniczny charakter sektora finansowego UE. Zarządzanie opiera się na dwóch filarach: przepisach UE i organach UE. Strukturę tę uzupełnia zestaw środków podjętych na poziomie strefy euro, na szczeblu regionalnym (z udziałem kilku państw członkowskich) i na szczeblu państw członkowskich.

2.1 Przepisy UE regulujące sektor finansowy

Sektor finansowy jest regulowany zarówno przepisami sektorowymi, jak i przekrojowymi.

Przepisy sektorowe

Przepisy sektorowe obejmują dyrektywę i rozporządzenie w sprawie wymogów kapitałowych (CRD/CRR)², dyrektywę Wypłacalność II³, dyrektywę w sprawie rynków instrumentów finansowych II (MiFID II)⁴, rozporządzenie w sprawie infrastruktury rynku europejskiego (EMIR)⁵ oraz rozporządzenie w sprawie rozrachunku papierów wartościowych i centralnych depozytów papierów wartościowych (CDPW)⁶. W tych aktach prawnych wprowadzono

² 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 (CRD);

rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych oraz zmieniające rozporządzenie (UE) nr 648/2012 (CRR).

³ Tekst skonsolidowany: 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).

⁴ 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 (MiFID II).

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (EMIR).

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych

wymogi ostrożnościowe służące zapewnieniu odporności, stabilności oraz należytego funkcjonowania instytucji finansowych, infrastruktury finansowej i systemu finansowego.

Jeśli chodzi o gotowość, w kilku aktach prawnych dotyczących poszczególnych sektorów określono wymogi regulujące zarządzanie ryzykiem operacyjnym, odporność operacyjną, odporność ICT, ciągłość działania i zarządzanie kryzysowe. Na przykład w sektorze bankowym CRR/CRD, dyrektywa w sprawie naprawy oraz restrukturyzacji i uporządkowanej likwidacji banków⁷, rozporządzenie w sprawie jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji (rozporządzenie SRMR)⁸ oraz dyrektywa w sprawie systemów gwarancji depozytów⁹ zapewniają osiągnięcie przez banki odporności na szeroki zakres potencjalnych zagrożeń, w tym zdarzenia ekstremalne. Oczekuje się, że banki wdrożą solidne ramy zarządzania i ramy zarządzania ryzykiem, w tym udoskonalone plany ciągłości działania, komunikacji i naprawy, aby skutecznie przeciwdziałać szerokiemu zakresowi ryzyka. Do kluczowych cech środków uwzględniających scenariusze ryzyka, zarówno ostrożnościowych, jak i reaktywnych, należą szczególne wymogi *ex ante* dla banków, takie jak plany naprawy i plany restrukturyzacji i uporządkowanej likwidacji, zgodnie z wymogami rozporządzenia w sprawie jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji oraz dyrektywy w sprawie naprawy oraz restrukturyzacji i uporządkowanej likwidacji banków.

Oprócz banków również zakłady ubezpieczeń, których funkcjonowanie regulują przepisy dyrektywy Wyplacalność II, firmy inwestycyjne, których funkcjonowanie regulują przepisy MiFID II, oraz infrastruktury rynkowe, takie jak kontrahenci centralni (CCP) i centralne depozyty papierów wartościowych, podlegają podobnym wymogom w zakresie zapewnienia odporności operacyjnej, ryzyka związanego z ICT, ciągłości działania i zarządzania kryzysowego. W razie potrzeby uzupełnieniem tych wymogów są wymogi dotyczące usprawnienia planowania naprawy oraz restrukturyzacji i uporządkowanej likwidacji. Zarządzanie aktywami i pozabankowe pośrednictwo finansowe podlegają również szerokim i coraz bardziej kompleksowym ramom regulacyjnym UE, w tym dyrektywie w sprawie przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe, dyrektywie dotyczącej zarządzających alternatywnymi funduszami inwestycyjnymi oraz rozporządzeniu w sprawie funduszy rynku pieniężnego. Instrumenty te nakładają wymogi dotyczące zarządzania ryzykiem, zarządzania płynnością, dźwigni finansowej, wyceny i przejrzystości,

depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012.

⁷ 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 (dyrektywa w sprawie naprawy oraz restrukturyzacji i uporządkowanej likwidacji banków).

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 806/2014 z dnia 15 lipca 2014 r. ustanawiające jednolite zasady i jednolitą procedurę restrukturyzacji i uporządkowanej likwidacji instytucji kredytowych i niektórych firm inwestycyjnych w ramach jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji oraz jednolitego funduszu restrukturyzacji i uporządkowanej likwidacji oraz zmieniające rozporządzenie (UE) nr 1093/2010 (rozporządzenie SRMR).

