DORA
OPERACYJNA ODPORNOŚĆ CYFROWA SEKTORA FINANSOWEGO

Komentarz

redakcja naukowa Mariola Lemonnier

Tomasz Bejm, Małgorzata Gryber, Szymon Kisiel
Mariola Lemonnier, Michał Mariański, Piotr Pałka
Dorota Sowińska-Kobelak, Jolanta Turczynowicz-Kieryłło

Wolters Kluwer

DORA
OPERACYJNA ODPORNOŚĆ CYFROWA SEKTORA FINANSOWEGO

Komentarz

redakcja naukowa Mariola Lemonnier

Tomasz Bejm, Małgorzata Gryber, Szymon Kisiel
Mariola Lemonnier, Michał Mariański, Piotr Pałka
Dorota Sowińska-Kobelak, Jolanta Turczynowicz-Kieryłło

Wolters Kluwer

WARSZAWA 2025

Stan prawny na 7 sierpnia 2025 r.

Recenzent
Dr hab. Piotr Zapadka, profesor UKSW

Wydawca
Grzegorz Jarecki

Redaktor prowadzący
Katarzyna Gierłowska

Opracowanie redakcyjne
JustLuk

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Komentarze do poszczególnych części napisali:

Tomasz Bejm – art. 3, 12, 15–21, 23–29, 31, 40–41, 45
Małgorzata Gryber – art. 22, 46–49
Szymon Kisiel – art. 1, 57–60
Mariola Lemonnier – art. 4, 44
Mariola Lemonnier, Piotr Pałka – Preambuła
Michał Mariański – art. 2, 61–64
Piotr Pałka – art. 5–11, 13–14, 32–36, 42–43, 56
Dorota Sowińska-Kobelak – art. 30, 37–39
Jolanta Turczynowicz-Kieryłło – art. 50–55

ISBN 978-83-8390-969-1 *ISBN PDF-a: 978-83-8390-970-7*

Wolters Kluwer Polska Sp. z o.o.
Dział Zarządzania Prawami Autorskimi i Treściami
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 692 477 076; e-mail: PL-ksiazki@wolterskluwer.com
księgarnia internetowa www.profinfo.pl

Spis treści

Wykaz skrótów

Akty prawne

dyrektywa 2009/65/WE – dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z 13.07.2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) (Dz.Urz. UE L 302, s. 32, ze zm.)

dyrektywa 2009/110/WE – dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z 16.09.2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.Urz. UE L 267, s. 7, ze zm.)

dyrektywa 2009/138/WE – dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25.11.2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.Urz. UE L 335, s. 1, ze zm.)

dyrektywa 2011/61/UE – dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z 8.06.2011 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.Urz. UE L 174, s. 1, ze zm.)

dyrektywa 2013/34/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/34/UE z 26.06.2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniająca dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylająca dyrektywy Rady 78/660/EWG i 83/349/EWG (Dz.Urz. UE L 182, s. 19, ze zm.)

dyrektywa 2013/36/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z 26.06.2013 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.Urz. UE L 176, s. 338, ze zm.)

dyrektywa 2014/59/UE – dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z 15.05.2014 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/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (Dz.Urz. UE L 173, s. 190, ze zm.)

dyrektywa 2015/2366 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 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.Urz. UE L 337, s. 35, ze zm.)

dyrektywa 2016/97 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z 20.01.2016 r. w sprawie dystrybucji ubezpieczeń (Dz.Urz. UE L 26, s. 19, ze zm.)

dyrektywa 2025/2 – dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2025/2 z 27.11.2024 r. w sprawie zmiany dyrektywy 2009/138/WE w odniesieniu do proporcjonalności, jakości nadzoru, sprawozdawczości, środków dotyczących gwarancji długoterminowych, narzędzi makroostrożnościowych, ryzyk dla zrównoważonego rozwoju oraz nadzoru nad grupą i nadzoru transgranicznego, a także w sprawie zmiany dyrektyw 2002/87/WE i 2013/34/UE (Dz.Urz. UE L 2025/2)

dyrektywa MiFID II – ang. Markets in Financial Instruments Directive II, dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z 15.05.2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.Urz. UE L 173, s. 349, ze zm.)

dyrektywa NIS 2 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.Urz. UE L 333, s. 80)

EKPC – Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)

k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2025 r. poz. 1071)

k.k. – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2025 r. poz. 383)

Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)

k.p.a. – ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572 ze zm.)

k.s.h. – ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2024 r. poz. 18 ze zm.)

nowelizacja z 25.06.2025 r. – ustawa z 25.06.2025 r. o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego oraz emitowaniem europejskich zielonych obligacji (Dz.U. poz. 1069)

p.k.e. – ustawa z 12.07.2024 r. – Prawo komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1221 ze zm.)

pr. bank. – ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2024 r. poz. 1646 ze zm.)

rozporządzenie 1060/2009 – rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 z 16.09.2009 r. w sprawie agencji ratingowych (Dz.Urz. UE L 302, s. 1, ze zm.)

rozporządzenie 1093/2010 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z 24.11.2010 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.Urz. UE L 331, s. 12, ze zm.)

rozporządzenie 1094/2010 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z 24.11.2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.Urz. UE L 331, s. 48, ze zm.)

rozporządzenie 1095/2010 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z 24.11.2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE (Dz.Urz. UE L 331, s. 84, ze zm.)

rozporządzenie 648/2012 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z 4.07.2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów w centralnych i repozytoriów transakcji (Dz.Urz. UE L 201, s. 1, ze zm.)

rozporządzenie 1024/2013 – rozporządzenie Rady (UE) nr 1024/2013 z 15.10.2013 r. w sprawie powierzenia Europejskiemu Bankowi Centralnemu szczególnych zadań dotyczących polityki ostrożnościowej nad instytucjami kredytowymi (Dz.Urz. UE L 287, s. 63)

rozporządzenie 600/2014 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z 15.05.2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (Dz.Urz. UE L 173, s. 84, ze zm.)

rozporządzenie 909/2014 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z 23.07.2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.Urz. UE L 257, s. 1, ze zm.)

rozporządzenie 2016/679, RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze zm.)

rozporządzenie 2016/1011 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1011 z 8.06.2016 r. w sprawie indeksów stosowanych jako wskaźniki referencyjne w instrumentach finansowych i umowach finansowych lub do pomiaru wyników funduszy inwestycyjnych i zmieniające dyrektywy 2008/48/WE i 2014/17/UE oraz rozporządzenie (UE) nr 596/2014 (Dz.Urz. UE L 171, s. 1, ze zm.)

rozporządzenie 2018/1725 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.Urz. UE L 295, s. 39)

rozporządzenie 2019/881 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15, ze zm.)

rozporządzenie 2019/2033 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2033 z 27.11.2019 r. w sprawie wymogów ostrożnościowych dla firm inwestycyjnych oraz zmieniające rozporządzenia (UE) nr 1093/2010, (UE) nr 575/2013, (UE) nr 600/2014 i (UE) nr 806/2014 (Dz.Urz. UE L 314, s. 1, ze zm.).

rozporządzenie 2020/1503 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/1503 z 7.10.2020 r. w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsięwzięć gospodarczych oraz zmieniające rozporządzenie (UE) 2017/1129 i dyrektywę (UE) 2019/1937 (Dz.Urz. UE L 347, s. 1)

rozporządzenie 2022/2554, DORA – ang. Digital Operational Resilience Act, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14.12.2022 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.Urz. UE L 333, s. 1, ze zm.)

rozporządzenie 2023/1114 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z 31.05.2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.Urz. UE L 150, s. 40, ze zm.)

rozporządzenie delegowane 2024/1502 – rozporządzenie delegowane Komisji (UE) 2024/1502 z 22.02.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 przez określenie kryteriów wyznaczania zewnętrznych dostawców usług ICT jako mających kluczowe znaczenie dla podmiotów finansowych (Dz.Urz. UE L 2024/1502)

rozporządzenie delegowane 2024/1505 – rozporządzenie delegowane Komisji (UE) 2024/1505 z 22.02.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 przez określenie wysokości opłat nadzorczych pobieranych przez wiodący organ nadzorczy od kluczowych zewnętrznych dostawców usług ICT oraz sposobu uiszczania tych opłat (Dz.Urz. UE L 2024/1505)

rozporządzenie delegowane 2024/1772 – rozporządzenie delegowane Komisji (UE) 2024/1772 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów (Dz.Urz. UE L 2024/1772)

rozporządzenie delegowane 2024/1773 – rozporządzenie delegowane Komisji (UE) 2024/1773 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych doprecyzowujących szczegółową treść polityki w zakresie ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT (Dz.Urz. UE L 2024/1773)

rozporządzenie delegowane 2024/1774 – rozporządzenie delegowane Komisji (UE) 2024/1774 z 13.03.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT (Dz.Urz. UE L 2024/1774, ze zm.)

rozporządzenie delegowane 2025/301 – rozporządzenie delegowane Komisji (UE) 2025/301 z 23.10.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających treść i terminy przedłożenia wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego dotyczących poważnych incydentów związanych z ICT, a także treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach (Dz.Urz. UE L 2025/301)

rozporządzenie delegowane 2025/303 – rozporządzenie delegowane Komisji (UE) 2025/303 z 31.10.2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w odniesieniu do regulacyjnych standardów technicznych określających informacje, które mają być przekazywane przez niektóre podmioty finansowe w powiadomieniu o zamiarze świadczenia usług w zakresie kryptoaktywów (Dz.Urz. UE 2025/303)

rozporządzenie delegowane 2025/532 – rozporządzenie delegowane Komisji (UE) 2025/532 z 24.03.2025 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających elementy, które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo usług ICT wspierających krytyczne lub istotne funkcje (Dz.Urz. UE L 2025/532)

rozporządzenie delegowane 2025/1190 – rozporządzenie delegowane Komisji (UE) 2025/1190 z 13.02.2025 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria stosowane do identyfikacji podmiotów finansowych zobowiązanych do przeprowadzania testów penetracyjnych pod kątem wyszukiwania zagrożeń, wymogi i standardy regulujące korzystanie z testerów wewnętrznych, wymogi dotyczące zakresu, metodyki testowania i podejścia dla każdego etapu procesu testowania oraz etapów testów odnoszących się do wyników, zamykania i środków naprawczych, a także rodzaj współpracy w zakresie nadzoru i inne odpowiednie rodzaje współpracy potrzebne do przeprowadzenia TLPT i do ułatwienia wzajemnego uznawania (Dz.Urz. UE L 2025/1190)

rozporządzenie MAR – ang. Market Abuse Regulation, rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z 16.04.2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady oraz dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (Dz.Urz. UE L 173, s. 1, ze zm.)

rozporządzenie wykonawcze 2025/302 – rozporządzenie wykonawcze Komisji (UE) 2025/302 z 23.10.2024 r. ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych formularzy, wzorów i procedur stosowanych przez podmioty finansowe do celów zgłaszania poważnych incydentów związanych z ICT i powiadamiania o znaczących cyberzagrożeniach (Dz.Urz. UE L 2025/302)

TFUE – Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 47, ze sprost.)

TUE – Traktat o Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 13)

u.n.r.f. – ustawa z 21.07.2006 r. o nadzorze nad rynkiem finansowym (Dz.U. z 2025 r. poz. 640 ze zm.)

u.n.r.k. – ustawa z 29.07.2005 r. o nadzorze nad rynkiem kapitałowym (Dz.U. z 2024 r. poz. 1161 ze zm.)

u.o.i.f. – ustawa z 29.07.2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2024 r. poz. 722 ze zm.)

Czasopisma

PPH – Przegląd Prawa Handlowego

Instytucje

EBA – Europejski Urząd Nadzoru Bankowego (ang. European Banking Authority)

EBC – Europejski Bank Centralny

EIOPA – Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (ang. European Insurance and Occupational Pensions Authority)

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ang. European Network and Information Security Agency)

ERRS – Europejska Rada ds. Ryzyka Systemowego

ESBC – Europejski System Banków Centralnych

ESMA – Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ang. European Securities and Markets Authority)

ETPC – Europejski Trybunał Praw Człowieka

EUN – Europejski Urząd Nadzoru (ang. ESA – European Supervisory Authority)

KNF – Komisja Nadzoru Finansowego

NIST – Narodowy Instytut Standaryzacji i Technologii (ang. National Institute of Standards and Technology)

OECD – Organizacja Współpracy Gospodarczej i Rozwoju (ang. Organisation for Economic Co-operation and Development)

SKOK – spółdzielcza kasa oszczędnościowo-kredytowa

UKNF – Urząd Komisji Nadzoru Finansowego

Inne

AFI – alternatywny fundusz inwestycyjny

BCP – plan ciągłości działania (ang. *business continuity plan*)

BIA – analiza wpływu na biznes (ang. *business impact analysis*)

CCP – kontrahent centralny (ang. *central counterparty*)

CDPW/CSD – centralny depozyt papierów wartościowych (ang. *central securities depository*)

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego (ang. *computer security incident response team*)

CTPP – kluczowy zewnętrzny dostawca usług ICT (ang. *critical ICT third-party service provider*)

DRP – plan odzyskiwania po awarii (ang. *disaster recovery plan/procedure*)

IORP – instytucja pracowniczych programów emerytalnych (ang. *institution for occupational retirement provision*)

ICT – technologie informacyjno-komunikacyjne (ang. *information and communication technology*)

ITS – wykonawcze standardy techniczne (ang. *implementing technical standards*)

MŚP – małe lub średnie przedsiębiorstwo

NCA – właściwy organ krajowy (ang. *national competent authority*)

RPO – cel punktu odzyskiwania (ang. *recovery point objective*)

RTO – docelowy czas odzyskiwania (ang. *recovery time objective*)

RTS – regulacyjne standardy techniczne (ang. *regulatory technical standards*)

TIBER-EU – oficjalne ramy testowania odporności cybernetycznej oparte na wywiadzie zagrożeń dla Unii Europejskiej (ang. *Threat Intelligence-Based Ethical Red Teaming Framework for the European Union*)

TLPT – testy penetracyjne ukierunkowane na analizę zagrożeń (ang. *Threat Led Penetration Testing*)

ZAFI – zarządzający alternatywnymi funduszami inwestycyjnymi

Wprowadzenie

W latach dwudziestych XX w. William „The Actor" Sutton był jednym z najsłynniejszych zbiegów w Ameryce, umieszczonych przez FBI na liście najbardziej poszukiwanych przestępców *Top Ten Fugitive*. Kiedy zapytano go, dlaczego rabuje banki, odpowiedział krótko: „Bo tam się trzyma pieniądze" („Because that's where the money is"). Ta prosta, a zarazem trafna odpowiedź ukazuje ponadczasową prawdę o motywacjach ludzkich – niezależnie od epoki pieniądze pozostają głównym celem tych, którzy chcą je zdobyć, często bez względu na środki. W dzisiejszym cyfrowym świecie odpowiedź Suttona wciąż brzmi aktualnie, choć metody uległy znaczącej zmianie. Współcześni przestępcy nie muszą się już przebierać jak aktorzy i wchodzić do banku z bronią – wystarczą im luki w zabezpieczeniach systemów informatycznych. W reakcji na te nowe wyzwania rozporządzenie DORA (ang. Digital Operational Resilience Act) ustanawia ramy prawne, które mają na celu przygotowanie instytucji finansowych do skutecznego zarządzania ryzykiem cyfrowym oraz ochronę przed współczesnymi „The Actors". Niniejszy komentarz pokazuje, że choć motywacje pozostają niezmienne, to sposoby obrony muszą być dostosowane do realiów cyfrowej transformacji, aby zapewnić bezpieczeństwo i stabilność sektora finansowego. Sektor finansowy jest głównym naturalnym celem cyberataków ze względu na wrażliwe dane, którymi się zajmuje, oraz potencjalnie niszczycielskie skutki finansowe naruszenia. Instytucje finansowe stają przed wyjątkowymi wyzwaniami w zakresie ochrony swojej infrastruktury oraz zapewnienia bezpieczeństwa transakcji i danych.

