C/2026/2621

26.5.2026

OPINIA EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 10 marca 2026 r.

w sprawie wniosku dotyczącego rozporządzenia w sprawie uproszczenia cyfrowych ram prawnych (aktu zbiorczego prawa cyfrowego)

(CON/2026/9)

(C/2026/2621)

Wprowadzenie i podstawa prawna

W dniu 9 grudnia 2025 r. Europejski Bank Centralny (EBC) otrzymał wniosek Parlamentu Europejskiego o wydanie opinii w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (aktu zbiorczego prawa cyfrowego) ([1]) (zwanego dalej „proponowanym rozporządzeniem").

Właściwość EBC do wydania opinii wynika z art. 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, jako że proponowane rozporządzenie zawiera przepisy wchodzące w zakres kompetencji EBC, w tym w szczególności dotyczących wdrażania polityki pieniężnej zgodnie z art. 127 ust. 2 tiret pierwsze oraz art. 282 ust. 1 Traktatu, sprawnego funkcjonowania systemów płatniczych zgodnie z art. 127 ust. 2 tiret czwarte i art. 282 ust. 1 Traktatu, nadzoru ostrożnościowego nad instytucjami kredytowymi zgodnie z art. 127 ust. 6 Traktatu oraz zadań EBC związanych ze zbieraniem informacji statystycznych zgodnie z art. 5 Statutu Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (zwanego dalej „Statutem ESBC"). Rada Prezesów wydała niniejszą opinię zgodnie ze zdaniem pierwszym art. 17 ust. 5 Regulaminu Europejskiego Banku Centralnego.

1. Uwagi ogólne

1.1. EBC popiera proponowane rozporządzenie, które jest ważną reformą mającą na celu uproszczenie i usprawnienie stosowania zbioru przepisów dotyczących sektora cyfrowego w Unii. W zakresie, w jakim proponowane rozporządzenie skutecznie przyczyni się do realizacji celów polegających na promowaniu polityk wzmacniających konkurencyjność Unii oraz zmniejszeniu obciążeń regulacyjnych dla obywateli, przedsiębiorstw i administracji, usunie ono przeszkody w świadczeniu usług i wesprze rozwój gospodarki cyfrowej w Unii, uwzględniając jednocześnie konieczność utrzymania najwyższych standardów w zakresie promowania wartości Unii, w tym przestrzegania praw podstawowych. Gospodarka cyfrowa zyskuje na znaczeniu i może mieć wpływ na prowadzenie polityki pieniężnej, ponieważ wpływa na otoczenie, w którym polityka pieniężna funkcjonuje, zmieniając strukturę konsumpcji i produkcji, modele biznesowe oraz ceny względne w sposób zróżnicowany w obrębie strefy euro i poszczególnych państw członkowskich. Zmiany te mają istotny wpływ na zmienne istotne dla polityki pieniężnej i ich pomiar, w tym na zatrudnienie, wydajność, produkcję potencjalną i inflację. Wpływają one również na sposób transmisji decyzji dotyczących polityki pieniężnej do gospodarstw domowych i przedsiębiorstw, co zwiększa niepewność i złożoność sytuacji, z jaką borykają się decydenci.

1.2. W szczególności EBC z zadowoleniem przyjmuje propozycje dotyczące uproszczenia zasad udostępniania danych przedsiębiorstwom przez organy administracji oraz organom administracji przez przedsiębiorstwa, a także przepisów regulujących przetwarzanie danych osobowych zawartych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/2854 ([2]) (zwanym dalej „aktem w sprawie danych"). EBC w szerokim zakresie uczestniczy w gromadzeniu, opracowywaniu, tworzeniu i rozpowszechnianiu danych, które wykorzystuje do realizacji zadań i działań wchodzących w zakres jego kompetencji. Kompetencje te obejmują, w razie potrzeby, zbieranie informacji statystycznych w celu wykonywania zadań Europejskiego Systemu Banków Centralnych (ESBC) na mocy art. 5 Statutu ESBC. EBC jest również zaangażowany w wiele wspólnych inicjatyw wspierających wymianę danych i współpracę z innymi instytucjami, organami i jednostkami organizacyjnymi Unii, a także z właściwymi

([1]) COM (2025) 837 final.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.U. L 2023/2854 z 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

organami państw członkowskich, państw trzecich i organizacji międzynarodowych. Wykonując swoje zadania, EBC może również w pewnych okolicznościach przetwarzać dane osobowe zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725 ([3]) (zwanym dalej „rozporządzeniem 2018/1725"). Z tych powodów EBC popiera środki, które przyczynią się do stworzenia spójnych i jednolitych ram regulacyjnych wspierających dostępność i wykorzystanie danych.