⁹ Dyrektywa Parlamentu Europejskiego i Rady 2014/49/UE z dnia 16 kwietnia 2014 r. w sprawie systemów gwarancji depozytów (dyrektywa w sprawie systemów gwarancji depozytów).

aby wspierać stabilność sektora. Działania na rzecz rozwoju unii oszczędności i inwestycji przez budowanie zdolności sektora finansowego UE do łączenia oszczędności z produktywnymi inwestycjami, a tym samym ulepszenie podziału ryzyka i dywersyfikacji w całym sektorze finansowym UE, przyczynią się do poprawy jego ogólnej odporności i gotowości.

Europejski Bank Centralny (EBC) – jednolity organ nadzoru dla dużych banków w 21 państwach członkowskich – oraz właściwe organy krajowe w strefie euro i poza nią stawiają odporność finansową i operacyjną banków w centrum swoich priorytetów nadzorczych. Banki zachęca się w szczególności do należytego uwzględnienia ryzyka geopolitycznego i włączenia go do swoich procesów zarządzania ryzykiem. W tym kontekście powinny one wziąć pod uwagę ekspozycje wobec kontrahentów w państwach niebędących członkami UE, potencjalny wpływ sankcji zagranicznych na ekspozycje oraz zależności od zewnętrznych dostawców usług i infrastruktury. Banki powinny ponadto opracować solidne ramy zarządzania i ochrony w odniesieniu do cyberzagrożeń i innych zagrożeń, które mogą mieć wpływ na ich odporność operacyjną. Obejmuje to środki mające na celu zwiększenie bezpieczeństwa i ochronę przed szkodami fizycznymi. Poza środkami specyficznymi dla danej instytucji unijne ramy ostrożnościowe dla banków odnoszą się również do szerszych kanałów ryzyka ogólnosystemowego i transgranicznego.

Ramy zarządzania kryzysowego zapewniają zestaw narzędzi, z którego można korzystać w przypadku zagrożenia rentowności dostawcy funkcji krytycznej. Zmienione ramy zarządzania kryzysowego i gwarantowania depozytów dla banków stanowią ważny krok w kierunku jeszcze większej skuteczności unijnego systemu zarządzania kryzysowego, w szczególności w odniesieniu do mniejszych i średnich banków; porozumienie polityczne w sprawie tych ram osiągnięto w czerwcu 2025 r.

Ważnym aspektem gotowości w sektorze finansowym jest zapewnienie wszystkim użytkownikom dostępu do instrumentów płatniczych, tj. do płatności zarówno gotówkowych, jak i elektronicznych. Aby zagwarantować dostępność **gotówki** w każdych okolicznościach, kluczowym środkiem na poziomie Eurosystemu jest utrzymywanie wspólnych zapasów strategicznych banknotów euro. EBC jest centralnym organem koordynującym i decyzyjnym oraz prowadzi okresowe ćwiczenia w zakresie zarządzania kryzysowego, w tym potencjalnej komunikacji kryzysowej. Na szczeblu krajowym krajowe banki centralne utrzymują plany ciągłości działania, aby zapewnić dostępność wypłat gotówki i depozytów.

Jednocześnie wniosek dotyczący statusu banknotów i monet euro jako prawnego środka płatniczego, przedstawiony przez Komisję 28 czerwca 2023 r., zmierza do tego, aby gotówka euro pozostała powszechnie akceptowana do celów płatności i łatwo dostępna dla obywateli, przedsiębiorstw i podmiotów publicznych w całej strefie euro. Wymogi dotyczące utrzymania w normalnych warunkach sprawnej infrastruktury wykorzystywanej w obsłudze gotówki wspierają dostępność gotówki w sytuacjach awaryjnych. Wniosek Komisji nie zawierał przepisu dotyczącego odporności, ale Rada dodała go w swoim mandacie negocjacyjnym i wymaga on od państw członkowskich posiadania planu odporności w odniesieniu do gotówki lub połączenia równoważnych środków.

Ponadto trzecia dyrektywa w sprawie usług płatniczych (PSD3), w sprawie której osiągnięto porozumienie polityczne w listopadzie 2025 r., ma na celu zwiększenie dostępu do gotówki w sklepach przez umożliwienie sprzedawcom detalicznym oferowania wypłat gotówki bez zakupu (w postaci tzw. cash-in-shops), do określonego limitu. Ułatwia to korzystanie z gotówki, zwłaszcza na obszarach wiejskich, dzięki doprecyzowaniu przepisów dla sprzedawców detalicznych i operatorów bankomatów.