Oddając w ręce czytelników komentarz do rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, zwanego DORA, grono autorów podzieliło się z czytelnikami nie tylko wiedzą, oceną, lecz także podejściem krytycznym do treści rozporządzenia. W publikacji omówiono konkretne wyzwania w zakresie cyberbezpieczeństwa w sektorze finansowym oraz rozwiązania mające na celu stawienia czoła tym zagrożeniom. Zanim podjęliśmy się tej wymagającej pracy intelektualnej i technicznej, przeanalizowaliśmy wiele aktów wykonawczych, delegowanych, mając na celu podstawowe zadanie rozporządzenia, jakim jest uzyskanie wysokiej odporności w zakresie ryzyka ICT podmiotów finansowych. Przedstawiliśmy w komentarzu rozwiązania prawne, organizacyjne, nadzorcze, biznesowe, a także porównawcze. Zostały wzięte pod uwagę także pewne zmiany w polskich przepisach dotyczących rynku finansowego z 2025 r. Ramy niniejszego komentarza nie pozwoliły na zajęcie się problematyką *soft law*, w tym rekomendacji polskiego organu nadzoru. Tematyka ta zasługuje na odrębne opracowanie. Nie koncentrowaliśmy się na teorii, ale staraliśmy się podawać rozwiązania praktyczne i syntetyczne. Komentarz jest pracą o charakterze interdy-

scyplinarnym i przekrojowym, stąd wystąpią zapewne pewne pominięcia czy uproszczenia, za które z góry przepraszamy.

Zagrożenia szybko ewoluują w sektorze finansowym, zaś pojawienie się nowych technologii, sztucznej inteligencji, komputerów kwantowych prawdopodobnie jeszcze bardziej przyspieszy ten trend. Instytucje finansowe muszą zatem przyjąć proaktywną postawę w zakresie cyberbezpieczeństwa, aby przewidywać nowe zagrożenia i być odpornymi na nie. Nie wiemy, jak szybko będzie się zmieniać prawo regulujące cyberbezpieczeństwo rynku finansowego, ale mamy świadomość, iż będą to, jak dotychczas, zmiany bardzo szybkie, głębokie i wymagające.

Sektor finansowy stoi przed wyjątkowymi wyzwaniami w zakresie cyberbezpieczeństwa ze względu na krytyczny charakter przetwarzanych danych i surowe przepisy, których musi przestrzegać. Aby skutecznie chronić swoje sieci i systemy, instytucje finansowe muszą przyjąć wieloaspektowe podejście, łącząc najnowocześniejsze technologie z zarządzaniem i ciągłym szkoleniem pracowników. Przewidując zagrożenia i wzmacniając bezpieczeństwo swoich systemów i organizacji, podmioty rynku finansowego mogą jednak lepiej chronić się pomimo ciągle zmieniającego się cyfrowego krajobrazu.

Autorzy

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

(Tekst mający znaczenie dla EOG)

(Dz.Urz. UE L 333, s. 1; sprost. Dz.Urz. UE L 2024/90177)

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego 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) W epoce cyfrowej technologie informacyjno-komunikacyjne (ICT) stanowią wsparcie dla złożonych systemów wykorzystywanych w codziennych działaniach. ICT napędzają naszą gospodarkę w najważniejszych sektorach, w tym w sektorze finansowym, oraz wzmacniają funkcjonowanie rynku wewnętrznego. Większy zakres cyfryzacji i wzajemnych powiązań zwiększa również ryzyko związane z ICT, przez co całe społeczeństwo – i w szczególności system finansowy – staje się bardziej podatne na cyberzagrożenia lub zakłócenia w funkcjonowaniu ICT. Chociaż powszechne korzystanie z systemów ICT i wysoki stopień cyfryzacji oraz łączności to obecnie podstawowe cechy działań podmiotów finansowych w Unii, ich odporność cyfrowa nie jest jeszcze odpowiednio uwzględniona w ich szerszych ramach operacyjnych ani włączona do tych ram.

(2) W minionych dziesięcioleciach korzystanie z ICT zaczęło odgrywać zasadniczą rolę, jeżeli chodzi o świadczenie usług finansowych, do tego stopnia, że obecnie ICT mają krytyczne znaczenie dla wykonywania typowych codziennych funkcji wszystkich podmiotów finansowych. Cyfryzacja obejmuje teraz na przykład płatności, w przypadku których w coraz większym stopniu przechodzi się od metod gotówkowych i papierowych do stosowania rozwiązań cyfrowych, a także rozliczanie i rozrachunek papierów wartościowych, handel elektroniczny i algorytmiczny, operacje udzielania pożyczek i finansowania, finansowanie *peer-to-peer*, rating kredytowy, obsługę roszczeń i działalność *back-office*. Sektor ubezpieczeń również uległ przeobrażeniom w związku z korzystaniem z ICT, czego przykładem jest pojawienie się pośredników ubezpieczeniowych oferujących swoje usługi przez internet i prowadzących działalność przy użyciu technologii ubezpieczeniowej (InsurTech) oraz zawieranie ubezpieczeń w formie cyfrowej. Finanse nie tylko stały się w dużej mierze cyfrowe w całym sektorze, ale cyfryzacja wzmocniła również wzajemne połączenia i zależności w ramach sektora finansowego oraz z infrastrukturą zewnętrzną i zewnętrznymi dostawcami usług.

(3) W sprawozdaniu z 2020 r. dotyczącym systemowego ryzyka w cyberprzestrzeni Europejska Rada ds. Ryzyka Systemowego (ERRS) potwierdziła, że istniejący wysoki poziom wzajemnych powiązań między podmiotami finansowymi, rynkami finansowymi i infrastrukturami rynku finansowego, a w szczególności współzależności między ich systemami ICT mogą stanowić podatność o charakterze systemowym, ponieważ lokalne cyberincydenty mogłyby szybko rozprzestrzenić się z każdego z około 22 000 unijnych podmiotów finansowych na cały system finansowy, bez żadnych przeszkód związanych z granicami geograficznymi. Poważne naruszenia związane z ICT występujące w sektorze finansowym nie dotyczą wyłącznie samych podmiotów finansowych. Naruszenia te zwiększają również ryzyko rozpowszechnienia lokalnych podatności we wszystkich kanałach oddziaływania finansowego oraz potencjalnie wywołują negatywne konsekwencje dla stabilności unijnego systemu finansowego, takie jak utrata płynności i ogólna utrata pewności i zaufania w odniesieniu do rynków finansowych.

(4) W ostatnich latach ryzyko związane z ICT przyciągnęło uwagę międzynarodowych, unijnych i krajowych decydentów, organów regulacyjnych i podmiotów normalizacyjnych, które starają się zwiększyć odporność cyfrową, określić standardy i koordynować prace regulacyjne lub nadzorcze w tym zakresie. Na szczeblu międzynarodowym Bazylejski Komitet Nadzoru Bankowego, Komitet ds. Systemów Płatności i Rozrachunku, Rada Stabilności Finansowej, Instytut Stabilności Finansowej, a także grupa G-7 i grupa G-20 dążą do zapewnienia właściwym organom i podmiotom gospodarczym z różnych jurysdykcji narzędzi mających na celu wzmocnienie odporności ich systemów finansowych. Prace te wynikały również z potrzeby należytego uwzględnienia ryzyka związanego z ICT w kontekście ściśle połączonego wzajemnie, globalnego systemu finansowego i dążenia do zapewnienia większej spójności odpowiednich najlepszych praktyk.

(5) Pomimo unijnych i krajowych ukierunkowanych polityk i inicjatyw ustawodawczych ryzyko związane z ICT nadal stanowi wyzwanie dla odporności operacyjnej, wydajności i stabilności unijnego systemu finansowego. Reformy, które przeprowadzono po kryzysie finansowym z 2008 r., doprowadziły przede wszystkim do wzmocnienia odporności finansowej unijnego sektora finansowego, a także miały na celu zabezpieczenie konkurencyjności i stabilności Unii z punktu widzenia gospodarki, standardów ostrożnościowych i zasad postępowania na rynku. Chociaż bezpieczeństwo ICT i odporność cyfrowa są częścią ryzyka operacyjnego, elementy te były w mniejszym stopniu przedmiotem agendy regulacyjnej po kryzysie finansowym i rozwijały się tylko w niektórych obszarach unijnej polityki dotyczącej usług finansowych oraz otoczenia regulacyjnego lub jedynie w niektórych państwach członkowskich.

(6) W swoim komunikacie z dnia 8 marca 2018 r. zatytułowanym „Plan działania w zakresie technologii finansowej: w kierunku bardziej konkurencyjnego i innowacyjnego europejskiego sektora finansowego" Komisja podkreśliła podstawowe znaczenie zwiększenia odporności unijnego sektora finansowego, w tym z operacyjnego punktu widzenia, dla zapewnienia jego bezpieczeństwa technologicznego oraz sprawnego funkcjonowania, szybkiego przywracania sprawności po naruszeniach i incydentach związanych z ICT, umożliwiając ostatecznie skuteczne i sprawne świadczenie usług finansowych w całej Unii, w tym w sytuacjach skrajnych, przy jednoczesnej ochronie konsumenta oraz utrzymaniu zaufania i pewności w odniesieniu do rynku.

(7) W kwietniu 2019 r. Europejski Urząd Nadzoru (Europejski Urząd Nadzoru Bankowego), (EUNB), ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1093/2010[4], Europejski Urząd Nadzoru (Europejski Urząd Nadzoru Ubezpieczeń *i* Pracowniczych Programów Emerytalnych), (EIOPA), ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1094/2010[5], oraz Europejski Urząd Nadzoru (Europejski Urząd Nadzoru Giełd i Papierów Wartościowych), (ESMA) ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1095/2010[6], (wspólnie znane jako „Europejskie Urzędy Nadzoru" lub „EUN") opublikowały wspólnie zalecenia techniczne, w których wezwały do przyjęcia spójnego podejścia do ryzyka związanego z ICT w sektorze finansów, oraz zaleciły wzmocnienie, w sposób proporcjonalny, operacyjnej odporności cyfrowej sektora usług finansowych za pomocą unijnej inicjatywy sektorowej.

(8) Unijny sektor finansowy jest regulowany za pomocą jednolitego zbioru przepisów i podlega Europejskiemu Systemowi Nadzoru Finansowego. Przepisy dotyczące operacyjnej odporności cyfrowej i bezpieczeństwa ICT nie zostały jednak jeszcze w pełni lub spójnie zharmonizowane, mimo że operacyjna odporność cyfrowa ma zasadnicze znaczenie dla zapewnienia stabilności finansowej i integralności rynku w epoce cyfrowej i nie jest mniej ważna niż na przykład wspólne standardy ostrożnościowe lub zasady postępowania na rynku. Należy zatem rozbudować jednolity zbiór przepisów i system nadzoru, tak aby uwzględniały również operacyjną odporność cyfrową, poprzez wzmocnienie mandatów właściwych organów w celu umożliwienia im sprawowania nadzoru w zakresie zarządzania ryzykiem ICT w sektorze finansowym w celu ochrony integralności i efektywności rynku wewnętrznego oraz ułatwieniu jego należytego funkcjonowania.

(9) Rozbieżności legislacyjne i niejednolite krajowe podejścia regulacyjne lub nadzorcze do ryzyka związanego z ICT powodują powstanie przeszkód dla funkcjonowania rynku wewnętrznego usług finansowych, utrudniając sprawne korzystanie ze swobody przedsiębiorczości i swobody świadczenia usług podmiotom finansowym prowadzącym działalność transgraniczną. Może zostać również zakłócona konkurencja między tego samego rodzaju podmiotami finansowymi działającymi w różnych państwach członkowskich. Dzieje się tak w przypadku obszarów, w których unijna harmonizacja jest bardzo ograniczona – takich jak testowanie operacyjnej odporności cyfrowej – lub nie istnieje – takich jak monitorowanie ryzyka ze strony zewnętrznych dostawców usług iCt. Rozbieżności wynikające ze zmian planowanych na szczeblu krajowym mogłyby spowodować dalsze przeszkody dla funkcjonowania rynku wewnętrznego ze szkodą dla uczestników rynku i dla stabilności finansowej.

(10) Dotychczasowe częściowe tylko uwzględnienie przepisów dotyczących ryzyka związanego z ICT na szczeblu Unii powoduje braki lub nakładanie się przepisów w istotnych obszarach, takich jak zgłaszanie incydentów związanych z ICT i testowanie operacyjnej odporności cyfrowej, oraz niespójności wynikające z wprowadzanych rozbieżnych przepisów krajowych lub nieefektywnego kosztowo stosowania nakładających się przepisów. Ma to szczególnie szkodliwy wpływ na użytkowników intensywnie wykorzystujących ICT, takich jak w sektorze finansowym, ponieważ ryzyko związane z technologią nie zna granic państwowych, a sektor finansowy wprowadza swoje usługi na szeroką, transgraniczną skalę w Unii i poza nią. Indywidualne podmioty finansowe prowadzące działalność trans- graniczną lub posiadające kilka zezwoleń (np. jeden podmiot finansowy może posiadać zezwolenia na prowadzenie działalności bankowej, jako firma inwestycyjna i jako instytucja płatnicza, przy czym każde z nich może być wydane przez różne właściwe organy w jednym lub w kilku państwach członkowskich) stają przed wyzwaniami operacyjnymi przy samodzielnym zwalczaniu ryzyka związanego z ICT oraz łagodzeniu negatywnego wpływu incydentów związanych z ICT w spójny, opłacalny sposób.

(11) Biorąc pod uwagę, że do jednolitego zbioru przepisów nie dołączono kompleksowych ram dotyczących ICT lub ryzyka operacyjnego, konieczna jest dalsza harmonizacja najważniejszych wymogów w zakresie operacyjnej odporności cyfrowej dla wszystkich podmiotów finansowych. Zdolności w zakresie ICT i ogólna odporność, rozwijane przez podmioty finansowe – na podstawie tych najważniejszych wymogów – w celu przetrwania przestojów operacyjnych, przyczyniłyby się do ochrony stabilności i integralności unijnych rynków finansowych, a tym samym do zapewnienia wysokiego poziomu ochrony inwestorów i konsumentów w Unii. Biorąc pod uwagę, że niniejsze rozporządzenie ma na celu przyczynienie się do sprawnego funkcjonowania rynku wewnętrznego, powinno ono opierać się na przepisach art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) zgodnie z jego wykładnią przyjętą w świetle utrwalonego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości").

(12) Niniejsze rozporządzenie ma na celu konsolidację i aktualizację wymogów dotyczących ryzyka związanego z ICT jako części wymogów dotyczących ryzyka operacyjnego zawartych dotychczas osobno w różnych unijnych aktach prawnych. Chociaż te akty prawne obejmowały główne kategorie ryzyka finansowego (np. ryzyko kredytowe, ryzyko rynkowe, ryzyko kredytowe kontrahenta i ryzyko płynności, ryzyko związane z postępowaniem na rynku), nie uwzględniono w nich – w momencie ich przyjęcia – w sposób kompleksowy wszystkich elementów odporności operacyjnej. Przepisy dotyczące ryzyka operacyjnego, jeżeli zostały szerzej rozwinięte w tych unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do zwalczania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie ukierunkowanym przepisom jakościowym dotyczącym zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania sprawności i odbudowy w odniesieniu do incydentów związanych z ICT lub zdolności w zakresie sprawozdawczości i testowania cyfrowego. Te akty prawne miały przede wszystkim obejmować i aktualizować podstawowe przepisy dotyczące nadzoru ostrożnościowego, integralności rynku lub postępowania na rynku. Poprzez konsolidację i aktualizację różnych przepisów dotyczących ryzyka związanego z ICT, wszystkie przepisy dotyczące ryzyka cyfrowego w sektorze finansowym powinny zostać po raz pierwszy zebrane w spójny sposób w jednym akcie ustawodawczym. Niniejsze rozporządzenie wypełnia braki lub eliminuje niespójności w niektórych z poprzednich aktów prawnych, w tym związane ze stosowaną w nich terminologią,

oraz wyraźnie odnosi się do ryzyka związanego z ICT za pośrednictwem ukierunkowanych przepisów w sprawie zdolności w zakresie zarządzania ryzykiem związanym z ICT, zgłaszania incydentów, testowania odporności operacyjnej oraz monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT. Zatem niniejsze rozporządzenie powinno również zwiększyć świadomość na temat ryzyka związanego z ICT i potwierdzić, że incydenty związane z ICT i brak odporności operacyjnej mogą zagrozić dobrej kondycji finansowej podmiotów finansowych.

(13) Podmioty finansowe powinny przyjąć to samo podejście i stosować się do tych samych, opartych na zasadach przepisów podczas zwalczania ryzyka związanego z ICT, uwzględniając przy tym swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności realizowanych usług, działań i operacji. Spójność przyczynia się do wzmocnienia zaufania do systemu finansowego oraz ochrony jego stabilności, zwłaszcza w czasach dużej zależności od systemów, platform i infrastruktur ICT, co powoduje większe ryzyko cyfrowe. Przestrzeganie zasad podstawowej higieny cyberbezpieczeństwa powinno również pozwolić uniknąć obciążania gospodarki znacznymi kosztami dzięki zminimalizowaniu wpływu i kosztów zakłóceń funkcjonowania ICT.