1.3. EBC jest również odpowiedzialny za zapewnienie zgodności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 ([4]) (zwanym dalej „rozporządzeniem DORA") w odniesieniu do instytucji kredytowych sklasyfikowanych jako istotne zgodnie z art. 6 ust. 4 rozporządzenia Rady (UE) nr 1024/2013 ([5]), zgodnie z uprawnieniami i zadaniami w zakresie nadzoru ostrożnościowego przyznanymi na mocy tego rozporządzenia ([6]). W ramach tej funkcji EBC otrzymuje od istotnych instytucji kredytowych zgłoszenia kierowane do ich właściwych organów krajowych dotyczące poważnych incydentów związanych z technologiami informacyjno-komunikacyjnymi (zwanych dalej „incydentami związanymi z ICT") oraz istotnych cyberzagrożeń. Ponadto jednym z podstawowych zadań ESBC jest wspieranie należytego funkcjonowania systemów płatniczych, zgodnie z art. 127 ust. 2 tiret czwarte Traktatu, który znajduje odzwierciedlenie w art. 3.1 Statutu ESBC. W tym kontekście EBC otrzymuje zgłoszenia dotyczące incydentów od instytucji płatniczych i instytucji pieniądza elektronicznego, a także od instytucji kredytowych, zgodnie z rozporządzeniem DORA. W świetle tych obowiązków i zadań EBC zasadniczo z zadowoleniem przyjmuje wysiłki na rzecz dalszego uproszczenia i harmonizacji ram zgłaszania incydentów związanych z ICT w Unii oraz wdrożenia scentralizowanego zgłaszania poważnych incydentów związanych z ICT. Ponieważ sektor finansowy odgrywa wiodącą rolę we wdrażaniu zharmonizowanych, kompleksowych i skutecznych ram zgłaszania incydentów, EBC popiera działania, które ułatwiają przestrzeganie wymogów dotyczących zgłaszania incydentów, opierając się na doświadczeniach zdobytych w sektorze finansowym.

1.4. EBC ma jednak wątpliwości co do stopnia, w jakim proponowane rozporządzenie przyczyniłoby się do realizacji celu w postaci uproszczenia w tych przypadkach, w których nie zmniejsza ono obciążenia związanego z przestrzeganiem przepisów, z jakim mierzą się przedsiębiorstwa i organy publiczne. W związku z tym EBC przedstawia w niniejszej opinii pewne szczegółowe uwagi techniczne i sugestie dotyczące proponowanego rozporządzenia.

1.5. Ze względu na te wątpliwości EBC z zadowoleniem przyjmuje również fakt, że Komisja przeprowadzi ocenę głównych rozdziałów aktu w sprawie danych do dnia 12 września 2028 r., a nowych rozdziałów – w ciągu pięciu lat od wejścia w życie proponowanego rozporządzenia ([7]). Podobnie ważne jest, aby klauzula przeglądowa zawarta w rozporządzeniu DORA ([8]) pozostała niezmieniona, zobowiązując Komisję do przeprowadzenia przeglądu i przedłożenia sprawozdania z funkcjonowania wielu aspektów tego rozporządzenia. Proces przeglądu powinien zapewnić dalsze skuteczne funkcjonowanie odnośnych przepisów, aby służyły one ich celom, wspierając tym samym rozwój gospodarki cyfrowej w Unii.