Oprócz dostępności gotówki kluczowe znaczenie ma utrzymanie ciągłości **usług płatniczych**, w tym płatności kartą, płatności opartych na przelewach między rachunkami (w tym za pośrednictwem telefonów komórkowych), dostępu do rachunków płatniczych i możliwości składania depozytów, aby w przypadku rozległych zakłóceń utrzymać zaufanie publiczne do systemu finansowego i porządek publiczny oraz zapewnić podstawowe funkcjonowanie gospodarki dzięki zapewnieniu społeczeństwu stałego dostępu do podstawowych usług.

Obecna druga dyrektywa w sprawie usług płatniczych reguluje inne aspekty, w tym zarządzanie ryzykiem operacyjnym i ryzykiem dla bezpieczeństwa oraz zgłaszanie poważnych incydentów. Celem jest zwiększenie bezpieczeństwa i odporności systemów płatniczych w całej UE.

Bezpieczeństwo i skuteczność systemów płatniczych są wspierane przez Eurosystem. Za jego pośrednictwem wprowadzono wymogi nadzorcze uwzględniające kluczowe scenariusze ryzyka określone w odniesieniu do europejskiego ekosystemu płatności. Ramy te ustanawiają kompleksowy zestaw wymogów dotyczących zarządzania ryzykiem operacyjnym. Obejmują one środki na potrzeby zarządzania ciągłością działania i terminowego przywracania sprawności, a także przepisy szczegółowe dotyczące bezpieczeństwa informacji, cyberodporności, bezpieczeństwa fizycznego, outsourcingu, zarządzania ryzykiem informatycznym i innych powiązanych obszarów. Ramy te obejmują elektroniczne instrumenty płatnicze (takie jak karty, polecenia zapłaty, polecenia przelewu, pieniądź elektroniczny i cyfrowe portfele), a także systemy (np. sieci kart) i aplikacje (np. portfele elektroniczne), które umożliwiają korzystanie z tych instrumentów.

Aby zapewnić większą ochronę, w art. 15 rozporządzenia EBC w sprawie systemów płatności o znaczeniu systemowym (SIPS) określono dodatkowe wymogi. Na przykład wymaga się w nim, aby systemy zapewniały przywrócenie sprawności w ciągu dwóch godzin (w tym przez wykorzystanie lokalizacji zapasowych) oraz aby operatorzy SIPS byli w stanie zakończyć rozrachunek wszystkich należnych płatności w danym dniu do końca dnia roboczego, w którym doszło do incydentu.

Projekt stworzenia cyfrowego euro – cyfrowej formy gotówki, uzupełniającej fizyczną gotówkę i prywatne rozwiązania płatnicze – zapewniłby społeczeństwu dodatkową metodę płatności, a jednocześnie sprzyjałby włączeniu cyfrowemu i finansowemu. Cyfrowe euro, jako pierwszy ujednoczony ogólnoeuropejski system płatności, pomogłoby również chronić międzynarodową rolę euro. Dzięki wzmocnieniu otwartej strategicznej autonomii UE i rozszerzeniu zakresu dostępnych instrumentów płatniczych projekt cyfrowego euro ma na celu dalsze wzmocnienie ogólnej odporności usług płatniczych. Jeżeli chodzi o wniosek dotyczący prawnego środka płatniczego, Rada dodała dodatkowe przepisy, aby jeszcze

bardziej zwiększyć odporność cyfrowego euro. W tym kontekście europejskie portfele tożsamości cyfrowej będą interoperacyjne z interfejsami użytkownika cyfrowego euro, co zapewni bezpieczne i płynne uwierzytelnianie użytkownika¹⁰.

Międzysektorowe przepisy w sektorze finansowym

Uzupełnieniem wyżej wymienionych przepisów finansowych jest akt w sprawie operacyjnej odporności cyfrowej (DORA), który jest aktem prawnym dotyczącym sektora finansowego i ma zastosowanie do całego sektora finansowego UE. Obejmuje on 20 różnych rodzajów podmiotów finansowych, w tym instytucje kredytowe, dostawców usług płatniczych, infrastruktury rynku finansowego, zakłady ubezpieczeń, agencje ratingowe i podmioty zarządzające aktywami.