(14) Rozporządzenie pomaga ograniczyć stopień złożoności regulacyjnej, wspiera spójność w zakresie nadzoru, zwiększa pewność prawa, a także przyczynia się do ograniczenia kosztów przestrzegania przepisów, zwłaszcza dla podmiotów finansowych prowadzących działalność transgraniczną, i do zmniejszenia zakłóceń konkurencji. W związku z tym wybór rozporządzenia na potrzeby ustanowienia wspólnych ram operacyjnej odporności cyfrowej podmiotów finansowych wydaje się najbardziej odpowiednim sposobem zagwarantowania jednolitego i spójnego stosowania wszystkich elementów zarządzania ryzykiem związanym z ICT przez unijny sektor finansowy.

(15) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148[7] stanowiła pierwsze horyzontalne ramy w zakresie cyberbezpieczeństwa obowiązujące na szczeblu Unii, mające też zastosowanie do trzech rodzajów podmiotów finansowych, a mianowicie instytucji kredytowych, systemów obrotu i kontrahentów centralnych. Jednak biorąc pod uwagę, że w dyrektywie (UE) 2016/1148 określono mechanizm identyfikacji na szczeblu krajowym operatorów usług kluczowych, jedynie niektóre instytucje kredytowe i systemy obrotu oraz niektórzy kontrahenci centralni zidentyfikowani przez państwa członkowskie są w praktyce objęci jej zakresem stosowania, a zatem mają obowiązek spełniać określone w niej wymogi w zakresie bezpieczeństwa ICT i zgłaszania incydentów. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555[8] ustanawia jednolite kryterium określania podmiotów objętych jej zakresem stosowania (zasada limitu wielkości), przy czym obejmuje nim też wspomniane trzy rodzaje podmiotów finansowych.

(16) Niemniej jednak biorąc pod uwagę, że niniejsze rozporządzenie zwiększa poziom harmonizacji różnych elementów odporności cyfrowej poprzez wprowadzenie wymogów w zakresie zarządzania ryzykiem związanym z ICT i zgłaszania incydentów związanych z ICT, które to wymogi są bardziej rygorystyczne w porównaniu z wymogami określonymi w obecnych unijnych przepisach dotyczących usług finansowych, ten wyższy poziom zapewnia zwiększoną harmonizację również w porównaniu z wymogami określonymi w dyrektywie (UE) 2022/2555. W związku z tym niniejsze rozporządzenie stanowi *lex specialis* względem dyrektywy (UE) 2022/2555. Jednocześnie, utrzymanie silnego związku między sektorem finansowym a unijnymi horyzontalnymi ramami w zakresie cyberbezpieczeństwa, określonymi obecnie w dyrektywie (UE) 2022/2555, ma zasadnicze znaczenie dla zapewnienia spójności z przyjętymi przez państwa członkowskie strategiami w zakresie cyberbezpieczeństwa oraz umożliwienia organom nadzoru finansowego uzyskania informacji na temat cyberincydentów wpływających na inne sektory objęte tą dyrektywą.

(17) Zgodnie z art. 4 ust. 2 Traktatu o Unii Europejskiej i bez uszczerbku dla kontroli sądowej sprawowanej przez Trybunał Sprawiedliwości niniejsze rozporządzenie nie powinno mieć wpływu na odpowiedzialność państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i ochrony bezpieczeństwa narodowego, np. jeżeli chodzi o przekazywanie informacji stojących w sprzeczności z ochroną bezpieczeństwa narodowego.

(18) Aby umożliwić międzysektorowy proces uczenia się i skutecznie czerpać z doświadczeń innych sektorów podczas reagowania na cyberzagrożenia, podmioty finansowe, o których mowa w dyrektywie (UE) 2022/2555, powinny pozostać częścią „ekosystemu" tej dyrektywy (np. Grupa Współpracy i zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)). EUN i właściwe organy krajowe powinny być w stanie uczestniczyć w dyskusjach na temat strategicznej polityki i technicznych pracach grupy współpracy na mocy tej dyrektywy oraz wymieniać informacje i dalej współpracować z pojedynczymi punktami kontaktowymi wyznaczonymi lub ustanowionymi zgodnie z tą dyrektywą. Właściwe organy zgodnie z niniejszym rozporządzeniem powinny również prowadzić konsultacje i współpracować z CSIRT. Właściwe organy powinny też mieć możliwość zwrócenia się o zalecenia techniczne do właściwych organów wyznaczonych lub ustanowionych zgodnie dyrektywą (UE) 2022/2555 i opracowania ustaleń dotyczących współpracy, służących zapewnieniu skutecznych i szybkich mechanizmów koordynacji działań.

(19) Ze względu na silne powiązania między cyfrową i fizyczną odpornością podmiotów finansowych, w niniejszym rozporządzeniu i w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557[9] należy zastosować spójne podejście do kwestii odporności podmiotów krytycznych. Z uwagi na to, że w przewidzianych w niniejszym rozporządzeniu obowiązkach w zakresie zarządzania ryzykiem związanym z ICT i w zakresie zgłaszania incydentów kompleksowo zajęto się kwestią fizycznej odporności podmiotów finansowych, obowiązki ustanowione w rozdziałach III i IV dyrektywy (UE) 2022/2557 nie powinny mieć zastosowania do podmiotów finansowych objętych zakresem stosowania tej dyrektywy.

(20) Dostawcy usług chmurowych stanowią jedną z kategorii infrastruktury cyfrowej objętej dyrektywą (UE) 2022/2555. Unijne ramy nadzoru (zwane dalej „ramami nadzoru") ustanowione niniejszym rozporządzeniem mają zastosowanie do wszystkich kluczowych zewnętrznych dostawców usług ICT, w tym dostawców usług chmurowych, jeżeli świadczą oni usługi ICT na rzecz podmiotów finansowych; należy zatem uznać, że stanowią one uzupełnienie nadzoru sprawowanego zgodnie z dyrektywą (UE) 2022/2555. Ponadto, wobec braku unijnych horyzontalnych ram ustanawiających organ nadzoru cyfrowego, ramy nadzoru ustanowione w niniejszym rozporządzeniu powinny obejmować dostawców usług chmurowych.

(21)[10] Aby zachować pełną kontrolę nad ryzykiem związanym z ICT, podmioty finansowe muszą posiadać kompleksowe umiejętności umożliwiające solidne i skuteczne zarządzanie ryzykiem związanym z ICT, wraz z konkretnymi mechanizmami oraz strategiami dotyczącymi obsługi wszystkich incydentów związanych z ICT oraz zgłaszania najpoważniejszych z nich. Podmioty finansowe powinny również dysponować strategiami na potrzeby testowania systemów, mechanizmów kontrolnych i procesów ICT, a także zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT. Należy podwyższyć podstawowy poziom operacyjnej odporności cyfrowej w odniesieniu do podmiotów finansowych, umożliwiając jednocześnie proporcjonalne stosowanie wymogów w odniesieniu do niektórych podmiotów finansowych, zwłaszcza mikroprzedsiębiorstw, a także podmiotów finansowych objętych uproszczonymi ramami zarządzania ryzykiem związanym z ICT. Aby ułatwić skuteczny nadzór nad instytucjami pracowniczych programów emerytalnych, który jest proporcjonalny i uwzględnia potrzebę zmniejszenia obciążeń administracyjnych dla właściwych organów, w odniesieniu do takich podmiotów finansowych w odpowiednich krajowych mechanizmach nadzoru należy uwzględnić wielkość tych podmiotów i ich ogólny profil ryzyka oraz charakter, skalę i stopień złożoności realizowanych usług, działań i operacji, nawet w przypadku gdy przekroczone zostały odpowiednie progi określone w art. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2341[11]. W szczególności działania nadzorcze powinny się koncentrować przede wszystkim na konieczności zwalczania poważnych zagrożeń w kontekście zarządzania ryzykiem związanym z ICT w odniesieniu do poszczególnych podmiotów.

Właściwe organy powinny również zachować ostrożne, lecz proporcjonalnego podejście w kwestii nadzoru nad instytucjami pracowniczych programów emerytalnych, które – zgodnie z art. 31 dyrektywy (UE) 2016/2341 – zlecają usługodawcom w drodze outsourcingu znaczną część swojej podstawowej działalności, m.in. zarządzanie aktywami, obliczenia aktuarialne, księgowość i zarządzanie danymi.

(22) Progi i taksonomie dotyczące zgłaszania incydentów związanych z ICT różnią się znacznie na szczeblu krajowym. Chociaż płaszczyznę porozumienia można osiągnąć dzięki odpowiednim pracom podejmowanym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) ustanowioną rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881[12] i grupę współpracy zgodnie z dyrektywą (UE) 2022/2555, rozbieżne podejścia do ustalania progów i stosowania taksonomii nadal istnieją lub mogą pojawić się w przypadku pozostałych podmiotów finansowych. Ze względu na te rozbieżności wprowadzono liczne wymogi, które podmioty finansowe muszą spełnić, zwłaszcza w sytuacji, gdy prowadzą działalność w kilku unijnych państwach członkowskich i gdy są częścią grupy finansowej. Ponadto takie rozbieżności mogą utrudniać tworzenie dalszych jednolitych lub scentralizowanych unijnych mechanizmów przyspieszających proces zgłaszania oraz wspierających szybką i sprawną wymianę informacji między właściwymi organami, co ma zasadnicze znaczenie dla zwalczania ryzyka związanego z ICT w przypadku ataków na wielką skalę, które mogą mieć konsekwencje systemowe.

(23) Aby zmniejszyć obciążenie administracyjne i potencjalnie powielające się obowiązki w zakresie zgłaszania incydentów w odniesieniu do niektórych podmiotów finansowych, obowiązek zgłaszania incydentów zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366[13] nie powinien mieć zastosowania do dostawców usług płatniczych, którzy są objęci zakresem stosowania niniejszego rozporządzenia. W związku z tym instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje płatnicze i dostawcy świadczący usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 tej dyrektywy, powinni zgłaszać od daty stosowania niniejszego rozporządzenia – zgodnie z niniejszym rozporządzeniem – wszelkie incydenty operacyjne lub incydenty w zakresie bezpieczeństwa związane z płatnościami, które wcześniej były zgłaszane zgodnie z tą dyrektywą, niezależnie od tego, czy są one związane z ICT.

(24) Aby umożliwić właściwym organom wykonywanie zadań nadzorczych poprzez uzyskanie pełnego przeglądu charakteru, częstotliwości, znaczenia i skutków incydentów związanych z ICT oraz aby wzmocnić

wymianę informacji między właściwymi organami publicznymi, w tym organami ścigania i organami ds. restrukturyzacji i uporządkowanej likwidacji, w niniejszym rozporządzeniu należy ustanowić solidny system zgłaszania incydentów związanych z ICT przewidujący odpowiednie wymogi, które wyeliminowałyby obecne luki w przepisach dotyczących usług finansowych, oraz usunąć istniejące pokrywające się i dublujące przepisy w celu obniżenia kosztów. Podstawowe znaczenie ma harmonizacja systemu zgłaszania incydentów związanych z ICT poprzez zobowiązanie wszystkich podmiotów finansowych do zgłaszania ich właściwym organom za pomocą jednolitych usprawnionych ram, zgodnie z niniejszym rozporządzeniem. Ponadto należy przyznać EUN uprawnienia do doprecyzowania istotnych elementów na potrzeby ram zgłaszania incydentów związanych z ICT, takich jak taksonomia, ramy czasowe, zbiory danych, wzory i mające zastosowanie progi. Aby zapewnić pełną zgodność z dyrektywą (UE) 2022/2555, podmioty finansowe powinny mieć możliwość dobrowolnego zgłaszania znaczących cyberzagrożeń odpowiedniemu właściwemu organowi, jeżeli uznają dane cyberzagrożenie za istotne dla systemu finansowego, użytkowników usług lub klientów.

(25) Wymogi w zakresie testowania operacyjnej odporności cyfrowej zostały opracowane w niektórych podsektorach finansowych i określają ramy, które nie zawsze są w pełni dostosowane. Prowadzi to do potencjalnego dublowania kosztów transgranicznych podmiotów finansowych i komplikuje wzajemne uznawanie wyników testowania operacyjnej odporności cyfrowej, co z kolei może spowodować fragmentację rynku wewnętrznego.

(26) Dodatkowo, w przypadku braku wymogu testowania w zakresie ICT, podatności pozostają niewykryte i powodują narażenie podmiotów finansowych na ryzyko związane z ICT, a ostatecznie stwarzają większe ryzyko dla stabilności i integralności sektora finansowego. Bez interwencji Unii testowanie operacyjnej odporności cyfrowej pozostałoby niejednolite i nie istniałby system wzajemnego uznawania wyników testowania w zakresie ICT między różnymi jurysdykcjami. Ponadto, biorąc pod uwagę, że prawdopodobieństwo przyjęcia przez inne podsektory finansowe systemów testowania na szeroką skalę jest niewielkie, ominęłyby je potencjalne korzyści wynikające z ram testowania, takie jak ujawnianie podatności i zagrożeń w zakresie ICT oraz testowanie zdolności obronnych i ciągłości działania, co przyczynia się do zwiększenia zaufania konsumentów, dostawców i partnerów biznesowych. Aby zlikwidować te pokrywające się przepisy oraz rozbieżności i luki w przepisach, należy wprowadzić przepisy dotyczące skoordynowanego systemu testowania, ułatwiając tym samym wzajemne uznawanie zaawansowanego testowania w odniesieniu do podmiotów finansowych, które spełniają kryteria określone w niniejszym rozporządzeniu.

(27) Zależność podmiotów finansowych od korzystania z usług ICT wynika częściowo z ich potrzeby dostosowania się do powstającej konkurencyjnej globalnej gospodarki cyfrowej, zwiększenia skuteczności ich działalności oraz zaspokojenia potrzeb konsumentów. Charakter i zakres takiej zależności stale zmieniał się w ostatnich latach, co przyczyniło się do obniżenia kosztów pośrednictwa finansowego, umożliwienia rozszerzania działalności i skalowalności w ramach prowadzenia działalności finansowej, przy jednoczesnym zapewnieniu szerokiego zakresu narzędzi ICT służących zarządzaniu złożonymi procesami wewnętrznymi.

(28) O takim intensywnym korzystaniu z usług ICT świadczą złożone ustalenia umowne, przy czym podmioty finansowe często napotykają trudności podczas negocjacji warunków umownych, które byłyby dostosowane do standardów ostrożnościowych lub innych wymogów regulacyjnych, którym podlegają, lub podczas innego rodzaju egzekwowania konkretnych praw, takich jak prawa dostępu lub prawa do audytu, nawet jeżeli te ostatnie są zapisane w umowach. Ponadto w wielu tych ustaleniach umownych nie przewidziano wystarczających gwarancji umożliwiających pełnoprawne monitorowanie procesów podwykonawstwa, pozbawiając tym samym podmioty finansowe możliwości oceny powiązanych zagrożeń. Ponadto biorąc pod uwagę, że zewnętrzni dostawcy usług ICT często świadczą wystandaryzowane usługi na rzecz różnego rodzaju klientów, takie ustalenia umowne nie zawsze odpowiednio uwzględniają indywidualne lub szczególne potrzeby podmiotów sektora finansowego.

(29) Chociaż unijne przepisy dotyczące usług finansowych zawierają kilka ogólnych przepisów dotyczących outsourcingu, monitorowanie wymiaru umownego nie jest w pełni zakorzenione w unijnym prawodawstwie. Z uwagi na brak wyraźnych i dostosowanych do potrzeb standardów unijnych, które miałyby zastosowanie do ustaleń umownych zawieranych z zewnętrznymi dostawcami usług ICT, nie można kompleksowo uwzględnić zewnętrznego źródła ryzyka związanego z ICT. W związku z tym konieczne jest określenie pewnych najważniejszych zasad mających wyznaczać kierunek zarządzania przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT, które to zasady mają szczególne znaczenie w przypadku, gdy podmioty finansowe korzystają z zewnętrznych dostawców usług ICT w celu wspierania ich krytycznych lub istotnych funkcji. Zasadom tym powinien towarzyszyć zestaw podstawowych praw umownych związanych z kilkoma elementami związanymi z wykonywaniem i wypowiadaniem ustaleń umownych w celu zapisania pewnych minimalnych zabezpieczeń w celu wzmocnienia zdolności podmiotów finansowych do skutecznego monitorowania wszystkich zagrożeń w zakresie ICT

powstających na poziomie zewnętrznych dostawców usług. Zasady te stanowią uzupełnienie przepisów sektorowych mających zastosowanie do outsourcingu.