2. **Przepisy dotyczące sektora cyfrowego**

2.1. EBC w pełni popiera proponowane rozporządzenie jako pierwszy krok w kierunku uproszczenia zbioru przepisów dotyczących sektora cyfrowego i usprawnienia ich stosowania. Zbiór przepisów dotyczących sektora cyfrowego, który powstał na przestrzeni lat w obszarach danych, sztucznej inteligencji, platform internetowych, ochrony danych i cyberbezpieczeństwa, stał się złożony i zawiera obecnie fragmentaryczne i nakładające się na siebie przepisy, które powodują niepewność zarówno dla organów publicznych, jak i przedsiębiorstw.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 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.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([5]) Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz.U. L 287 z 29.10.2013, s. 63, ELI: http://data.europa.eu/eli/reg/2013/1024/oj).

([6]) Art. 46 lit. a) rozporządzenia DORA.

([7]) Art. 1 pkt 26 proponowanego rozporządzenia zmieniający art. 49 aktu w sprawie danych. Zob. także pkt 1.2 opinii Europejskiego Banku Centralnego CON/2022/30 z dnia 5 września 2022 r. w sprawie wniosku dotyczącego rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) (Dz.U. C 402 z 19.10.2022, s. 5).

([8]) Art. 58 rozporządzenia DORA.

2.2. Konsolidacja w akcie w sprawie danych zasad określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/868 ([9]) dotyczących ponownego wykorzystywania chronionych danych będących w posiadaniu podmiotów sektora publicznego w państwach członkowskich oraz zasad określonych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/1024 ([10]) dotyczących ponownego wykorzystywania dokumentów będących w posiadaniu organów sektora publicznego państw członkowskich lub przedsiębiorstw publicznych zapewnia bardziej spójną strukturę i bardziej jednolite definicje kluczowych terminów, ułatwiając stosowanie zasad dotyczących udostępniania danych. Ponadto uchylono zdezaktualizowane przepisy, zwłaszcza te zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1807 ([11]).

2.3. Dla krajowych banków centralnych (KBC), które zazwyczaj są organami sektora publicznego państw członkowskich i w związku z tym podlegają przepisom mającym na celu ułatwienie ponownego wykorzystania danych, stanowi to pożądane uporządkowanie. EBC i KBC odniosą również korzyści z jaśniejszych rozwiązań dotyczących dostępności danych, w szczególności źródeł otwartych danych, które zostały sklasyfikowane jako zbiory danych o wysokiej wartości ([12]). Zbiory te są szeroko wykorzystywane przez EBC przy wykonywaniu zadania wynikającego z art. 5 ust. 1 Statutu ESBC polegającego na gromadzeniu informacji statystycznych niezbędnych do wykonywania zadań ESBC.

2.4. Przykładowo informacje dotyczące przedsiębiorstw i ich struktury własnościowej są wykorzystywane do prowadzenia Rejestru Danych Instytucji i Podmiotów Powiązanych (RIAD), który jest wspólnym zbiorem danych referencyjnych o prawnych oraz innych statystycznych jednostkach instytucjonalnych; gromadzenie tych danych wspiera procesy biznesowe w całym Eurosystemie oraz wykonywanie zadań ESBC i Jednolitego Mechanizmu Nadzorczego (SSM) ([13]). W przypadku gdy EBC może polegać na otwartych danych, tj. danych w otwartym formacie, które mogą być swobodnie wykorzystywane, ponownie wykorzystywane i udostępniane przez dowolną osobą w dowolnym celu ([14]), jest on w stanie zmniejszyć obciążenie podmiotów sprawozdających związane z przekazywaniem takich danych oraz udostępniać te informacje bez ograniczeń w ramach ESBC oraz innym organom publicznym, z którymi współpracuje. EBC z zadowoleniem przyjmuje fakt, że rozwiązania dotyczące udostępniania danych i dokumentów przez organy administracji przedsiębiorstwom ([15]) pozostają bez uszczerbku dla unijnego systemu prawnego wykluczającego dostęp do danych i dokumentów szczególnie chronionych ze względu na poufność informacji statystycznych i tajemnicę służbową.