DORA kładzie duży nacisk na odporność podmiotów finansowych, ich poziom gotowości do przetrwania potencjalnych zakłóceń w dziedzinie ICT oraz na zarządzanie ryzykiem wynikającym z zależności podmiotów finansowych od zewnętrznych dostawców usług ICT, w tym ryzykiem systemowym i ryzykiem koncentracji stwarzanym przez dostawców ICT, którzy mają kluczowe znaczenie dla sektora finansowego UE. DORA ustanawia zharmonizowane i solidne ramy służące wzmocnieniu zdolności sektora finansowego UE do zapobiegania zakłóceniom związanym z ICT, przetrwania ich, reagowania na nie i odzyskiwania sprawności po ich wystąpieniu. Podmioty finansowe muszą wprowadzić kompleksowe ramy zarządzania ryzykiem związanym z ICT, obejmujące zarządzanie, ewidencję aktywów, identyfikację ryzyka, ochronę, wykrywanie, reagowanie, przywracanie sprawności i ciągłe ulepszanie. Zapewnia to proaktywne zarządzanie słabymi punktami oraz odpornością systemów i procesów. Podmioty finansowe są również zobowiązane do wykrywania, klasyfikowania i zgłaszania właściwym organom poważnych incydentów związanych z ICT z zastosowaniem uzgodnionych definicji, progów i terminów, aby umożliwić skoordynowane reagowanie we wszystkich jurysdykcjach. Wymaga to regularnego testowania i oceny ich procesów, narzędzi i ustaleń w zakresie odporności i gotowości.

Podmioty finansowe muszą również zarządzać ryzykiem związanym z korzystaniem z usług zewnętrznych dostawców usług ICT, w szczególności kluczowych zewnętrznych dostawców usług ICT. W DORA zobowiązano podmioty finansowe do przeprowadzania badania due diligence w odniesieniu do ryzyka koncentracji przed zawarciem nowych umów z zewnętrznymi dostawcami usług ICT. DORA przewiduje mechanizm nadzoru, w ramach którego trzy Europejskie Urzędy Nadzoru (EUN)¹¹ nadzorują kluczowych zewnętrznych dostawców usług ICT na skalę ogólnoeuropejską, co zwiększa ogólną operacyjną odporność cyfrową w całym sektorze finansowym UE. W listopadzie 2025 r. Europejskie Urzędy

¹⁰ Europejskie ramy tożsamości cyfrowej ustanawiają bezpieczny i godny zaufania ekosystem cyfrowej identyfikacji i uwierzytelniania oraz wykorzystywania dowodów cyfrowych, który będzie dostępny dla wszystkich obywateli UE do końca 2026 r. Europejskie portfele tożsamości cyfrowej będą bezpośrednio sprzyjać odporności i gotowości sektora finansowego UE na wypadek kryzysu oraz chronić przed oszustwami i kradzieżą tożsamości w płatnościach, onboardingu klientów i innych usługach finansowych.

¹¹ Te trzy Europejskie Urzędy Nadzoru to Europejski Urząd Nadzoru Bankowego (EUNB), Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA) oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA).

Nadzoru opublikowały wykaz wyznaczonych kluczowych zewnętrznych dostawców usług ICT na podstawie DORA. Ramy DORA są szczególnie dobrze dostosowane do zarządzania cyberbezpieczeństwem, łącznością, gotowością i ryzykiem operacyjnym o istotnym wymiarze międzynarodowym.

Poza DORA, stanowiącym *lex specialis* w odniesieniu do sektora finansowego, sektor finansowy jest również objęty horyzontalnymi porozumieniami o współpracy w zakresie odporności fizycznej i cyfrowej na podstawie dyrektywy w sprawie odporności podmiotów krytycznych (CER)¹² i dyrektywy NIS 2.

Dyrektywa CER tworzy nadrzędne ramy dotyczące odporności podmiotów krytycznych na wszystkie zagrożenia. Zobowiązano w niej wyznaczone podmioty krytyczne do przeprowadzania ocen ryzyka, opracowywania krajowych strategii i wprowadzania konkretnych środków w zakresie odporności, aby zapewnić im możliwość dalszego pełnienia niezbędnych funkcji społecznych. Chociaż w dyrektywie tej uwzględniono sektor bankowy i infrastruktury rynku finansowego jako sektory krytyczne, sektor finansowy nie wchodzi w zakres wszystkich istotnych wymogów rozporządzenia CER, ponieważ jest objęty znacznie bardziej szczegółowymi wymogami wynikającymi z rozporządzenia DORA. Niemniej jednak sektor finansowy jest objęty zakresem dyrektywy CER w odniesieniu do horyzontalnych porozumień o współpracy.