(30) Obecnie oczywiste jest, że nie ma wystarczającej jednorodności i spójności w monitorowaniu ryzyka ze strony zewnętrznych dostawców usług ICT oraz zależności od zewnętrznych dostawców usług ICT. Pomimo działań odnoszących się do outsourcingu, m.in. w postaci wytycznych EUNB w sprawie outsourcingu z 2019 r. oraz zaleceń ESMA w sprawie outsourcingu zlecanego dostawcom usług chmurowych z 2021 r., w unijnych przepisach niewystarczającą uwagę poświęca się szerszemu problemowi przeciwdziałania ryzyku systemowemu, które może powstać w wyniku kontaktu sektora finansowego z ograniczoną liczbą kluczowych zewnętrznych dostawców usług ICT. Ten brak przepisów na szczeblu unijnym jest spotęgowany brakiem krajowych przepisów dotyczących kompetencji i narzędzi umożliwiających organom nadzoru finansowego osiągnięcie właściwego zrozumienia zależności od zewnętrznych dostawców usług ICT i odpowiednie monitorowanie zagrożeń wynikających z koncentracji zależności od zewnętrznych dostawców usług ICT.

(31) Biorąc pod uwagę potencjalne ryzyko systemowe spowodowane rozpowszechnieniem się praktyk dotyczących out-sourcingu oraz koncentracją zewnętrznych dostawców usług ICT, a także mając na uwadze niewystarczający charakter krajowych mechanizmów, by zapewnić organom nadzoru finansowego odpowiednie narzędzia umożliwiające określanie ilościowo i jakościowo konsekwencji ryzyka związanego z ICT występującego u kluczowych zewnętrznych dostawców usług ICT, a także łagodzenie tych konsekwencji, konieczne jest ustanowienie odpowiednich ram nadzoru umożliwiających stałe monitorowanie działań zewnętrznych dostawców usług ICT będących kluczowymi zewnętrznymi dostawcami usług ICT dla podmiotów finansowych, z zapewnieniem poufności i bezpieczeństwa klientom innym niż podmioty finansowe. Choć świadczenie usług ICT wewnątrz grupy wiąże się z konkretnym ryzykiem i konkretnymi korzyściami, nie należy go automatycznie uznawać za mniej ryzykowne niż świadczenie usług ICT przez dostawców spoza grupy finansowej, a tym samym powinno ono być objęte tymi samymi ramami regulacyjnymi. Niemniej jednak w przypadku gdy usługi ICT są świadczone w ramach tej samej grupy finansowej, podmioty finansowe mogą mieć większą kontrolę nad dostawcami wewnątrz grupy, co należy uwzględnić w ogólnej ocenie ryzyka.

(32) W związku z tym, że ryzyka związane z ICT stają się coraz bardziej złożone i zaawansowane, solidne środki wykrywania ryzyka w zakresie ICT i zapobiegania mu zależą w dużej mierze od regularnej wymiany analiz zagrożeń i podatności między podmiotami finansowymi. Wymiana informacji przyczynia się do zwiększania świadomości na temat cyberzagrożeń. To z kolei wzmacnia zdolność podmiotów finansowych do zapobiegania przekształcaniu się cyberzagrożeń w realne incydenty związane z ICT oraz umożliwia podmiotom finansowym skuteczniejsze ograniczanie skutków incydentów związanych z ICT oraz szybsze przywracanie sprawności. Wydaje się, że wobec braku wytycznych na szczeblu Unii szereg czynników ogranicza taką wymianę analiz, zwłaszcza niepewność co do zgodności z ochroną danych osobowych, przepisami antymonopolowymi i zasadami dotyczącymi odpowiedzialności.

(33) Ponadto wątpliwości dotyczące rodzaju informacji, które można udostępnić innym uczestnikom rynku lub organom innym niż organy nadzoru (takim jak ENISA, w przypadku wkładu analitycznego, lub Europol – w celu egzekwowania prawa), skutkują wstrzymaniem przekazywania przydatnych informacji. W związku z tym obecnie zakres i jakość wymiany informacji pozostają ograniczone i podzielone, a istotne wymiany przeprowadzane są w większości lokalnie (za pośrednictwem inicjatyw krajowych) oraz bez żadnych spójnych ogólnounijnych ustaleń w zakresie wymiany informacji dostosowanych do potrzeb zintegrowanego systemu finansowego. Trzeba zatem wzmocnić te kanały komunikacyjne.

(34) Należy zachęcać podmioty finansowe, by wymieniały między sobą informacje i analizy na temat cyberzagrożeń oraz by wspólnie wykorzystywały swoją indywidualną wiedzę i praktyczne doświadczenie na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed cyberzagrożeniami i reagowania na cyberzagrożenia poprzez udział w rozwiązaniach mających na celu wymianę informacji. W związku z tym konieczne jest umożliwienie powstania na szczeblu Unii mechanizmów ustaleń dotyczących dobrowolnej wymiany informacji, które – pod warunkiem wdrożenia w zaufanych środowiskach – pomogłyby społeczności sektora finansowego zapobiegać cyberzagrożeniom i wspólnie na nie reagować poprzez szybkie ograniczenie rozpowszechnienia ryzyka związanego z ICT i utrudnienie wystąpienia potencjalnego efektu domina we wszystkich kanałach finansowych. Mechanizmy te powinny być zgodne z mającymi zastosowanie unijnymi zasadami prawa konkurencji określonymi w komunikacie Komisji z dnia 14 stycznia 2011 r. zatytułowanym „Wytyczne w sprawie stosowania art. 101 Traktatu o funkcjonowaniu Unii Europejskiej do horyzontalnych porozumień kooperacyjnych", a także z unijnymi przepisami o ochronie danych, w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[14]. Powinny one działać w oparciu o co najmniej jedną z podstaw prawnych ustanowionych w art. 6 tego rozporządzenia, np. w kontekście przetwarzania danych osobowych, które jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, o czym jest mowa w art. 6 ust. 1 lit. f) tego rozporządzenia, a także w kontekście

przetwarzania danych osobowych niezbędnych do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędnych do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, o czym mowa, odpowiednio, w art. 6 ust. 1 lit. c) i e) tego rozporządzenia.

(35) Aby utrzymać wysoki poziom operacyjnej odporności cyfrowej całego sektora finansowego, a jednocześnie dotrzymać kroku rozwojowi technologicznemu, niniejsze rozporządzenie powinno zwalczać ryzyko wynikające ze wszystkich rodzajów usług ICT. W tym celu definicję usług ICT w kontekście niniejszego rozporządzenia należy rozumieć szeroko jako obejmującą usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego. Definicja ta powinna na przykład obejmować tzw. usługi OTT, które należą do kategorii usług łączności elektronicznej. Powinna wyłączać jedynie ograniczoną kategorię tradycyjnych usług telefonii analogowej kwalifikujących się jako usługi publicznej komutowanej sieci telefonicznej (PSTN), usługi z wykorzystaniem linii naziemnej, podstawowej usługi telefonicznej (POTS) lub usługi telefonii stacjonarnej.

(36) Niezależnie od szerokiego zakresu stosowania przewidzianego w niniejszym rozporządzeniu, stosując zasady dotyczące operacyjnej odporności cyfrowej, należy uwzględniać istotne różnice między podmiotami finansowymi pod względem ich wielkości i ogólnego profilu ryzyka. Co do zasady, rozdzielając zasoby i zdolności na wdrażanie ram zarządzania ryzykiem związanym z ICT, podmioty finansowe powinny należycie dostosować swoje potrzeby związane z ICT do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności realizowanych usług, działań i operacji, natomiast właściwe organy powinny nadal oceniać i weryfikować podejście do takiego rozdziału.

(37) Dostawcy świadczący usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366, są wyraźnie włączeni do zakresu stosowania niniejszego rozporządzenia, z uwzględnieniem szczególnego charakteru ich działalności i wynikającego z niej ryzyka. Dodatkowo instytucje pieniądza elektronicznego i instytucje płatnicze, zwolnione zgodnie z art. 9 ust. 1 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE[15] oraz art. 32 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366, zostają włączone do zakresu stosowania niniejszego rozporządzenia, nawet jeżeli nie udzielono im zezwolenia na emisję pieniądza elektronicznego lub nie udzielono im zezwolenia na świadczenie i wykonywanie usług płatniczych zgodnie z dyrektywą (UE) 2015/2366. Niemniej jednak instytucje świadczące żyro pocztowe, o których mowa w art. 2 ust. 5 pkt 3) dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE[16], są wyłączone z zakresu stosowania niniejszego rozporządzenia. Właściwymi organami instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366, instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE i dostawców świadczących usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366, są właściwe organy wyznaczone zgodnie z art. 22 dyrektywy (UE) 2015/2366.

(38) Ponieważ większe podmioty finansowe mogą korzystać z większych zasobów i są w stanie szybko przeznaczyć środki finansowe na opracowanie struktur zarządzania i stworzenie szeregu strategii korporacyjnych, wymóg tworzenia bardziej złożonych rozwiązań w zakresie zarządzania należy nałożyć wyłącznie na podmioty finansowe, które nie są mikroprzedsiębiorstwami w rozumieniu niniejszego rozporządzenia. Podmioty takie są lepiej przygotowane w szczególności do ustanowienia specjalnych stanowisk w strukturach zarządzania w celu nadzorowania ustaleń umownych z zewnętrznymi dostawcami usług ICT lub w celu zarządzania kryzysowego, do organizowania zarządzania w zakresie ryzyka związanego z ICT zgodnie z modelem trzech linii obrony lub do ustanowienia wewnętrznego modelu zarządzania ryzykiem i kontroli ryzyka oraz do poddania swoich ram zarządzania ryzykiem związanym z ICT audytowi wewnętrznemu.

(39) Niektóre podmioty finansowe korzystają ze zwolnień lub są objęte bardzo łagodnymi ramami regulacyjnymi na mocy odpowiednich przepisów sektorowych prawa Unii. Takie podmioty finansowe obejmują zarządzających alternatywnymi funduszami inwestycyjnymi, o których mowa w art. 3 ust. 2 dyrektywy Parlamentu Europejskiego i Rady 2011/61/UE[17], zakłady ubezpieczeń i zakłady reasekuracji, o których mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE[18], oraz instytucje pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników. W świetle tych zwolnień włączenie takich podmiotów finansowych do zakresu stosowania niniejszego rozporządzenia nie byłoby proporcjonalne. Dodatkowo w niniejszym rozporządzeniu uznaje się specyfikę struktury rynku pośrednictwa ubezpieczeniowego, w związku z czym pośrednicy ubezpieczeniowi, pośrednicy reasekuracyjni i pośrednicy oferujący ubezpieczenia uzupełniające kwalifikujący się jako mikroprzedsiębiorstwa, czy małe lub średnie przedsiębiorstwa, nie powinni podlegać niniejszemu rozporządzeniu.

(40) Ponieważ podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE, są wyłączone z zakresu stosowania tej dyrektywy, państwa członkowskie powinny w związku z tym mieć możliwość podjęcia decyzji o zwolnieniu takich podmiotów mających siedzibę na ich odpowiednich terytoriach z zakresu stosowania niniejszego rozporządzenia.

(41) Analogicznie, aby dostosować niniejsze rozporządzenie do zakresu stosowania dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE[19], z zakresu stosowania niniejszego rozporządzenia należy wyłączyć osoby fizyczne i prawne, o których mowa w art. 2 i 3 tej dyrektywy, które posiadają zezwolenie na świadczenie usług inwestycyjnych bez konieczności uzyskiwania zezwolenia na mocy dyrektywy 2014/65/UE. Niemniej jednak w art. 2 dyrektywy 2014/65/UE wyłącza się z zakresu stosowania tej dyrektywy podmioty, które kwalifikują się jako podmioty finansowe do celów niniejszego rozporządzenia, takie jak centralne depozyty papierów wartościowych, przedsiębiorstwa zbiorowego inwestowania lub zakłady ubezpieczeń i zakłady reasekuracji. Wyłączenie osób i podmiotów, o których mowa w art. 2 i 3 tej dyrektywy, z zakresu stosowania niniejszego rozporządzenia nie powinno obejmować tych centralnych depozytów papierów wartościowych, przedsiębiorstw zbiorowego inwestowania ani zakładów ubezpieczeń czy reasekuracji.

(42) Na mocy przepisów sektorowych prawa Unii niektóre podmioty finansowe – ze względu na ich wielkość lub świadczone usługi – są objęte łagodniejszymi wymogami lub zwolnieniami. Ta kategoria podmiotów finansowych obejmuje małe i niepowiązane wzajemnie firmy inwestycyjne oraz małe instytucje pracowniczych programów emerytalnych, które mogą być wyłączone z zakresu stosowania dyrektywy (UE) 2016/2341 na warunkach określonych w art. 5 tej dyrektywy przez odnośne państwa członkowskie i które obsługują programy emerytalne liczące łącznie nie więcej niż 100 uczestników, a także instytucje zwolnionych na mocy dyrektywy 2013/36/UE. W związku z tym zgodnie z zasadą proporcjonalności oraz w celu zachowania ducha przepisów sektorowych prawa Unii te podmioty finansowe również należy objąć uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia. Regulacyjne standardy techniczne, które mają zostać opracowane przez EUN, nie powinny zmieniać proporcjonalnego charakteru ram zarządzania ryzykiem związanym z ICT obejmujących te podmioty finansowe. Ponadto, zgodnie z zasadą proporcjonalności, uproszczone ramy zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny też obejmować instytucje płatnicze, o których mowa w art. 32 ust. 1 dyrektywy (UE) 2015/2366, i instytucje pieniądza elektronicznego, o których mowa w art. 9 dyrektywy 2009/110/WE, zwolnione zgodnie z krajowymi przepisami transponującymi te unijne akty prawne, przy czym instytucje płatnicze i instytucje pieniądza elektronicznego, które nie zostały zwolnione zgodnie z odpowiednimi krajowymi przepisami transponującymi przepisy sektorowe prawa Unii, powinny przestrzegać ogólnych ram ustanowionych w niniejszym rozporządzeniu.