2.5. W proponowanym rozporządzeniu wprowadzono istotną zmianę ([16]) dotyczącą obowiązku udostępniania danych przez posiadaczy danych EBC – a także innym organom sektora publicznego, Komisji oraz organom Unii – w przypadku wystąpienia wyjątkowej potrzeby wykorzystania tych danych ([17]). Postanowienie to umożliwia EBC zwrócenie się do podmiotów posiadających dane o ich udostępnienie, jeżeli jest to konieczne w celu zareagowania na sytuację niebezpieczeństwa publicznego lub w przypadku wykazania wyjątkowej potrzeby. Ponieważ termin „posiadacze danych" został zdefiniowany szeroko ([18]), przepis ten pozwala EBC na gromadzenie danych w tych wyjątkowych przypadkach od szerszego kręgu osób niż jest to dozwolone w sytuacji, gdy EBC gromadzi

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

([10]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 172 z 26.6.2019, s. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.U. L 303 z 28.11.2018, s. 59), ELI: http://data.europa.eu/eli/reg/2018/1807/oj).

([12]) Zgodnie z art. 13 ust. 1 dyrektywy w sprawie otwartych danych kategorie tematyczne zbiorów danych o wysokiej wartości obejmują dane geoprzestrzenne, dane dotyczące obserwacji Ziemi i środowiska, dane meteorologiczne, dane statystyczne, dane dotyczące przedsiębiorstw i ich własności oraz dane dotyczące mobilności. Zgodnie z art. 13 ust. 2 Komisja jest uprawniona do przyjmowania aktów delegowanych w celu wprowadzania zmian w załączniku I poprzez dodawanie nowych tematycznych kategorii zbiorów danych o wysokiej wartości, aby odzwierciedlić rozwój technologii i rynku.

([13]) Wytyczne Europejskiego Banku Centralnego (UE) 2018/876 z dnia 1 czerwca 2018 r. w sprawie Rejestru Danych Instytucji i Podmiotów Powiązanych (EBC/2018/16) (Dz.U. L 154 z 18.6.2018, s. 3, ELI: http://data.europa.eu/eli/guideline/2018/876/oj).

([14]) Zob. motyw 16 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 172 z 26.6.2019, s. 56, ELI: http://data.europa.eu/eli/dir/2019/1024/oj).

([15]) Art. 1 pkt 18 proponowanego rozporządzenia, wprowadzający nowy rozdział VIIc do aktu w sprawie danych.

([16]) Art. 1 ust. 7 proponowanego rozporządzenia, wprowadzający nowy art. 15a do aktu w sprawie danych.

([17]) Art. 14 i 15 aktu w sprawie danych.

([18]) Termin „posiadacz danych" jest zdefiniowany w art. 2 ust. 13 aktu w sprawie danych i oznacza osobę fizyczną lub prawną, która ma prawo lub obowiązek – zgodnie z tym rozporządzeniem, mającym zastosowanie prawem Unii lub prawem krajowym przyjętym zgodnie z prawem Unii – wykorzystywać i udostępniać dane, w tym – o ile zostało to przewidziane umową – dane z produktu lub dane z usługi powiązanej pobrane lub wygenerowane przez nią podczas świadczenia powiązanej usługi.

informacje statystyczne na podstawie swoich dotychczasowych uprawnień. EBC może gromadzić informacje statystyczne wyłącznie od członków populacji sprawozdawczej zdefiniowanej w rozporządzeniu Rady (WE) nr 2533/98 ([19]), którzy należą przede wszystkim do sektora „instytucji finansowych" zdefiniowanego w europejskim systemie rachunków ([20]) lub są osobami prawnymi i fizycznymi, które posiadają określone pozycje finansowe lub zawierają transakcje finansowe.

2.6. Jak już wcześniej stwierdził EBC, umożliwienie organom władzy publicznej dostępu do danych pochodzących od prywatnych posiadaczy danych i ich wykorzystywania do określonych celów leżących w interesie publicznym przynosi znaczne korzyści ([21]). Wykonując swoje zadania w zakresie polityki pieniężnej, EBC w szerokim zakresie korzysta nie tylko z oficjalnych statystyk sporządzanych przez siebie przy wsparciu KBC i europejskiego systemu statystycznego, ale również z nieoficjalnych i nietradycyjnych źródeł danych. Dane nietradycyjne mogą pochodzić na przykład z informacji o cenach o wysokiej częstotliwości, wskaźników mobilności ludności lub innych źródeł danych, które niekoniecznie znajdują się w posiadaniu instytucji finansowych. EBC jest uprawniony do żądania tych danych od prywatnych posiadaczy danych wyłącznie w przypadku wystąpienia wyjątkowej potrzeby.