Dyrektywa NIS 2 zapewnia szersze ramy cyberbezpieczeństwa w różnych sektorach krytycznych. DORA uznaje się za *lex specialis* w stosunku do dyrektywy NIS 2, co oznacza, że wymogi dotyczące zarządzania ryzykiem i zgłaszania incydentów określone w DORA mają zastosowanie jako sektorowy akt prawny Unii zamiast dyrektywy NIS 2. Jak poinformowała Komisja w swoich wytycznych dotyczących stosowania art. 4 ust. 1 i 2 dyrektywy NIS 2¹³, nadal mają zastosowanie niektóre przepisy określone w dyrektywie NIS 2, które mają zasadnicze znaczenie dla zapewnienia gotowości i osiągnięcia wysokiego poziomu odporności podmiotów finansowych, w tym wymogi dotyczące przyjęcia strategii cyberbezpieczeństwa i ustanowienia krajowych ram zarządzania cyberkryzysami (z obowiązkiem wyznaczenia organów ds. zarządzania cyberkryzysami oraz przyjęcia krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę), obejmujących sektory bankowości i infrastruktury rynku finansowego. Ponadto zespoły reagowania na incydenty bezpieczeństwa komputerowego („CSIRT”) i europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe”) powinny wykonywać swoje zadania w odniesieniu do sektorów bankowości i infrastruktur rynku finansowego.

Środki gotowości określone dla sektora finansowego mają na celu zrównoważenie potrzeby odporności z zasadą proporcjonalności. Wymogi regulacyjne i nadzorcze są dostosowane do wielkości, złożoności i systemowego znaczenia instytucji, aby uniknąć nakładania nieproporcjonalnych obciążeń na mniejsze podmioty. Aby uniknąć niepotrzebnych obciążeń

¹² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. W art. 5 ust. 5 dyrektywy przewidziano, że Komisja – we współpracy z państwami członkowskimi – opracowuje dobrowolny wspólny formularz sprawozdawczy do celów wykonania art. 5 ust. 4 dyrektywy.

¹³ C(2023)6068.

administracyjnych, zharmonizowane ramy, takie jak DORA, usprawniają wymogi w całym sektorze, co zapewnia spójność przy jednoczesnym ograniczeniu powielania działań.

2.2 Organy UE: narzędzia i współpraca

Organom UE powierza się specjalne narzędzia, które można uruchomić w sytuacjach nadzwyczajnych i które utrzymują ustalenia dotyczące gotowości w celu zapewnienia ciągłości działania. Na przykład trzem Europejskim Urzędem Nadzoru przyznano uprawnienia nadzwyczajne w ustanawiających je rozporządzeniach. Po formalnym stwierdzeniu istnienia sytuacji nadzwyczajnej przez Radę (jak przewidziano w art. 18 rozporządzeń dotyczących Europejskich Urzędów Nadzoru) mogą one na podstawie art. 9 tymczasowo ograniczyć działalność finansową w drodze indywidualnych decyzji. Pełnią one również ogólną funkcję koordynacyjną pomiędzy organami krajowymi oraz w ramach Europejskiego Systemu Nadzoru Finansowego (ESNF) (art. 31).

Jak wspomniano powyżej, EBC jest jednolitym organem nadzoru dla banków w 21 państwach członkowskich uczestniczących w Jednolitym Mechanizmie Nadzorczym i zapewnia spójny nadzór ostrożnościowy na całym obszarze. Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji jest dla tych państw członkowskich jedynym organem ds. restrukturyzacji i uporządkowanej likwidacji odpowiedzialnym za restrukturyzację i uporządkowaną likwidację upadających banków, a tym samym za ochronę stabilności finansowej i minimalizację kosztów ponoszonych przez podatników.

Aby zwiększyć odporność operacyjną, wszystkie organy UE opracowały wewnętrzne procedury zapewniające ciągłość działania, gotowość i zarządzanie incydentami krytycznymi w sytuacji różnych zagrożeń. Regularnie testują one te środki, aby zapewnić ciągłość działania i określić najpilniejsze procesy biznesowe, które należy przeprowadzić w sytuacji nadzwyczajnej, a także poziom, na jakim należy to uczynić.

Biorąc pod uwagę potrzebę zachowania integralności i prawidłowego funkcjonowania jednolitego rynku oraz wysoki stopień wzajemnych powiązań i ryzyko skutków ubocznych w sektorze finansowym UE, koordynacja między różnymi organami UE i zaangażowanie państw członkowskich ma zasadnicze znaczenie dla przewidywania kryzysów i zarządzania kryzysami, które mogą mieć wpływ na wiele części UE jednocześnie. Zaangażowanie na wczesnym etapie i szybka współpraca mają decydujące znaczenie zarówno na etapie planowania, jak i na każdym etapie kryzysu. Aby ułatwić współpracę i wymianę informacji, które mogą być istotne również w sytuacji kryzysowej, kilka organów UE zastosowało instrumenty współpracy między sobą lub z właściwymi organami krajowymi bądź krajowymi organami ds. restrukturyzacji i uporządkowanej likwidacji, lub zawarło protokoły ustaleń (np. protokół ustaleń między EBC a Jednolitą Radą ds. Restrukturyzacji i Uporządkowanej Likwidacji), a także przeprowadza symulacje w celu zapewnienia odpowiedniej gotowości na sytuacje kryzysowe.