(43)[20] Analogicznie podmioty finansowe, które kwalifikują się jako mikroprzedsiębiorstwa lub są objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia, nie powinny być zobowiązane do ustanowienia funkcji polegającej na monitorowaniu uzgodnień zawartych z zewnętrznymi dostawcami usług ICT w sprawie korzystania z usług ICT; do wyznaczenia członka kadry kierowniczej wyższego szczebla jako odpowiedzialnego za nadzorowanie związanej z tym ekspozycji na ryzyko i odpowiedniej dokumentacji; do powierzenia obowiązku zarządzania ryzykiem związanym z ICT i sprawowania nadzoru nad nim przez funkcję kontroli i zapewnienia odpowiedniego stopnia niezależności takiej funkcji kontroli w celu uniknięcia konfliktów interesów; do dokumentowania uproszczonych ram zarządzania ryzykiem związanym z ICT; poddawania ich przeglądowi co najmniej raz w roku; do ich regularnego poddawania audytowi wewnętrznemu; do przeprowadzania dogłębnych ocen po istotnych zmianach w ich infrastrukturze sieci i systemów informatycznych oraz powiązanych procedurach, do regularnego przeprowadzania analiz ryzyka w odniesieniu do przestarzałych systemów ICT, do poddawania wdrażania planów reagowania i przywracania sprawności ICT niezależnym wewnętrznym przeglądom audytowym, do posiadania funkcji zarządzania w sytuacji kryzysowej, do rozszerzenia zakresu testowania ciągłości działania oraz planów reagowania i przywracania sprawności w celu uwzględnienia scenariuszy pracy awaryjnej obejmujących przełączanie się z podstawowej infrastruktury ICT na urządzenia redundantne, do zgłaszania właściwym organom, na ich żądanie, szacunkowych łącznych rocznych kosztów i strat spowodowanych poważnymi incydentami związanymi z ICT, do utrzymywania nadmiarowych zdolności w zakresie ICT, do informowania właściwych organów krajowych o zmianach wdrożonych w następstwie przeglądów przeprowadzonych po wystąpieniu incydentu związanego z ICT, do ciągłego monitorowania odpowiednich zmian technologicznych, do ustanowienia kompleksowego programu testowania operacyjnej odporności cyfrowej stanowiącego integralną część ram zarządzania ryzykiem związanym z ICT przewidzianych w niniejszym rozporządzeniu ani do przyjęcia strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT i dokonywania jej regularnego przeglądu. Dodatkowo mikroprzedsiębiorstwa powinny być zobowiązane do oceny potrzeby utrzymywania takich nadmiarowych zdolności w zakresie ICT w oparciu o ich profil ryzyka. Mikroprzedsiębiorstwa powinny korzystać z bardziej elastycznego systemu w odniesieniu do programów testowania operacyjnej odporności cyfrowej. Rozważając rodzaj i częstotliwość przeprowadzanych testów, mikroprzedsiębiorstwa powinny odpowiednio wyważyć cel polegający na utrzymaniu wysokiej operacyjnej odporności cyfrowej, dostępne zasoby i ich ogólny profil ryzyka. Mikroprzedsiębiorstwa i podmioty finansowe objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny być zwolnione z obowiązku przeprowadzania zaawansowanego

testowania narzędzi, systemów i procesów ICT z wykorzystaniem testów penetracyjnych ukierunkowanych przez analizę zagrożeń (TLPT), jako że taki obowiązek powinien dotyczyć wyłącznie podmiotów finansowych spełniających kryteria określone w niniejszym rozporządzeniu. Ze względu na swoje ograniczone możliwości mikroprzedsiębiorstwa powinny mieć możliwość uzgodnienia z zewnętrznym dostawcą usług ICT, że przysługujące danemu podmiotowi finansowemu prawa dostępu, kontroli i audytu zostaną przekazane niezależnemu podmiotowi trzeciemu, który zostanie wyznaczony przez zewnętrznego dostawcę usług ICT, pod warunkiem że dany podmiot finansowy będzie mógł w dowolnym momencie zwrócić się do odpowiedniego niezależnego podmiotu trzeciego o wszystkie istotne informacje na temat wyników zewnętrznego dostawcy usług ICT i o poświadczenie tych wyników.

(44)[21] Ponieważ jedynie od podmiotów finansowych objętych zaawansowanym testowaniem odporności cyfrowej powinno wymagać się przeprowadzenia testów penetracyjnych ukierunkowanych przez analizę zagrożeń, procesy administracyjne i koszty finansowe związane z przeprowadzeniem takich testów powinny być ponoszone przez niewielki odsetek podmiotów finansowych.

(45) Aby zapewnić pełną zgodność i ogólną spójność między strategiami biznesowymi poszczególnych podmiotów finansowych a zarządzaniem ryzykiem związanym z ICT, należy zobowiązać organy zarządzające tych podmiotów finansowych do utrzymania kluczowej i aktywnej roli w kierowaniu i dostosowywaniu ram zarządzania ryzykiem związanym z ICT oraz ogólnej strategii w zakresie operacyjnej odporności cyfrowej. W podejściu, które przyjmą organy zarządzające, należy nie tylko skoncentrować się na środkach zapewniających odporność systemów ICT, ale także uwzględnić ludzi i procesy poprzez zestaw polityk, w których na każdym szczeblu struktury korporacyjnej i w odniesieniu do wszystkich pracowników buduje się świadomość czynników ryzyka w cyberprzestrzeni i zaangażowanie na rzecz ścisłego przestrzegania zasad w zakresie higieny cyberbezpieczeństwa na wszystkich szczeblach. Ostateczna odpowiedzialność organu zarządzającego za zarządzanie w zakresie ryzyka związanego z ICT podmiotu finansowego powinna stanowić nadrzędną zasadę w tym kompleksowym podejściu, przekładającą się dodatkowo na ciągłe zaangażowanie organu zarządzającego w kontrolę monitorowania zarządzania w zakresie ryzyka związanego z ICT.

(46) Co więcej, zasada pełnej i ostatecznej odpowiedzialności organu zarządzającego za zarządzanie ryzykiem związanym z ICT podmiotu finansowego idzie w parze z koniecznością zabezpieczenia poziomu inwestycji związanych z ICT oraz ogólnego budżetu podmiotu finansowego, tak aby podmiot ten mógł osiągnąć wysoki poziom operacyjnej odporności cyfrowej.

(47) W niniejszym rozporządzeniu, inspirowanym odpowiednimi międzynarodowymi, krajowymi i sektorowymi najlepszymi praktykami, wytycznymi, zaleceniami i podejściami w zakresie zarządzania ryzykiem w cyberprzestrzeni, promuje się zestaw zasad ułatwiających ustanowienie ogólnej struktury zarządzania ryzykiem związanym z ICT. Tym samym, dopóki podstawowe możliwości wprowadzane przez podmioty finansowe odpowiadają różnym funkcjom w ramach zarządzania ryzykiem związanym z ICT (identyfikacja, ochrona i zapobieganie, wykrywanie, reagowanie i przywracanie sprawności, uczenie się i rozwój oraz komunikacja) określonym w niniejszym rozporządzeniu, podmioty finansowe powinny zachować swobodę korzystania z modeli zarządzania ryzykiem związanym z ICT, dla których opracowano inne ramy lub kategorie.

(48) Aby nadążyć za zmieniającym się krajobrazem cyberzagrożeń, podmioty finansowe powinny na bieżąco aktualizować systemy ICT, które muszą być niezawodne i posiadać zdolność nie tylko do zagwarantowania przetwarzania danych niezbędnych do świadczenia ich usług, ale również do zapewnienia wystarczającej odporności technologicznej pozwalającej podmiotom finansowym na odpowiednie zaspokajanie dodatkowych potrzeb w zakresie przetwarzania danych, jakie mogą wynikać z trudnych warunków rynkowych lub innych niekorzystnych sytuacji.

(49)[22] Skuteczne plany ciągłości działania i plany przywracania sprawności są konieczne, aby umożliwić podmiotom finansowym szybkie i sprawne rozwiązywanie incydentów związanych z ICT, w szczególności cyberataków, poprzez ograniczenie szkód i priorytetowe traktowanie wznowienia działalności i działań naprawczych zgodnie z ich politykami dotyczącymi zarządzania kopiami zapasowymi. Takie wznowienie działalności nie powinno jednak w żaden sposób zagrażać integralności i bezpieczeństwu sieci i systemów informatycznych lub dostępności, autentyczności, integralności czy poufności danych.

(50) Choć niniejsze rozporządzenie pozwala podmiotom finansowym na określenie w sposób elastyczny zakładanego czasu przywrócenia systemów i akceptowalny poziom utraty danych, a tym samym na wyznaczanie go poprzez pełne uwzględnienie charakteru i krytyczności danych funkcji oraz wszelkich szczególnych potrzeb biznesowych, powinno jednak nakładać na te podmioty wymóg przeprowadzenia oceny potencjalnego ogólnego wpływu na efektywność rynku przy określaniu takich celów.

(51) Inicjatorzy cyberataków zwykle dążą do osiągnięcia zysków finansowych bezpośrednio u źródła, narażając tym samym podmioty finansowe na poważne konsekwencje. Aby zapobiec niedostępności lub utracie integralności systemów ICT, a tym samym by uniknąć naruszeń poufnych danych i uszkodzeń fizycznej infrastruktury ICT, należy znacznie usprawnić i uprościć procedurę zgłaszania przez podmioty finansowe poważnych incydentów związanych z ICT. Procedurę zgłaszania incydentów związanych

z ICT należy ujednolicić: wszystkie podmioty finansowe powinny być zobowiązane do zgłaszania tych incydentów bezpośrednio do swoich odpowiednich właściwych organów. W przypadku gdy nadzór nad podmiotem finansowym sprawuje więcej niż jeden właściwy organ krajowy, państwa członkowskie powinny wyznaczyć jeden właściwy organ do celów takich zgłoszeń. Instytucje kredytowe sklasyfikowane jako istotne zgodnie z art. 6 ust. 4 rozporządzenia Rady (UE) nr 1024/2013[23] powinny przekazywać takie zgłoszenia właściwym organom krajowym, które następnie powinny przekazać stosowne sprawozdanie Europejskiemu Bankowi |Centralnemu (EBC).

(52) Bezpośrednie zgłaszanie incydentów powinno umożliwić organom nadzoru finansowego natychmiastowy dostęp do informacji na temat poważnych incydentów związanych z ICT. Organy nadzoru finansowego powinny z kolei przekazywać szczegółowe informacje na temat takich poważnych incydentów związanych z ICT organom publicznym spoza sektora finansowego (takim jak właściwe organy i pojedyncze punkty kontaktowe na mocy dyrektywy (UE) 2022/2555, krajowe organy ochrony danych i organom ścigania w przypadku poważnych incydentów o charakterze przestępczym związanych z ICT), aby zwiększyć wiedzę takich organów o takich incydentach oraz – w przypadku CSIRT – ułatwić szybką pomoc, której można udzielić podmiotom finansowym, stosownie do przypadku. Dodatkowo państwa członkowskie powinny mieć możliwość określenia, że to same podmioty finansowe powinny przekazywać takie informacje organom publicznym spoza obszaru usług finansowych. Te przepływy informacji powinny umożliwić podmiotom finansowym szybkie korzystanie z wszelkich istotnych informacji technicznych, porad dotyczących środków zaradczych oraz działań następczych ze strony takich organów. Informacje na temat poważnych incydentów związanych z ICT powinny być wzajemnie przekazywane: organy sprawujące nadzór finansowy powinny przekazywać podmiotowi finansowemu wszelkie niezbędne informacje zwrotne lub wytyczne, natomiast EUN powinny udostępniać zanonimizowane dane na temat cyberzagrożeń i podatności związanych z danym incydentem, aby wspomóc szerzej pojętą zbiorową obronę.

(53) Chociaż wszystkie podmioty finansowe powinny być objęte wymogiem zgłaszania incydentów, przewiduje się, że wymóg ten nie będzie wszystkich ich obciążać w ten sam sposób. Odpowiednie progi w zakresie istotności i ramy czasowe zgłaszania incydentów powinny być należycie dostosowane, w kontekście aktów delegowanych opartych na regulacyjnych standardach technicznych, które mają zostać opracowane przez EUN, tak by uwzględniać jedynie poważne incydenty związane z ICT. Dodatkowo przy określaniu ram czasowych do celów obowiązków w zakresie zgłaszania incydentów należy uwzględnić specyfikę podmiotów finansowych.

(54) Niniejsze rozporządzenie powinno nakładać na instytucje kredytowe, instytucje płatnicze, dostawców świadczących usługę dostępu do informacji o rachunku i instytucje pieniądza elektronicznego wymóg zgłaszania wszelkich incydentów operacyjnych lub w zakresie bezpieczeństwa związanych z płatnościami, które wcześniej były zgłaszane na mocy dyrektywy (UE) 2015/2366, niezależnie od tego, czy są one związane z ICT.

(55) EUN należy powierzyć zadanie polegające na ocenie możliwości i warunków ewentualnej centralizacji zgłoszeń dotyczących incydentów związanych z ICT na szczeblu Unii. Taka centralizacja mogłaby obejmować jeden unijny węzeł informacyjny na potrzeby zgłaszania poważnych incydentów związanych z ICT, który by otrzymywał odpowiednie zgłoszenia bezpośrednio i automatycznie powiadamiał właściwe organy krajowe albo który by służył jedynie jako centralne miejsce do przekazywania odpowiednich zgłoszeń przez właściwe organy krajowe i tym samym pełnił funkcję koordynującą. EUN należy powierzyć zadanie polegające na przygotowaniu, w porozumieniu z EBC i ENISA, wspólnego sprawozdania badającego możliwość ustanowienia takiego jednego unijnego węzła informacyjnego.

(56)[24] W celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej oraz zgodnie zarówno z odpowiednimi standardami międzynarodowymi (np. określonymi przez G-7 podstawowymi elementami dotyczącymi testów penetracyjnych ukierunkowanych przez analizę zagrożeń), jak i ramami stosowanymi w Unii, takimi jak TIBER-EU, podmioty finansowe powinny regularnie testować swoje systemy ICT i personel wykonujący obowiązki związane z ICT pod kątem skuteczności ich zdolności w zakresie zapobiegania, wykrywania, reagowania i przywracania sprawności, aby wykrywać i eliminować potencjalne podatności w zakresie ICT. Aby odzwierciedlić różnice istniejące między różnymi podsektorami finansowymi i w ramach tych podsektorów w zakresie gotowości podmiotów finansowych do reagowania w obszarze cyberbezpieczeństwa, testowanie powinno obejmować szeroki zakres narzędzi i działań, począwszy od oceny podstawowych wymogów (np. oceny podatności i skanowanie pod tym kątem, analizy otwartych źródeł informacji, oceny bezpieczeństwa sieci, analizy luk, kontrole bezpieczeństwa fizycznego, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, w miarę możliwości przeglądy kodu źródłowego, testy scenariuszowe, testy kompatybilności, testy wydajności lub testy kompleksowe) aż po bardziej zaawansowane testowanie przy użyciu TLPT. Takie zaawansowane testowanie powinno być wymagane jedynie w przypadku podmiotów finansowych wystarczająco zaawansowanych z punktu widzenia ICT, aby były w stanie przeprowadzić takie testy. Wymagane w niniejszym rozporządzeniu testowanie operacyjnej odporności cyfrowej powinno być zatem bardziej rygorystyczne

dla podmiotów finansowych spełniających kryteria określone w niniejszym rozporządzeniu (np. dużych systemowych i zaawansowanych z punktu widzenia ICT instytucji kredytowych, giełd papierów wartościowych, centralnych depozytów papierów wartościowych oraz kontrahentów centralnych) niż dla innych podmiotów finansowych. Jednocześnie testowanie operacyjnej odporności cyfrowej przy użyciu TLPT powinno mieć większe znaczenie w przypadku podmiotów finansowych prowadzących działalność w podstawowych podsektorach usług finansowych i odgrywających rolę systemową (np. płatności, bankowość oraz systemy rozliczeń i rozrachunku), a mniejsze w przypadku innych podsektorów (np. podmiotów zarządzających aktywami oraz agencji ratingowych itp.).

(57) Podmioty finansowe prowadzące działalność transgraniczną i korzystające ze swobody przedsiębiorczości lub swobody świadczenia usług w Unii powinny spełniać jeden zestaw wymogów w zakresie zaawansowanego testowania (np. TLPT) w swoim macierzystym państwie członkowskim, a testowanie to powinno obejmować infrastrukturę ICT we wszystkich jurysdykcjach, w których dana transgraniczna grupa finansowa prowadzi działalność w Unii, co pozwoli takim transgranicznym grupom finansowym ponosić koszty przeprowadzenia testów związanych z ICT tylko w jednej jurysdykcji.

(58) Aby wykorzystać wiedzę fachową zdobytą już przez niektóre właściwe organy, w szczególności w odniesieniu do wdrażania ram TIBER-EU, niniejsze rozporządzenie powinno umożliwiać państwom członkowskim wyznaczenie jednego organu publicznego jako odpowiedzialnego w sektorze finansowym na szczeblu krajowym za wszelkie kwestie dotyczące TLPT lub powinno umożliwiać właściwym organom – w przypadku braku takiego wyznaczenia – przekazanie wykonywania zadań związanych z TLPT innemu krajowemu właściwemu organowi finansowemu.

(59)[25] Z uwagi na to, że niniejsze rozporządzenie nie nakłada na podmioty finansowe wymogu objęcia wszystkich krytycznych lub istotnych funkcji pojedynczym testem penetracyjnym ukierunkowanym przez analizę zagrożeń, podmioty te powinny mieć możliwość określenia, które z tych funkcji i jaką ich liczbę należy objąć zakresem takiego testu.

(60) Testowanie zbiorcze w rozumieniu niniejszego rozporządzenia – z udziałem kilku podmiotów finansowych w TLPT i w odniesieniu do którego zewnętrzny dostawca usług ICT może zawrzeć ustalenia umowne bezpośrednio z testerem zewnętrznym – powinno być dozwolone jedynie w przypadku, gdy można racjonalnie przewidywać, że jakość lub bezpieczeństwo usług świadczonych przez zewnętrznego dostawcę usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia lub poufność danych związanych z takimi usługami będą zagrożone. Testowanie zbiorcze powinno też podlegać zabezpieczeniom (kierowanie przez jeden wyznaczony podmiot finansowy, określenie liczby uczestniczących podmiotów finansowych), aby zapewnić poddanie uczestniczących podmiotów finansowych rygorystycznym testom spełniającym cele TLPT zgodnie z niniejszym rozporządzeniem.