2.7. Główną zmianą, jaką wprowadza proponowane rozporządzenie, jest ograniczenie przypadków, w których uprawnienie to może być wykonywane, do niebezpieczeństwa publicznego, z wyłączeniem innych przypadków, w których może zaistnieć wyjątkowa potrzeba wykorzystania danych. EBC musiałby wykazać wyjątkową potrzebę wykorzystania określonych danych w celu wykonywania swoich ustawowych obowiązków w interesie publicznym w ramach reagowania na niebezpieczeństwo publiczne, łagodzenia go lub wsparcia procesu przywracania stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego.

2.8. EBC popiera cele tych zmian, uznając za słuszne uproszczenie ram wymiany danych między przedsiębiorstwami a organami administracji na podstawie aktu w sprawie danych oraz wyjaśnienie wszelkich niejasności, które mogły pojawić się w przy nakładaniu obowiązków na przedsiębiorstwa. EBC popiera również pogląd, że niezbędne jest zachowanie roli statystyki publicznej na podstawie aktu w sprawie danych, ponieważ zaktualizowane unijne ramy dotyczące statystyki europejskiej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 223/2009 ([22]) nie odnoszą się do niebezpieczeństwa publicznego ([23]).

2.9. W przeciwieństwie jednak do członków europejskiego systemu statystycznego, którzy mogą pod pewnymi warunkami gromadzić dane od prywatnych posiadaczy danych w celu wykonywania swoich zadań statystycznych ([24]), EBC nie ma uprawnień do gromadzenia informacji statystycznych od prywatnych posiadaczy danych, którzy nie są podmiotami sprawozdającymi, z wyjątkiem przypadków, w których zachodzi wyjątkowa potrzeba. W celu pozyskania takich danych. EBC może polegać wyłącznie na mechanizmach umożliwiających przekazywanie danych z europejskiego systemu statystycznego do ESBC. Jeżeli zakres przedmiotowego postanowienia zostanie zawężony tak, aby obejmował wyłącznie niebezpieczeństwo publiczne, niezwykle ważne jest zapewnienie jego sprawnego i jednoznacznego stosowania w sytuacjach nadzwyczajnych, w których potrzebne są dodatkowe źródła danych, aby EBC mógł wykonywać swoje zadania w zakresie zbierania danych statystycznych albo inne zadania w zakresie bankowości centralnej lub nadzoru ostrożnościowego. EBC zaleca zatem dalsze uproszczenie warunków, które muszą być spełnione przez organy władzy publicznej w celu żądania danych, ponieważ przyczyniłoby się to również do zminimalizowania złożoności, z jaką borykają się posiadacze danych podczas weryfikacji, czy warunki te są spełnione.

2.10. Ponadto EBC uważa, że należy podjąć dalsze kroki w celu doprecyzowania definicji „niebezpieczeństwa publicznego". Jednym z elementów tej definicji jest to, że musi ono być „stwierdzone się lub oficjalnie ogłoszone zgodnie z odpowiednimi procedurami przewidzianymi w prawie Unii lub prawie krajowym" ([25]). Ponieważ jednak podstawy prawne w prawie pierwotnym i wtórnym, na których można oprzeć stwierdzenie lub ogłoszenie niebezpieczeństwa publicznego, są niejednolite, należy jaśniej wskazać, że w przypadku takiego stwierdzenia lub

([19]) Art. 2 rozporządzenia Rady (WE) nr 2533/98 z dnia 23 listopada 1998 r. dotyczącego zbierania informacji statystycznych przez Europejski Bank Centralny (Dz.U. L 318 z 27.11.1998, s. 8, ELI: http://data.europa.eu/eli/reg/1998/2533/oj).