Ważnym kamieniem milowym w tych pracach są unijne ramy koordynacji w odniesieniu do cyberincydentów o charakterze systemowym (EU-SCICF), ustanowione w styczniu 2025 r.

przez Europejskie Urzędy Nadzoru. Ramy te stanowią strategiczną podstawę współpracy podczas poważnych incydentów cyberbezpieczeństwa¹⁴. Ich celem jest ułatwienie szybkiej wymiany informacji i wspólnego reagowania przez wprowadzenie protokołów oceny i ograniczania zagrożeń we wszystkich państwach członkowskich UE.

Ponadto w czerwcu 2025 r. Rada przyjęła Plan działania UE na rzecz zarządzania cyberkryzysami¹⁵ jako ważny przewodnik dla państw członkowskich służący zwiększeniu ich gotowości oraz zdolności wykrywania incydentów cyberbezpieczeństwa i reagowania na nie, oparty na wszystkich odpowiednich mechanizmach, w tym mechanizmach utworzonych na mocy dyrektywy NIS 2, DORA (EU-SCICF) i aktu w sprawie cybersolidarności.

W tych ramach można przeprowadzać regularne ćwiczenia, aby utrzymać solidność i skuteczność gotowości i zdolności reagowania. Ponadto na szczęblu międzynarodowym protokół G-7 dotyczący reagowania na incydenty cyberbezpieczeństwa ma na celu ujednoczenie globalnych działań w zakresie reagowania na zagrożenia cyberbezpieczeństwa dotyczące sektora finansowego oraz zapewnienie terminowego i skoordynowanego reagowania we wszystkich jurysdykcjach.

Każdy organ UE przeprowadza regularne oceny ryzyka i stosuje inne środki w celu zidentyfikowania najistotniejszych rodzajów ryzyka w odniesieniu do swojego mandatu i swoich funkcji. Oceny ryzyka przeprowadza się we współpracy z organami krajowymi, co przyczynia się do wypracowania wspólnego i bardziej dogłębnego zrozumienia krajobrazu ryzyka i zagrożeń, które należy traktować priorytetowo. Oceny ryzyka często uwzględnia się w systemach wczesnego ostrzegania, które z kolei stanowią część ram gotowości organów UE. Ponadto istniejące ustalenia regulacyjne i nadzorcze między organami UE a zainteresowanymi stronami z sektora prywatnego umożliwiają stały dialog na temat wzajemnych oczekiwań co do gotowości¹⁶.

2.3 Ramy na szczęblu krajowym i regionalnym

Poza przepisami na szczęblu UE państwa członkowskie opracowały własne krajowe programy gotowości¹⁷. Programy te zazwyczaj wykraczają poza sektor finansowy i obejmują gotowość społeczeństwa jako całości na szczęblu krajowym. Z tego powodu programy krajowe różnią się w poszczególnych państwach członkowskich, co odzwierciedla różne krajowe struktury rządowe i administracyjne oraz zakres kompetencji. Jednocześnie te programy krajowe funkcjonują w spójnych ramach UE i w coraz większym stopniu współdziałają z ustaleniami na szczęblu UE i mechanizmami koordynacji transgranicznej.

¹⁴ EU-SCICF wdraża również art. 49 DORA w celu poprawy koordynacji z innymi ramami kryzysowymi UE.

¹⁵ Zalecenie Rady z dnia 6 czerwca 2025 r. w sprawie Planu działania UE na rzecz zarządzania cyberkryzysami (Dz.U. C, C/2025/3445, 20.6.2025, <http://data.europa.eu/eli/C/2025/3445/oj>).

¹⁶ W strategii UE na rzecz unii gotowości uznano znaczenie takich partnerstw. Działania kluczowe nr 36 i 37 mają na celu ustanowienie publiczno-prywatnej grupy zadaniowej ds. gotowości oraz opracowanie publiczno-prywatnych protokołów na wypadek sytuacji wyjątkowych we wszystkich sektorach.

¹⁷ W ramach prac nad realizacją mandatu objętego działaniem nr 25 przedstawionym w załączniku do wspólnego komunikatu w sprawie strategii na rzecz unii gotowości Komisja wykorzystała również trwające dyskusje z państwami członkowskimi na temat programów gotowości.

Gotowość sektora finansowego jest zawsze kluczowym elementem krajowych strategii gotowości. Sektor ten odgrywa wiodącą rolę w zakresie gotowości i jest przykładem dla innych sektorów. Krajowe strategie gotowości dla sektora finansowego wykraczają poza dorobek UE i koncentrują się na krajowych kwestiach operacyjnych. Różnice między krajowymi systemami finansowymi (np. główne cechy krajowego sektora bankowego, zakres wykorzystania gotówki, przyjęcie euro, uczestnictwo w unii bankowej) znajdują naturalne odzwierciedlenie w sposobie oceny i zapewnienia krajowego poziomu gotowości sektora finansowego.