(61) Aby wykorzystać zasoby wewnętrzne dostępne na poziomie przedsiębiorstwa, niniejsze rozporządzenie powinno umożliwiać korzystanie z wewnętrznych testerów do celów przeprowadzania TLPT, pod warunkiem że uzyskano zgodę od organu nadzoru, nie występuje konflikt interesów i że TLTP są przeprowadzane naprzemiennie przez testerów wewnętrznych i zewnętrznych (okresowo – zmiana co trzy testy), przy czym dostawcy analiz zagrożeń wykorzystywanych w ramach TLPT zawsze muszą być podmiotem zewnętrznym względem danego podmiotu finansowego. Pełną odpowiedzialność za prowadzenie TLPT powinien ponosić podmiot finansowy. Potwierdzenia wydawane przez odpowiednie organy powinny służyć wyłącznie do celów wzajemnego uznawania i nie powinny wykluczać działań następczych niezbędnych, by wyeliminować ryzyko związane z ICT, na które dany podmiot finansowy jest narażony, nie powinny też być postrzegane jako potwierdzenie przez organ nadzoru zdolności podmiotu finansowego w zakresie zarządzania ryzykiem związanym z ICT i jego łagodzenia.

(62) Aby zapewnić należyte monitorowanie ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym, konieczne jest ustanowienie zbioru opartych na zasadach przepisów regulujących monitorowanie przez podmioty finansowe ryzyka występującego w kontekście funkcji zlecanych zewnętrznym dostawcom usług ICT, zwłaszcza w odniesieniu do usług ICT wspierających krytyczne lub istotne funkcje, oraz, w bardziej ogólnym zakresie, w kontekście wszelkich zależności od zewnętrznych dostawców usług ICT.

(63) Aby sprostać stopniowi złożoności różnych źródeł ryzyka związanego z ICT, uwzględniając przy tym dużą liczbę i różnorodność dostawców rozwiązań technologicznych umożliwiających sprawne świadczenie usług finansowych, niniejsze rozporządzenie powinno obejmować wielu różnych zewnętrznych dostawców usług ICT, w tym dostawców usług chmurowych, oprogramowania, usług analizy danych i dostawców usług przetwarzania danych. Analogicznie, z uwagi na to, że podmioty finansowe powinny skutecznie i spójnie określać wszystkie rodzaje ryzyka i nimi zarządzać, m.in. w kontekście usług ICT zamawianych w ramach grupy finansowej, należy doprecyzować, że przedsiębiorstwa, które są częścią grupy finansowej i świadczą usługi ICT głównie na rzecz swojej jednostki dominującej lub na rzecz jednostek zależnych lub oddziałów swojej jednostki dominującej, jak również podmioty finansowe świadczące usługi ICT na rzecz innych podmiotów finansowych także powinny być uznawane za zewnętrznych

dostawców usług ICT na mocy niniejszego rozporządzenia. Ponadto w związku ze zmieniającym się rynkiem usług płatniczych, który jest coraz bardziej zależny od złożonych rozwiązań technicznych, oraz w świetle pojawiających się rodzajów usług płatniczych i rozwiązań związanych z płatnościami, uczestnicy ekosystemu usług płatniczych prowadzący działania przetwarzania płatności lub obsługujący infrastrukturę płatniczą również powinni być uznawani za zewnętrznych dostawców usług ICT na mocy niniejszego rozporządzenia, z wyjątkiem banków centralnych prowadzących systemy płatności lub systemy rozrachunku papierów wartościowych oraz organów publicznych świadczących usługi związane z ICT w kontekście pełnienia funkcji państwa.

(64) Podmiot finansowy powinien przez cały czas ponosić pełną odpowiedzialność za wypełnianie swoich obowiązków określonych w niniejszym rozporządzeniu. Podmioty finansowe powinny stosować proporcjonalne podejście do monitorowania zagrożeń występujących na poziomie zewnętrznego dostawcy usług ICT i odpowiednio uwzględnić charakter, skalę, stopień złożoności i znaczenie swoich zależności w zakresie ICT, krytyczność lub znaczenie usług, procesów lub funkcji objętych ustaleniami umownymi, a ostatecznie na podstawie starannej oceny wszelkiego potencjalnego wpływu na ciągłość i jakość usług finansowych na szczeblu indywidualnym i grupowym, w zależności od przypadku.

(65) Takie monitorowanie należy prowadzić zgodnie ze strategicznym podejściem do ryzyka ze strony zewnętrznych dostawców usług ICT sformalizowanym poprzez przyjęcie przez organ zarządzający podmiotu finansowego specjalnej strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT, opartej na ciągłym badaniu wszystkich takich zależności od zewnętrznych dostawców usług ICT. Aby zwiększyć świadomość organów sprawujących nadzór co do zależności od zewnętrznych dostawców usług ICT, a także w celu dalszego wspierania prac prowadzonych w kontekście ram nadzoru ustanowionych w niniejszym rozporządzeniu, wszystkie podmioty finansowe powinny być zobowiązane do prowadzenia rejestru informacji obejmującego wszystkie ustalenia umowne dotyczące korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT. Organy sprawujące nadzór finansowy powinny mieć możliwość żądania dostępu do pełnego rejestru lub określonych jego części, i tym samym uzyskania podstawowych informacji umożliwiających lepsze zrozumienie zależności podmiotów finansowych w obszarze ICT.

(66) Gruntowna analiza poprzedzająca zawarcie umowy powinna mieć miejsce przed formalnym dokonaniem ustaleń umownych i powinna się koncentrować w szczególności na takich elementach, jak krytyczność lub znaczenie usług wspieranych w ramach planowanej umowy w zakresie ICT, niezbędne zgody organów nadzoru lub inne warunki, możliwe powiązane ryzyko koncentracji; należy ją przeprowadzić z zastosowaniem należytej staranności w procesie selekcji i oceny zewnętrznych dostawców usług ICT oraz dokonać oceny potencjalnych konfliktów interesów. W przypadku ustaleń umownych dotyczących krytycznych lub istotnych funkcji podmioty finansowe powinny brać pod uwagę fakt, czy zewnętrzni dostawcy usług ICT stosują najbardziej aktualne i najwyższe standardy bezpieczeństwa informacji. Wypowiedzenie ustaleń umownych mogłoby być spowodowane wystąpieniem co najmniej szeregu okoliczności wskazujących na braki po stronie zewnętrznego dostawcy usług ICT, w szczególności poważnych naruszeń przepisów lub warunków umownych, okoliczności ujawniających potencjalne zmiany w wykonywaniu funkcji przewidzianych w warunkach umownych, dowodów na słabości danego zewnętrznego dostawcy usług ICT w ogólnym zarządzaniu ryzykiem związanym z ICT, lub okoliczności wskazujących na niezdolność odpowiedniego właściwego organu do sprawowania nadzoru nad danym podmiotem finansowym.

(67) Aby zaradzić skutkom systemowym koncentracji ryzyka ze strony zewnętrznych dostawców usług ICT, niniejsze rozporządzenie promuje zrównoważone rozwiązania poprzez elastyczne i stopniowe podejście do takiego ryzyka koncentracji, ponieważ nałożenie jakichkolwiek sztywnych limitów lub ścisłych ograniczeń może utrudniać prowadzenie działalności gospodarczej i ograniczać swobodę zawierania umów. Podmioty finansowe powinny dokładnie oceniać swoje planowane ustalenia umowne w celu określenia prawdopodobieństwa wystąpienia takiego ryzyka, w tym poprzez dogłębną analizę ustaleń dotyczących podwykonawstwa, zwłaszcza w przypadku zawierania ich z zewnętrznymi dostawcami usług ICT mającymi siedzibę w państwie trzecim. Na tym etapie oraz w celu osiągnięcia odpowiedniej równowagi między koniecznością zachowania swobody zawierania umów a koniecznością zagwarantowania stabilności finansowej, nie uważa się za właściwe określenia zasad w odniesieniu do sztywnych limitów i ograniczeń dotyczących ekspozycji wobec zewnętrznych dostawców usług ICT. W kontekście ram nadzoru wiodący organ nadzorczy wyznaczony zgodnie z niniejszym rozporządzeniem powinien – w odniesieniu do kluczowych zewnętrznych dostawców usług ICT zwracać szczególną uwagę na pełne zrozumienie skali współzależności, wykrywać konkretne przypadki, w których wysoki poziom koncentracji kluczowych zewnętrznych dostawców usług ICT w Unii może stanowić zagrożenie dla stabilności i integralności systemu finansowego Unii, i utrzymywać dialog z kluczowymi zewnętrznymi dostawcami usług ICT w przypadku stwierdzenia takiego konkretnego zagrożenia.

(68) Aby regularnie oceniać i monitorować zdolność zewnętrznego dostawcy usług ICT do bezpiecznego świadczenia usług na rzecz podmiotu finansowego bez negatywnego wpływu na operacyjną odporność

cyfrową tego podmiotu, należy ujednolicić kilka najważniejszych elementów umownych z zewnętrznymi dostawcami usług ICT. Takie ujednolicenie powinno obejmować minimum obszarów mających kluczowe znaczenie dla umożliwienia pełnego monitorowania zagrożeń, które mogłyby się pojawić ze strony zewnętrznego dostawcy usług ICT, przez podmiot finansowy w kontekście konieczności zapewnienia odporności cyfrowej tego podmiotu finansowego ze względu na jego głębokie uzależnienie od stabilności, funkcjonalności, dostępności i bezpieczeństwa otrzymywanych usług ICT.

(69) Renegocjując ustalenia umowne w celu dostosowania ich do wymogów niniejszego rozporządzenia, podmioty finansowe i zewnętrzni dostawcy usług ICT powinni zapewnić, by ustalenia te obejmowały najważniejsze postanowienia umowne, jak przewidziano w niniejszym rozporządzeniu.

(70) Określona w niniejszym rozporządzeniu definicja „krytycznej lub istotnej funkcji" obejmuje definicję „funkcji krytycznych" określoną w art. 2 ust. 1 pkt 35 dyrektywy Parlamentu Europejskiego i Rady 2014/59/UE[26]. W związku z tym funkcje uznawane za krytyczne zgodnie z dyrektywą 2014/59/UE są ujęte w definicji funkcji krytycznych w rozumieniu niniejszego rozporządzenia.

(71) Niezależnie od tego czy funkcje wspierane przez usługi ICT mają charakter krytyczny lub istotny, w ustaleniach umownych należy w szczególności zawrzeć specyfikację kompletnych opisów funkcji i usług, miejsc, w których takie funkcje i usługi są świadczone i w których mają być przetwarzane dane, jak również wskazanie opisów gwarantowanych poziomów usług. Innymi elementami o podstawowym znaczeniu dla umożliwienia podmiotowi finansowemu monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT są: postanowienia umowne określające sposób, w jaki zewnętrzny dostawca usług ICT zapewnia dostęp, dostępność, integralność, bezpieczeństwo i ochronę danych osobowych, przepisy ustanawiające odpowiednie gwarancje umożliwiające dostęp do danych, ich odzyskiwanie i zwrot w przypadku niewypłacalności, rozwiązania, zaprzestania działalności gospodarczej zewnętrznego dostawcy usług ICT, a także przepisy nakładające na zewnętrznych dostawców usług ICT wymóg udzielania pomocy w przypadku incydentów związanych ze świadczonymi usługami ICT bez dodatkowych kosztów lub za opłatą określoną *ex ante*; przepisy dotyczące obowiązku pełnej współpracy zewnętrznego dostawcy usług ICT z właściwymi organami i organami ds. restrukturyzacji i uporządkowanej likwidacji podmiotu finansowego; oraz przepisy dotyczące praw do wypowiedzenia umowy i związane z tym minimalne okresy wypowiedzenia ustaleń umownych, zgodnie oczekiwaniami właściwych organów i organów ds. restrukturyzacji i uporządkowanej likwidacji.

(72) W uzupełnieniu takich postanowień umownych i z myślą o zapewnieniu, aby podmioty finansowe zachowały pełną kontrolę nad wszelkimi wydarzeniami ze strony podmiotu zewnętrznego, które mogą mieć negatywny wpływ na ich bezpieczeństwo w obszarze ICT, w umowach na świadczenie usług ICT wspierających krytyczne lub istotne funkcje należy również przewidzieć następujące elementy: specyfikację pełnych opisów gwarantowanych poziomów usług wraz z dokładnymi ilościowymi i jakościowymi celami w zakresie wyników, aby umożliwić bez zbędnej zwłoki odpowiednie działania naprawcze w przypadku nieosiągnięcia uzgodnionych gwarantowanych poziomów usług; odpowiednie okresy wypowiedzenia i obowiązki zewnętrznego dostawcy usług ICT w zakresie zgłaszania incydentów w przypadku wydarzeń, które mogą mieć istotny wpływ na zdolność skutecznego świadczenia przez tego dostawcę odnośnych usług ICT; wymóg wobec zewnętrznego dostawcy usług ICT, by wdrażał i testował plany awaryjne w związku z prowadzoną działalnością oraz posiadał środki, narzędzia i polityki w zakresie bezpieczeństwa ICT, które umożliwiają bezpieczne świadczenie usług, oraz by uczestniczył w przeprowadzanych przez podmiot finansowy TLPT i w pełni współpracował w tym zakresie.

(73) Umowy na świadczenie usług ICT wspierających krytyczne lub istotne funkcje powinny również zawierać przepisy umożliwiające korzystanie z praw dostępu kontroli i audytu przez podmiot finansowy lub wyznaczoną osobę trzecią oraz prawa do sporządzania kopii jako kluczowych instrumentów bieżącego monitorowania przez podmioty finansowe wyników zewnętrznego dostawcy usług ICT w połączeniu z pełną współpracą tego ostatniego podczas kontroli. Analogicznie właściwemu organowi podmiotu finansowego powinno przysługiwać, na podstawie otrzymanych zawiadomień, podobne prawo do kontroli i audytu zewnętrznego dostawcy usług ICT, z zastrzeżeniem ochrony informacji poufnych.

(74) W takich ustaleniach umownych należy również przewidzieć specjalne strategie wyjścia umożliwiające w szczególności obowiązkowe okresy przejściowe, w których zewnętrzni dostawcy usług ICT powinni nadal świadczyć odpowiednie usługi, aby zmniejszyć ryzyko zakłóceń na poziomie podmiotu finansowego lub umożliwić temu ostatniemu skuteczne przejście do korzystania z innych zewnętrznych dostawców usług ICT lub, alternatywnie, skorzystanie z rozwiązań dostępnych w ramach struktury wewnętrznej, stosownie do stopnia złożoności świadczonej usługi ICT. Co więcej, podmioty finansowe objęte zakresem stosowania dyrektywy 2014/59/UE powinny zapewnić, by odpowiednie umowy na usługi ICT były solidne i w pełni egzekwowalne w przypadku restrukturyzacji i uporządkowanej likwidacji tych podmiotów finansowych. W związku z tym zgodnie z oczekiwaniami organów ds. restrukturyzacji i uporządkowanej likwidacji te podmioty finansowe powinny zapewnić, by odpowiednie umowy na usługi ICT wykazywały się odpornością na wypadek restrukturyzacji i uporządkowanej likwidacji. Dopóki te podmioty finansowe wypełniają swoje zobowiązania płatnicze, powinny zapewnić, by odpowiednie umowy dotyczące

usług ITC – oprócz innych wymogów – zawierały też klauzule o niemożności ich wypowiedzenia, zawieszenia i modyfikacji z powodu restrukturyzacji lub uporządkowanej likwidacji.

(75) Ponadto dobrowolne stosowanie standardowych klauzul umownych opracowanych przez organy publiczne lub instytucje unijne, w szczególności stosowanie klauzul umownych opracowanych przez Komisję na potrzeby usług chmurowych może zapewnić dodatkowy komfort podmiotom finansowym i zewnętrznym dostawcom usług ICT poprzez zwiększenie poziomu pewności prawa w zakresie korzystania z usług chmurowych przez sektor finansowy, z zachowaniem pełnej zgodności z wymogami i oczekiwaniami określonymi w unijnych przepisach dotyczących usług finansowych. Prace służące opracowaniu standardowych klauzul umownych opierają się na środkach przewidzianych już w Planie działania w zakresie technologii finansowej z 2018 r., w którym zapowiedziano, że Komisja zamierza wspierać i ułatwiać opracowywanie standardowych klauzul umownych dotyczących korzystania z usług chmurowych na zasadzie outsourcingu przez podmioty finansowe, czerpiąc z międzysektorowych wysiłków zainteresowanych podmiotów świadczących usługi chmurowe, które Komisja ułatwiła dzięki zaangażowaniu sektora finansowego.