([20]) Zob. europejski system rachunków narodowych i regionalnych (ESA 2010) dostępny na stronie internetowej Eurostatu pod adresem www.ec.europa.eu/eurostat.

([21]) Pkt 2.3.1 opinii CON/2022/30.

([22]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich (Dz.U. L 87 z 31.3.2009, s. 164, ELI: http://data.europa.eu/eli/reg/2009/223/oj).

([23]) Motyw 15 proponowanego rozporządzenia.

([24]) Art. 17b rozporządzenia (WE) 223/2009.

([25]) Art. 2 ust. 29 rozporządzenia (WE) 2023/2854.

ogłoszenia definicja „niebezpieczeństwa publicznego" nie wymaga spełnienia żadnych dodatkowych kryteriów – ze względu na konieczność podjęcia pilnych działań w obliczu niebezpieczeństwa publicznego. Przykładowo rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2747 ([26]) umożliwia Radzie uruchomienie trybu podwyższonej czujności dotyczącej rynku wewnętrznego w przypadku zagrożenia kryzysem, który w ciągu kolejnych sześciu miesięcy może przerodzić się w sytuację nadzwyczajną na rynku wewnętrznym. Należy doprecyzować, że jeżeli zadania organu władzy publicznej obejmują łagodzenie niebezpieczeństwa publicznego, zagrożenie niebezpieczeństwem publicznym powinno uzasadniać wyjątkową potrzebę zwrócenia się o dane. Ponadto decyzja Rady 2014/415/UE ([27]) ustanawiająca zintegrowane uzgodnienia dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych w celu zastosowania klauzuli solidarności (art. 222 Traktatu) nie ogranicza zakresu okoliczności, w których decyzja ta ma zastosowanie, do sytuacji wyjątkowych „ograniczonych w czasie" ([28]). Należy zatem doprecyzować, że definicja niebezpieczeństwa publicznego jest w pełni zgodna z sytuacjami, w których na mocy prawa Unii i prawa krajowego stosuje się środki nadzwyczajne, i nie jest od nich bardziej restrykcyjna.

2.11. W odniesieniu do postanowień dotyczących rekompensat ([29]) EBC z zadowoleniem przyjmuje wymóg bezpłatnego udostępniania danych w celu zareagowania na niebezpieczeństwo publiczne, z wyjątkiem sytuacji, gdy posiadacz danych jest mikroprzedsiębiorstwem lub małym przedsiębiorstwem. EBC uważa jednak, że ważne jest zapewnienie, aby – w przypadku gdy organy władzy publicznej uzyskują dostęp do danych będących w posiadaniu podmiotów prywatnych – nie ponosiły one nieracjonalnych kosztów. Ponieważ każdy wniosek o udostępnienie danych służy interesowi publicznemu, dane powinny być udostępniane po kosztach i bez nakładania „rozsądnej marży" ([30]).

3. **Ochrona danych**

3.1. EBC z zadowoleniem przyjmuje zmiany w proponowanym rozporządzeniu, które mają na celu uproszczenie przepisów dotyczących ochrony danych. W obszarach kompetencji EBC istnieje kilka kwestii, które wymagają dalszej analizy, aby osiągnąć cel, jakim jest uproszczenie – zarówno pod względem zmniejszenia obciążeń administracyjnych, jak i zapewnienia skutecznego, terminowego i bezpiecznego zgłaszania incydentów.

3.2. EBC przeprowadza we współpracy z KBC szeroki zakres operacji przetwarzania danych osobowych. Ponadto EBC współpracuje z właściwymi organami krajowymi w zakresie prowadzenia czynności przetwarzania danych osobowych w dziedzinie nadzoru bankowego. Jako instytucja Unii EBC przetwarza dane osobowe zgodnie z rozporządzeniem 2018/1725, natomiast KBC i właściwe organy krajowe przetwarzają dane osobowe zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([31]) (zwanym dalej „rozporządzeniem RODO").