Biorąc pod uwagę kluczową rolę odgrywaną przez organy publiczne, zwłaszcza w przypadku kryzysu lub poważnego incydentu, wiarygodne funkcje krótkoterminowego finansowania muszą pozostać dostępne, aby uniknąć niedoborów płynności lub finansowania na poziomie państwa i sektora publicznego w szerszym ujęciu oraz aby uniknąć szerszych skutków dla społeczeństwa pod względem zaufania publicznego i stabilności finansowej. Nie dotyczy to jednak w ten sam sposób wszystkich ram kryzysowych: w szczególności restrukturyzacja i uporządkowana likwidacja banków ma na celu ograniczenie zależności od środków publicznych przez umorzenie lub konwersję długu oraz mechanizmy restrukturyzacji i uporządkowanej likwidacji finansowane przez branżę.

Aby zapewnić odporność funkcji rządów w zakresie krótkoterminowego finansowania, krajowe urzędy ds. zarządzania długiem opracowały plany awaryjne i plany ciągłości działania, aby mogły nadal funkcjonować również w przypadku kryzysu. Uzupełnieniem tych środków jest coraz częstsza wymiana najlepszych praktyk i koordynacja zarówno na szczeblu UE, jak i na szczeblu regionalnym.

Ponadto Europejski Mechanizm Stabilności (EMS) oferuje szereg instrumentów pomocy finansowej mających na celu ochronę stabilności finansowej przez udzielanie pomocy członkom EMS, aby zwiększyć zdolność strefy euro do radzenia sobie z kryzysem zadłużenia publicznego i trudnościami finansowymi banków. Instrumenty te mają na celu zaradzenie kryzysom systemowym oraz uzupełnienie krajowej i unijnej gotowości operacyjnej w przypadku bardziej realnych scenariuszy zakłóceń. Niektóre państwa członkowskie opracowały porozumienia dwustronne w celu zapewnienia dostępności krótkoterminowego finansowania w razie niedostępności którejkolwiek z podstawowych funkcji krajowych urzędów ds. zarządzania długiem. Sfinalizowanie oczekiwanej zmiany Porozumienia ustanawiającego EMS jeszcze bardziej wzmocniłoby sieć bezpieczeństwa strefy euro.

Równolegle istnieją regionalne fora koordynacyjne, takie jak mechanizm współpracy nordycko-bałtyckiej – ważna inicjatywa regionalna skoncentrowana na krajach nadbałtyckie. Fora te wspierają współpracę w dziedzinie nadzoru finansowego i zarządzania kryzysowego, wymianę informacji na temat ocen ryzyka i planowanie strategiczne. Pokazują one, w jaki sposób współpraca regionalna może zwiększyć gotowość.

Kilka państw członkowskich utworzyło specjalne prywatno-publiczne partnerstwa lub fora w kontekście krajowych programów gotowości (obejmujące przedstawicieli sektora prywatnego z kilku branż).

Ogólnie rzecz biorąc, te ustalenia na szczeblu unijnym, regionalnym i krajowym stanowią część wielopoziomowych ram gotowości, w których koordynację i współpracę na szczeblu unijnym i regionalnym uzupełniają działania krajowe.

3. Testy warunków skrajnych

Jak uznano w zaleceniu Rady w sprawie wzmocnienia odporności infrastruktury krytycznej¹⁸, kluczowym aspektem gotowości są testy warunków skrajnych. W sektorze finansowym testy warunków skrajnych stanowią już integralną i zasadniczą część nadzoru nad instytucjami finansowymi i dostawcami infrastruktury rynku finansowego. Testy warunków skrajnych zwiększają gotowość sektora finansowego przez symulację poważnych kryzysów (takich jak recesje, wstrząsy klimatyczne lub cyberataki) w celu wykrycia niedoborów kapitału i płynności instytucji finansowych. Zmusza to instytucje i dostawców do poprawy zarządzania ryzykiem, podniesienia buforów kapitałowych, udoskonalenia planowania strategicznego i budowania odporności na przyszłe wstrząsy, a przez to zwiększa ogólną stabilność finansową i buduje zaufanie rynku.

Testy warunków skrajnych wspierają również gotowość dzięki uchwyceniu ogólnosystemowych i transgranicznych kanałów ryzyka, w tym źródeł globalnej niestabilności finansowej, napięć geopolitycznych, incydentów cyberbezpieczeństwa i zakłóceń w funkcjonowaniu infrastruktury krytycznej.