(76) Aby wesprzeć ujednolicenie i poprawę efektywności podejść w zakresie nadzoru w odniesieniu do ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym oraz wzmocnić operacyjną odporność cyfrową podmiotów finansowych, które w przypadku usług ICT wspierających świadczenie usług finansowych polegają na kluczowych zewnętrznych dostawcach usług ICT, a tym samym przyczynić się do utrzymania stabilności systemu finansowego Unii oraz integralności wewnętrznego rynku usług finansowych, kluczowi zewnętrzni dostawcy usług ICT powinni być objęci unijnymi ramami nadzoru. Choć ustanowienie ram nadzoru jest uzasadnione z uwagi na wartość dodaną działań na szczeblu Unii oraz nieodłączną rolę i specyfikę korzystania z usług ICT w świadczeniu usług finansowych, należy jednocześnie przypomnieć, że rozwiązanie to wydaje się odpowiednie jedynie w kontekście niniejszego rozporządzenia, które dotyczy konkretnie operacyjnej odporności cyfrowej w sektorze finansowym. Niemniej jednak takich ram nadzoru nie należy uznawać za nowy model unijnego nadzoru w innych obszarach usług i działań finansowych.

(77) Ramy nadzoru powinny mieć zastosowanie wyłącznie do kluczowych zewnętrznych dostawców usług ICT. Należy zatem wprowadzić mechanizm wyznaczania, aby uwzględnić wymiar i charakter zależności sektora finansowego od takich zewnętrznych dostawców usług ICT. Mechanizm ten powinien obejmować zestaw kryteriów ilościowych i jakościowych, które określałyby parametry krytyczności jako podstawę do objęcia ramami nadzoru. Aby zapewnić dokładność tej oceny i niezależnie od struktury organizacyjnej zewnętrznego dostawcy usług ICT, takie kryteria powinny – w przypadku zewnętrznego dostawcy usług ICT będącego częścią szerszej grupy – uwzględniać całą strukturę grupy tego zewnętrznego dostawcy usług ICT. Z jednej strony kluczowi zewnętrzni dostawcy usług ICT, którzy nie zostali automatycznie wyznaczeni na podstawie wspomnianych wyżej kryteriów, powinni mieć możliwość dobrowolnego przystąpienia do ram nadzoru, natomiast z drugiej strony ci zewnętrzni dostawcy usług ICT, których objęto już ramami mechanizmu nadzoru wspierającymi realizację zadań Europejskiego Systemu Banków Centralnych, o których mowa w art. 127 ust. 2 TFUE, powinni zostać zwolnieni.

(78) Analogicznie podmioty finansowe, które świadczą usługi ICT na rzecz innych podmiotów finansowych, powinny być zwolnione z ram nadzoru – choć należą do kategorii zewnętrznych dostawców usług ICT na mocy niniejszego rozporządzenia – ponieważ podlegają już mechanizmom nadzorczym ustanowionym przez odpowiednie unijne przepisy dotyczące usług finansowych. W stosownych przypadkach w kontekście działań nadzorczych właściwe organy powinny też uwzględniać ryzyko związane z ICT dla podmiotów finansowych, które jest stwarzane przez podmioty finansowe świadczące usługi ICT. Podobnie ze względu na mechanizmy monitorowania ryzyka istniejące na poziomie grupy to samo zwolnienie powinno zostać wprowadzone względem zewnętrznych dostawców usług ICT świadczących usługi głównie na rzecz podmiotów w ramach swojej grupy. Zewnętrzni dostawcy usług ICT świadczący usługi wyłącznie w jednym państwie członkowskim na rzecz podmiotów finansowych działających tylko w tym państwie członkowskim również powinni zostać zwolnieni z mechanizmu wyznaczania ze względu na ich ograniczoną działalność i brak skutków transgranicznych.

(79) Transformacja cyfrowa zachodząca w usługach finansowych doprowadziła do bezprecedensowego poziomu wykorzystania usług ICT i uzależnienia się od nich. Ponieważ świadczenie usług finansowych bez korzystania z usług chmurowych, rozwiązań w zakresie oprogramowania i usług związanych z danymi nie jest już możliwe, unijny ekosystem finansowy stał się wewnętrznie współzależny od pewnych usług ICT świadczonych przez dostawców usług ICT. Niektórzy z tych dostawców, innowacyjni w opracowywaniu i stosowaniu technologii opartych na ICT, odgrywają znaczącą rolę w świadczeniu usług finansowych lub zostali włączeni do łańcucha wartości usług finansowych. Tym samym mają teraz kluczowe znaczenie dla stabilności i integralności unijnego systemu finansowego. Ta powszechna zależność od usług świadczonych przez kluczowych zewnętrznych dostawców usług ICT, w połączeniu ze współzależnością systemów informacyjnych różnych podmiotów gospodarczych, tworzy bezpośrednie i potencjalnie poważne ryzyko dla unijnego systemu usług finansowych i dla ciągłości świadczenia usług finansowych, gdyby

kluczowych zewnętrznych dostawców usług ICT dotknęły zakłócenia operacyjne lub poważne cyberincydenty. Cyberincydenty charakteryzują się wyjątkową zdolnością do zwielokrotniania i rozprzestrzeniania się w całym systemie finansowym w znacznie szybszym tempie niż inne rodzaje ryzyka monitorowane w sektorze finansowym oraz mogą mieć zasięg międzysektorowy i wykraczać poza granice geograficzne. Mogą przekształcić się w kryzys systemowy, w którym zaufanie do systemu finansowego zostanie podkopane w wyniku zakłócenia funkcji wspierających gospodarkę realną lub w związku ze znacznymi stratami finansowymi, i osiągnąć poziom, na którym system finansowy nie będzie w stanie przetrwać lub będzie wymagać uruchomienia poważnych środków amortyzacji wstrząsów. Aby zapobiec urzeczywistnieniu tych scenariuszy, a przez to zagrożeniu stabilności finansowej i integralności Unii, należy zapewnić spójność praktyk nadzorczych dotyczących ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansów, w szczególności poprzez nowe przepisy umożliwiające unijny nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT.

(80) Ramy nadzoru w dużej mierze zależą od stopnia współpracy między wiodącym organem nadzorczym i kluczowym zewnętrznym dostawcą usług ICT, który dostarcza podmiotom finansowym usługi mające wpływ na świadczenie usług finansowych. Skuteczny nadzór opiera się m.in. na zdolności wiodącego organu nadzorczego do skutecznego przeprowadzania misji monitorujących i kontroli w celu oceny zasad, mechanizmów kontroli i procesów stosowanych przez kluczowych zewnętrznych dostawców usług ICT, a także potencjalnego skumulowanego wpływu ich działań na stabilność finansową i integralność systemu finansowego. Jednocześnie podstawowe znaczenie ma to, by kluczowi zewnętrzni dostawcy usług ICT stosowali się do zaleceń wiodącego organu nadzorczego i reagowali na jego uwagi. Ponieważ brak współpracy ze strony kluczowych zewnętrznych dostawców usług ICT dostarczających usługi mające wpływ na świadczenie usług finansowych, np. odmowa udzielenia dostępu do ich pomieszczeń lub przedłożenia informacji, ostatecznie skutkowałby sytuacją, w której wiodący organ nadzorczy zostałby pozbawiony podstawowych narzędzi umożliwiających ocenę ryzyka ze strony zewnętrznych dostawców usług ICT, i mógłby mieć negatywny wpływ na stabilność finansową i integralność systemu finansowego, należy też przewidzieć adekwatny system kar.

(81) W tym kontekście trudności związane z egzekwowaniem tych kar pieniężnych od kluczowych zewnętrznych dostawców usług ICT mających siedzibę w państwach trzecich nie mogą uniemożliwiać nałożenia przez wiodący organ nadzorczy kar pieniężnych w celu zmuszenia kluczowych zewnętrznych dostawców usług ICT do wypełnienia obowiązków w zakresie przejrzystości i dostępu określonych w niniejszym rozporządzeniu. Aby zapewnić możliwość wyegzekwowania takich kar oraz umożliwić szybkie uruchomienie procedur gwarantujących prawa kluczowych zewnętrznych dostawców usług ICT do obrony w kontekście mechanizmu wyznaczania i wydawania zaleceń, kluczowi zewnętrzni dostawcy usług ICT świadczący usługi podmiotom finansowym mające wpływ na świadczenie usług finansowych powinni być zobowiązani do utrzymywania odpowiedniej obecności biznesowej w Unii. Ze względu na charakter nadzoru i brak porównywalnych ustaleń w innych jurysdykcjach nie istnieją odpowiednie alternatywne mechanizmy zapewniające osiągnięcie tego celu poprzez skuteczną współpracę z organami nadzoru finansowego w państwach trzecich w odniesieniu do monitorowania wpływu cyfrowego ryzyka operacyjnego ze strony systemowych zewnętrznych dostawców usług ICT kwalifikujących się jako kluczowi zewnętrzni dostawcy usług ICT mający siedzibę w państwach trzecich. W związku z tym, aby móc dalej świadczyć usługi ICT na rzecz podmiotów finansowych w Unii, zewnętrzni dostawcy usług ICT mający siedzibę w państwach trzecich, wyznaczeni jako kluczowi zgodnie z niniejszym rozporządzeniem powinni w ciągu 12 miesięcy od takiego wyznaczenia podjąć wszelkie działania niezbędne do uzyskania zdolności prawnej wewnątrz Unii w drodze ustanowienia jednostki zależnej, zgodnie z definicją zawartą w unijnym dorobku prawnym, a mianowicie w dyrektywie Parlamentu Europejskiego i Rady 2013/34/UE[27].

(82) Wymóg utworzenia jednostki zależnej w Unii nie powinien uniemożliwiać kluczowemu zewnętrznemu dostawcy usług ICT świadczenia usług ICT i powiązanego wsparcia technicznego z obiektów i infrastruktury znajdującej się poza Unią. Niniejsze rozporządzenie nie nakłada obowiązku lokalizacji danych, ponieważ nie nakłada wymogu, by czynności przechowywania i przetwarzania danych były przeprowadzane w Unii.

(83) Kluczowi zewnętrzni dostawcy usług ICT powinni mieć możliwość świadczenia usług ICT z dowolnego miejsca na świecie, niekoniecznie lub nie tylko z obiektów znajdujących się w Unii. Działania nadzorcze powinny być prowadzone w pierwszej kolejności w obiektach znajdujących się w Unii i poprzez kontakty z podmiotami znajdującymi się w Unii, w tym w jednostkach zależnych ustanowionych przez kluczowych zewnętrznych dostawców usług ICT zgodnie z niniejszym rozporządzeniem. Niemniej jednak takie działania wewnątrz Unii mogą być niewystarczające, by wiodący organ nadzorczy mógł w pełni i skutecznie wykonywać swoje obowiązki wynikające z niniejszego rozporządzenia. Wiodący organ nadzorczy powinien zatem mieć również możliwość wykonywania swoich odpowiednich uprawnień nadzorczych w państwach trzecich. Wykonywanie tych uprawnień w państwach trzecich powinno umożliwić wiodącemu organowi nadzorczemu zbadanie obiektów, z których kluczowy zewnętrzny dostawca usług ICT faktycznie świadczy usługi ICT lub usługi wsparcia technicznego lub nimi zarządza, i powinno pozwolić

wiodącemu organowi nadzorczemu na kompleksowy ogląd i zrozumienie – pod kątem operacyjnym – sposobu, w jaki dany dostawca usług ICT zarządza ryzykiem związanym z ICT. Możliwość wykonywania przez wiodący organ nadzorczy – jako agencję unijną – uprawnień poza terytorium Unii powinna być należycie ustrukturyzowana i obwarowana stosownymi warunkami, w szczególności chodzi tu o zgodę ze strony danego kluczowego zewnętrznego dostawcy usług ICT. Podobnie odpowiednie organy państwa trzeciego powinny być poinformowane i nie wyrażać sprzeciwu w odniesieniu do działań wiodącego organu nadzorczego wykonywanych na ich terytorium. Aby jednak zapewnić skuteczne wdrożenie i bez uszczerbku dla odpowiednich kompetencji instytucji Unii i państw członkowskich, takie uprawnienia muszą też być w pełni zakorzenione w porozumieniach o współpracy administracyjnej zawartych z odpowiednimi organami danego państwa trzeciego. Niniejsze rozporządzenie powinno zatem umożliwić EUN zawieranie porozumień o współpracy administracyjnej z odpowiednimi organami państw trzecich, które w żaden sposób nie powinny tworzyć zobowiązań prawnych w odniesieniu do Unii i jej państw członkowskich.

(84) Aby ułatwić komunikację z wiodącym organem nadzorczym i zapewnić odpowiednią reprezentację, kluczowi zewnętrzni dostawcy usług ICT będący częścią grupy powinni wyznaczyć jedną osobę prawną jako swój punkt koordynacyjny.

(85) Ramy nadzoru powinny pozostawać bez uszczerbku dla kompetencji państw członkowskich, jeżeli chodzi o prowadzenie własnych misji w zakresie sprawowania nadzoru lub monitorowania w odniesieniu do zewnętrznych dostawców usług ICT, których nie wyznaczono jako kluczowych na mocy niniejszego rozporządzenia, ale którzy są uznawani za istotnych na szczeblu krajowym.

(86) Aby wykorzystać wielowarstwową strukturę instytucjonalną w obszarze usług finansowych, Wspólny Komitet EUN powinien nadal zapewniać ogólną międzysektorową koordynację w odniesieniu do wszystkich kwestii dotyczących ryzyka związanego z ICT, zgodnie ze swoimi zadaniami w zakresie cyberbezpieczeństwa. Powinien być wspierany przez nowy podkomitet (zwany dalej „forum nadzoru"), który będzie prowadził prace przygotowawcze zarówno w zakresie indywidualnych decyzji skierowanych do kluczowych zewnętrznych dostawców usług ICT, jak i wydawania zbiorowych zaleceń, w szczególności w odniesieniu do analizy porównawczej programów dotyczących sprawowania nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, a także określania najlepszych praktyk w zakresie rozwiązywania problemów związanych z ryzykiem koncentracji w obszarze ICT.

(87) Aby zapewnić odpowiedni i skuteczny nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT na szczeblu Unii, w niniejszym rozporządzeniu przewidziano, że dowolny z trzech EUN może zostać wyznaczony jako wiodący organ nadzorczy. Przypisanie poszczególnych kluczowych zewnętrznych dostawców usług ICT jednemu z trzech EUN powinno być oparte na ocenie tego, w którym sektorze finansowym dane podmioty finansowe przeważają i któremu z EUN sektor ten podlega. Podejście to powinno prowadzić do zrównoważonego podziału zadań i obowiązków między trzema EUN w kontekście sprawowania funkcji nadzorczych oraz powinno możliwie najlepiej wykorzystywać zasoby kadrowe i specjalistyczną wiedzę techniczną dostępne w każdym z trzech EUN.

(88) Wiodącym organom nadzorczym należy powierzyć niezbędne uprawnienia do prowadzenia dochodzeń, przeprowadzania kontroli na miejscu i kontroli zdalnych w obiektach i lokalizacjach kluczowych zewnętrznych dostawców usług ICT oraz uzyskiwania pełnych i aktualnych informacji. Uprawnienia te powinny umożliwić wiodącym organom nadzorczym uzyskanie rzeczywistego wglądu w rodzaj, wymiar i wpływ ryzyka ze strony zewnętrznych dostawców usług ICT dla podmiotów finansowych i ostatecznie dla systemu finansowego Unii. Powierzenie EUN roli wiodących organów nadzorczych jest jednym z warunków wstępnych do zrozumienia i wyeliminowania systemowego wymiaru ryzyka związanego z ICT w sektorze finansów. Wpływ kluczowych zewnętrznych dostawców usług ICT na unijny sektor finansowy oraz potencjalne problemy wynikające z powiązanym ryzykiem koncentracji w obszarze ICT wymagają przyjęcia wspólnego podejścia na szczeblu Unii. Jednoczesne przeprowadzanie licznych audytów i korzystanie z praw dostępu, wykonywane osobno przez szereg właściwych organów, przy niewielkiej lub braku jakiejkolwiek koordynacji pomiędzy nimi, uniemożliwiłoby organom nadzoru finansowego uzyskanie pełnego i kompleksowego przeglądu ryzyka ze strony zewnętrznych dostawców usług ICT w Unii, powodując też przy tym redundancję, obciążenie i złożoność na poziomie kluczowych zewnętrznych dostawców usług ICT, gdyby zostali oni objęci dużą liczbą wniosków o monitorowanie i kontrolę.

(89) Ze względu na to, że dla konkretnego dostawcy fakt bycia wyznaczonym jako kluczowy zewnętrzny dostawca usług ICT niesie za sobą poważne konsekwencje, niniejsze rozporządzenie powinno zapewniać przestrzeganie praw kluczowych zewnętrznych dostawców usług ICT w całym okresie wdrażania ram nadzoru. Zanim dostawcy zostaną wyznaczeni jako kluczowi, powinni oni przykładowo mieć prawo przedłożyć wiodącemu organowi nadzorczemu uzasadnione oświadczenie zawierające wszelkie istotne informacje na potrzeby oceny związanej z ich wyznaczeniem. W związku z tym, że wiodący organ nadzorczy powinien być uprawniony do przedstawiania zaleceń w zakresie ryzyka związanego z ICT oraz odpowiednich środków zaradczych, w tym prawa do sprzeciwiania się określonym ustaleniom umownym, które ostatecznie wpływają na stabilność podmiotu finansowego lub systemu

finansowego, przed finalizacją tych zaleceń kluczowi dostawcy usług ICT również powinni mieć możliwość przedstawienia wyjaśnień dotyczących spodziewanego wpływu rozwiązań proponowanych w tych zaleceniach na klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia i zaproponowania rozwiązań służących łagodzeniu ryzyka. Kluczowi dostawcy usług ICT, którzy nie zgadzają się z zaleceniami, również przedstawić uzasadnione wyjaśnienie powodów, dla których nie zamierzają przyjąć danego zalecenia. W przypadku gdy nieprzed- stawienia takiego uzasadnienia lub uznania przedstawionego uzasadnienia za niewystarczające, wiodący organ nadzorczy powinien wydać publiczne ogłoszenie opisujące zwięźle kwestię niezgodności.

(90) Właściwe organy powinny mieć za zadanie sprawdzenie tego, czy zalecenia wydane przez wiodący organ nadzorczy w ramach jego funkcji dotyczących nadzoru ostrożnościowego nad podmiotami finansowymi są przestrzegane pod kątem merytorycznym. Właściwe organy powinny mieć możliwość wymagania od podmiotów finansowych, by te podjęły dodatkowe środki w celu zwalczania ryzyka stwierdzonego w zaleceniach wiodącego organu nadzorczego, oraz we właściwym czasie powinny wydać stosowne zawiadomienia. W przypadku gdy wiodący organ nadzorczy kieruje zalecenia do kluczowych zewnętrznych dostawców usług ICT, którzy podlegają nadzorowi na mocy dyrektywy (UE) 2022/2555, właściwe organy powinny mieć możliwość skonsultowania się, na zasadzie dobrowolności i przed przyjęciem dodatkowych środków, z właściwymi organami na mocy tej dyrektywy w celu przyjęcia skoordynowanego podejścia do danych kluczowych zewnętrznych dostawców usług ICT.

(91) Sprawowanie nadzoru powinno opierać się na trzech zasadach operacyjnych mających na celu zapewnienie:

a) ścisłej koordynacji pomiędzy EUN działającymi jako wiodący organ nadzorczy, poprzez wspólną sieć nadzoru,

b) spójności z ramami ustanowionymi dyrektywą (UE) 2022/2555 (poprzez dobrowolne konsultacje z organami na mocy tej dyrektywy w celu uniknięcia powielania środków ukierunkowanych na kluczowych zewnętrznych dostawców usług ICT), oraz

c) staranności w celu zminimalizowania potencjalnego ryzyka zakłócenia usług świadczonych przez kluczowych dostawców usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia.

(92) Ramy nadzoru nie powinny zastępować, ani w żaden sposób lub w żadnej części stanowić zamiennika obowiązku zarządzania przez podmioty finansowe ryzykiem wynikającym z korzystania z zewnętrznych dostawców usług ICT, w tym obowiązku bieżącego monitorowania ustaleń umownych uzgodnionych z kluczowymi zewnętrznymi dostawcami usług ICT. Analogicznie ramy nadzoru nie powinny mieć wpływu na pełną odpowiedzialność podmiotów finansowych za przestrzeganie i wywiązywanie się ze wszystkich zobowiązań prawnych ustanowionych w niniejszym rozporządzeniu i w odpowiednich przepisach dotyczących usług finansowych.

(93) Aby uniknąć powielania i nakładania się działań, właściwe organy powinny powstrzymać się od samodzielnego podejmowania jakichkolwiek środków mających na celu monitorowanie ryzyka ze strony kluczowych zewnętrznych dostawców usług ICT i w tym względzie powinny opierać się na ocenie odpowiednich wiodących organów nadzorczych. W każdym przypadku wszelkie środki należy uprzednio skoordynować i uzgodnić z danymi wiodącymi organami nadzorczymi *w kontekście* wykonywania zadań objętych ramami nadzoru.

(94) Aby wspierać ujednolicenie na szczeblu międzynarodowym stosowania najlepszych praktyk, które mają być stosowane przy dokonywaniu przeglądu i monitorowaniu cyfrowego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT, należy zachęcać EUN do zawierania porozumień o współpracy z odpowiednimi organami nadzoru i organami regulacyjnymi państw trzecich.

(95) Aby wykorzystać szczególne kompetencje, umiejętności techniczne i wiedzę pracowników specjalizujących się w ryzyku operacyjnym i ryzyku związanym z ICT w ramach właściwych organów, trzy EUN oraz – na zasadzie dobrowolności – właściwe organy na mocy dyrektywy (UE) 2022/2555 i wiodący organ nadzorczy powinny korzystać z umiejętności i wiedzy poszczególnych krajów w zakresie nadzoru i ustanowić specjalne zespoły ds. kontroli dla każdego z poszczególnych kluczowych zewnętrznych dostawców usług ICT, łącząc multidyscyplinarne zespoły w celu wspierania zarówno przygotowania, jak i realizacji działań nadzorczych, w tym dochodzeń ogólnych i kontroli u kluczowych zewnętrznych dostawców usług ICT, a także z myślą o wszelkich niezbędnych działaniach następczych.

(96) Choć koszty wynikające z zadań nadzorczych byłyby w pełni finansowane z opłat pobieranych od kluczowych zewnętrznych dostawców usług ICT, EUN prawdopodobnie poniosą, przed rozpoczęciem obowiązywania ram nadzoru, koszty wdrożenia specjalnych systemów ICT wspierających przyszły nadzór, ponieważ specjalne systemy ICT musiałyby zostać wcześniej opracowane i wdrożone. W związku z tym niniejsze rozporządzenie przewiduje model finansowania hybrydowego, w ramach którego ramy nadzoru jako takie byłyby w całości finansowane z opłat, a opracowywanie systemów ICT w EUN byłoby finansowane ze środków unijnych i wkładów wnoszonych przez właściwe organy krajowe.

(97) Właściwe organy powinny posiadać wszelkie wymagane uprawnienia w zakresie sprawowania nadzoru, prowadzenia dochodzeń i nakładania kar, aby zapewnić prawidłowe wykonywanie obowiązków spoczywających na nich na mocy niniejszego rozporządzenia. Powinny one co do zasady publikować zawiadomienia o nakładanych karach administracyjnych. Ponieważ podmioty finansowe i zewnętrzni dostawcy usług ICT mogą mieć siedziby w różnych państwach członkowskich oraz podlegać nadzorowi różnych właściwych organów, należy ułatwić stosowanie niniejszego rozporządzenia, z jednej strony, poprzez ścisłą współpracę pomiędzy odpowiednimi właściwymi organami, w tym EBC w zakresie zadań szczególnych powierzonych mu na mocy rozporządzenia Rady (UE) nr 1024/2013, oraz, z drugiej strony, poprzez konsultacje z EUN w drodze wzajemnej wymiany informacji i dzięki zapewnieniu pomocy w kontekście odpowiedniej działalności nadzorczej.

(98) W celu dalszego ilościowego i jakościowego określenia kryteriów wyznaczania kluczowych zewnętrznych dostawców usług ICT oraz ujednolicenia opłat z tytułu nadzoru, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE, aby uzupełnić niniejsze rozporządzenie w odniesieniu do bardziej szczegółowego określenia skutków systemowych, jakie awaria lub przestój operacyjny zewnętrznego dostawcy usług ICT mogłyby mieć dla podmiotów finansowych, na rzecz których świadczy usługi, liczby globalnych instytucji o znaczeniu systemowym lub innych instytucji o znaczeniu systemowym, które polegają na danym zewnętrznym dostawcy usług ICT, liczby zewnętrznych dostawców usług ICT działających na danym rynku, kosztów migracji danych i nakładów pracy w zakresie ICT do innych zewnętrznych dostawców usług ICT, a także wysokości opłat z tytułu nadzoru oraz sposobu ich uiszczania. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby były one prowadzone zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[28]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te powinny otrzymywać wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji powinni systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(99) Regulacyjne standardy techniczne powinny zapewniać spójną harmonizację wymogów ustanowionych w niniejszym rozporządzeniu. Opracowanie projektów regulacyjnych standardów technicznych, które nie wymagają podejmowania decyzji politycznych, w celu przedłożenia Komisji, należy powierzyć EUN działającym jako organy dysponujące wysokim poziomem wiedzy specjalistycznej. Należy opracować regulacyjne standardy techniczne w dziedzinie zarządzania ryzykiem związanym z ICT, zgłaszania poważnych incydentów związanych z ICT, testowania i w odniesieniu do najważniejszych wymogów dotyczących należytego monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT. Komisja i EUN powinny zapewnić, aby wspomniane standardy i wymogi mogły być stosowane przez wszystkie podmioty finansowe w sposób proporcjonalny do ich wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności ich usług, działań i operacji. Komisja powinna być uprawniona do przyjmowania tych regulacyjnych standardów technicznych w drodze aktów delegowanych zgodnie z art. 290 TFUE oraz zgodnie z art. 10–14 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

(100) W celu ułatwienia porównywalności sprawozdań dotyczących poważnych incydentów związanych z ICT i poważnych incydentów operacyjnych lub poważnych incydentów w zakresie bezpieczeństwa związanych z płatnościami oraz w celu zapewnienia przejrzystości w zakresie ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT, EUN powinny opracować projekty wykonawczych standardów technicznych ustanawiających standardowe wzory, formularze i procedury dla podmiotów finansowych na potrzeby zgłaszania poważnych incydentów związanych z ICT i poważnych incydentów operacyjnych lub poważnych incydentów w zakresie bezpieczeństwa związanych z płatnościami, jak również standardowych wzorów na potrzeby rejestrowania informacji. Przy opracowywaniu tych standardów EUN powinny brać pod uwagę wielkość i ogólny profil ryzyka danego podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji. Komisja powinna być uprawniona do przyjmowania tych wykonawczych standardów technicznych w drodze aktów wykonawczych zgodnie z art. 291 TFUE oraz zgodnie z art. 15 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 oraz (UE) nr 1095/2010.

(101) Ponieważ dalsze wymogi określono już w aktach delegowanych i wykonawczych opartych na regulacyjnych i wykonawczych standardach technicznych w rozporządzeniach Parlamentu Europejskiego i Rady (WE) nr 1060/2009[29], (UE) nr 648/2012[30], (UE) nr 600/2014[31] i (UE) nr 909/2014[32], należy upoważnić EUN, indywidualnie albo wspólnie za pośrednictwem Wspólnego Komitetu, do przedłożenia Komisji regulacyjnych i wykonawczych standardów technicznych w celu przyjęcia aktów delegowanych i wykonawczych przenoszących i aktualizujących istniejące przepisy dotyczące zarządzania ryzykiem związanym z ICT.

(102) Ponieważ niniejsze rozporządzenie, wraz z dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2556[33], pociąga za sobą konsolidację przepisów dotyczących zarządzania ryzykiem związanym z ICT obejmujących wiele rozporządzeń i dyrektyw z unijnego dorobku prawnego w zakresie usług finansowych, w tym rozporządzeń (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) nr 909/2014 oraz

rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1011[34], w celu zapewnienia pełnej spójności należy zmienić te rozporządzenia, aby wyjaśnić, że mające zastosowanie przepisy dotyczące ryzyka związanego z ICT ustanowiono w niniejszym rozporządzeniu.

(103) W związku z tym zakres odpowiednich artykułów związanych z ryzykiem operacyjnym, na mocy których powierzono uprawnienia ustanowione w rozporządzeniach (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 (UE) nr 909/2014 oraz (UE) 2016/1011 do przyjmowania aktów delegowanych i wykonawczych, należy zawęzić z myślą o przeniesieniu do niniejszego rozporządzenia wszystkich przepisów obejmujących aspekty operacyjnej odporności cyfrowej stanowiących obecnie część tych rozporządzeń.

(104) Potencjalne systemowe ryzyko w cyberprzestrzeni związane z wykorzystywaniem infrastruktury ICT umożliwiającej funkcjonowanie systemów płatniczych i prowadzenie działań w zakresie przetwarzania płatności powinno być należycie uwzględnione na szczeblu Unii poprzez zharmonizowane przepisy dotyczące odporności cyfrowej. W tym celu Komisja powinna szybko ocenić potrzebę dokonania przeglądu zakresu stosowania niniejszego rozporządzenia, dostosowując taki przegląd do wyniku kompleksowego przeglądu przewidzianego na mocy dyrektywy (UE) 2015/2366. Liczne ataki na wielką skalę w ostatnim dziesięcioleciu pokazują, że systemy płatności są narażone na cyberzagrożenia. Systemy płatnicze i działania w zakresie przetwarzania płatności, które zostały umieszczone w centrum łańcucha usług płatniczych i wykazują silne powiązania z ogólnym systemem finansowym, mają obecnie podstawowe znaczenie dla funkcjonowania unijnych rynków finansowych. Cyberataki na takie systemy mogą powodować poważne zakłócenia w działalności operacyjnej i mieć bezpośredni wpływ na najważniejsze funkcje gospodarcze, takie jak uproszczenie płatności, oraz pośrednie skutki dla powiązanych procesów gospodarczych. Do czasu wprowadzenia na szczeblu Unii zharmonizowanego systemu oraz nadzoru nad operatorami systemów płatniczych i podmiotami prowadzącymi czynności przetwarzania, państwa członkowskie mogą, przy stosowaniu przepisów wobec operatorów systemów płatniczych i podmiotów prowadzących czynności przetwarzania podlegających nadzorowi w ramach ich jurysdykcji – z myślą o stosowaniu podobnych praktyk rynkowych – inspirować się wymogami w zakresie operacyjnej odporności cyfrowej ustanowionymi w niniejszym rozporządzeniu.

(105) Ponieważ cel niniejszego rozporządzenia, a mianowicie osiągnięcie wysokiego poziomu operacyjnej odporności cyfrowej w odniesieniu do regulowanych podmiotów finansowych, nie może zostać w wystarczającym stopniu osiągnięty przez państwa członkowskie, gdyż wymaga harmonizacji wielu różnych przepisów w prawie Unii i prawie krajowym, natomiast ze względu na skalę i skutki osiągnięcie tego celu może być bardziej skuteczne na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(106) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[35] skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia 10 maja 2021 r.[36],

[1] Dz.Urz. UE C 343 z 26.08.2021 r., s. 1.

[2] Dz.Urz. UE C 155 z 30.04.2021 r., s. 38.

[3] Stanowisko Parlamentu Europejskiego z 10.11.2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z 28.11.2022 r.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z 24.11.2010 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.Urz. UE L 331, s. 12).

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z 24.11.2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.Urz. UE L 331, s. 48).

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z 24.11.2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE (Dz Urz. UE L 331, s. 84).

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1).

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (zob. s. 80 niniejszego Dziennika Urzędowego).

[9] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14.12.2022 r. w sprawie odporności podmiotów krytycznych i uchylenia dyrektywy Rady 2008/114/WE (zob. s. 164 niniejszego Dziennika Urzędowego).

[10] Motyw 21 zmieniony przez pkt 1 sprostowania z 12.03.2024 r. (Dz.Urz. UE L 2024/90177) zmieniającego nin. rozporządzenie z dniem 16.01.2023 r.