W **systemie bankowym** do inicjowania i koordynowania ogólnounijnych testów warunków skrajnych dla sektora bankowego jest upoważniony Europejski Urząd Nadzoru Bankowego (EUNB). Na podstawie tego upoważnienia EUNB przeprowadza co dwa lata ogólnounijny test warunków skrajnych obejmujący około 75 % sektora bankowego. W dyrektywie w sprawie wymogów kapitałowych upoważniono również właściwe organy do przeprowadzania w miarę potrzeb, jednak co najmniej raz do roku, nadzorczych testów warunków skrajnych w instytucjach, które organy te nadzorują. Ponadto EUNB wydał wytyczne, by zagwarantować stosowanie przez organy wspólnych metod podczas przeprowadzania corocznych nadzorczych testów warunków skrajnych.

W ramach unii bankowej testy warunków skrajnych, analizy scenariuszy i symulacje na potrzeby przeglądu i oceny nadzorczej regularnie przeprowadza EBC. EBC wykonuje też ukierunkowane przeglądy ustaleń dotyczących cyberodporności i outsourcingu.

W sektorze **ubezpieczeń i instytucji pracowniczych programów emerytalnych** ogólnounijne testy warunków skrajnych dla zakładów ubezpieczeń i zakładów reasekuracji oraz dla instytucji pracowniczych programów emerytalnych (IORP)¹⁹ przeprowadza regularnie

¹⁸ Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej (2023/C 20/01).

¹⁹ W kilku państwach członkowskich instytucje pracowniczych programów emerytalnych nie są objęte zakresem dyrektywy IORP II i w związku z tym nie są regulowane przepisami UE. Takie fundusze emerytalne nie podlegają testom warunków skrajnych przeprowadzanym przez EIOPA.

co trzy lata EIOPA; obejmują one element ryzyka w cyberprzestrzeni i element ryzyka związanego z klimatem.

Regularne ogólnounijne testy warunków skrajnych odporności CCP przeprowadza Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) w ramach ocen przewidzianych w art. 32 rozporządzenia w sprawie ESMA i art. 24a EMIR. Chociaż testy te koncentrują się na odporności CCP na niekorzystne zmiany na rynku, ESMA uwzględnia również inne rodzaje zagrożeń zewnętrznych.

Scenariusze niekorzystne na potrzeby testów warunków skrajnych przeprowadzanych przez EUNB (banki), EIOPA (ubezpieczenia, fundusze emerytalne) i ESMA (CCP) opracowuje Europejska Rada ds. Ryzyka Systemowego (ERRS).

Dyrektywa 2014/49/UE w sprawie systemów gwarancji depozytów nakłada na państwa członkowskie obowiązek wykonywania wynikających z niej zadań. Wyniki przeprowadzanych w tym kontekście testów są następnie wykorzystywane przez EUNB do przeprowadzania wzajemnych ocen w celu zbadania odporności systemów gwarancji depozytów.

4. Perspektywy

Sektor finansowy UE opiera się na solidnych i wielowymiarowych ramach gotowości. Ramy te składają się ze szczegółowych przepisów sektorowych, przepisów przekrojowych oraz mechanizmów współpracy między poszczególnymi segmentami sektora i między państwami członkowskimi. Gotowość sektora finansowego UE ma również wymiar zewnętrzny, dzięki któremu UE wzmacnia nie tylko jego stabilność finansową, ale także jego rolę jako wiarygodnego i niezawodnego sektora finansowego na szczeblu globalnym.

Sektor finansowy UE dowiódł swojej odporności podczas poprzednich kryzysów. Pokazał, że jest w stanie przetrwać pandemię COVID-19, rosyjską agresję na Ukrainę, kryzysy finansowe w innych jurysdykcjach, cyberataki i wiele innych zdarzeń.

Biorąc jednak pod uwagę bezprecedensowe zagrożenia i bardziej niepewne otoczenie geopolityczne, w jakim znajduje się UE, ważne jest, aby stale oceniać poziom gotowości sektora finansowego UE. UE kontynuuje te prace i może wprowadzić wszelkie dostosowania niezbędne do zapewnienia szybkich, skoordynowanych i proporcjonalnych działań zapobiegawczych i reaktywnych, na szczeblu zarówno UE, jak i państw członkowskich, z myślą o utrzymaniu stałego kursu i zachowaniu podstawowych funkcji sektora finansowego UE. Oczekuje się, że w przyszłości rozwój unii oszczędności i inwestycji oraz wprowadzenie cyfrowego euro poprawią ogólną odporność sektora finansowego UE i dodatkowo podniosą poziom jego gotowości.