3.3. W przypadkach gdy EBC i KBC lub właściwe organy krajowe wspólnie określają cele i sposoby przetwarzania danych osobowych, takiego przetwarzania dokonują jako współadministratorzy ([32]). Natomiast w przypadku gdy jeden podmiot określa cele i sposoby przetwarzania, a drugi przetwarza dane osobowe w jego imieniu, stosunek między nimi jest stosunkiem między administratorem a podmiotem przetwarzającym ([33]). W obu przypadkach EBC przetwarza dane osobowe na podstawie rozporządzenia 2018/1725, natomiast KBC i właściwe organy krajowe przetwarzają dane osobowe na podstawie rozporządzenia RODO. W związku z tym ta sama operacja przetwarzania jest jednocześnie regulowana dwoma odrębnymi, ale uzupełniającymi się instrumentami prawnymi Unii.

([26]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2747 z dnia 9 października 2024 r. w sprawie ustanowienia ram środków dotyczących sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego oraz w sprawie zmiany rozporządzenia Rady (WE) nr 2679/98 (akt o sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego) (Dz.U. L 2024/2747 z 8.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2747/oj).

([27]) Decyzja Rady 2014/415/UE z dnia 24 czerwca 2014 r. w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności (Dz.U. L 192 z 1.7.2014, s. 53, ELI: http://data.europa.eu/eli/dec/2014/415/oj).

([28]) Art. 2 ust. 29 rozporządzenia (WE) 2023/2854.

([29]) Art. 1 pkt 12 proponowanego rozporządzenia zastępujący art. 20 aktu w sprawie danych.

([30]) Zob. pkt 2.3. opinii CON/2022/30.

([31]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([32]) W rozumieniu art. 26 rozporządzenia RODO i art. 28 rozporządzenia 2018/1725.

([33]) W rozumieniu art. 28 rozporządzenia RODO i art. 29 rozporządzenia 2018/1725.

3.4. Jednym z takich przykładów jest sytuacja, w której zarówno EBC, jak i KBC korzystające z usługi natychmiastowego rozliczania płatności w systemie TARGET (TIPS) przetwarzają dane osobowe w ramach systemu TIPS. W takim przypadku zawarto porozumienie o współadministrowaniu. Podobnie przetwarzanie danych osobowych w kontekście przyszłego cyfrowego euro może wymagać zawarcia umowy lub porozumienia o ochronie danych między EBC a KBC strefy euro.

3.5. Przy wykonywaniu zadań ESBC i SSM we współpracy z KBC i właściwymi organami krajowymi niezwykle ważne dla EBC jest, aby akty prawne regulujące przetwarzanie danych osobowych były w jak największym stopniu ujednolicone i wzajemnie zgodne. EBC z zadowoleniem przyjmuje zatem fakt, że proponowane zmiany rozporządzenia RODO i rozporządzenia 2018/1725 są wprowadzane równolegle, co przyczynia się do ustanowienia spójnych i jednolitych ram prawnych. Dzięki temu rozbieżne terminy wejścia w życie i rozpoczęcia stosowania tych aktów prawnych nie powodują niepewności prawa.

3.6. W związku z tym, w świetle współpracy EBC z KBC i właściwymi organami krajowymi w zakresie przetwarzania danych osobowych, gdy jest to konieczne do wykonywania zadań ESBC i SSM, EBC przedstawia następujące kwestie do rozważenia:

3.7. W odniesieniu do mechanizmu pojedynczego punktu kontaktowego EBC zaleca upoważnienie współadministratorów do zgłaszania naruszeń ochrony danych osobowych w imieniu wszystkich współadministratorów ([34]). Jest to możliwe, ponieważ proponowane rozporządzenie wprowadza zharmonizowany pojedynczy punkt kontaktowy, za pośrednictwem którego podmioty mogą, w drodze jednego zgłoszenia, jednocześnie wypełniać swoje obowiązki w zakresie zgłaszania incydentów wynikające z wielu aktów prawnych Unii. Dzięki wdrożeniu zasady „zgłoś raz, udostępnij wielu" pojedynczy punkt kontaktowy ma na celu zmniejszenie obciążeń administracyjnych dla podmiotów przy jednoczesnym zapewnieniu skutecznego, terminowego i bezpiecznego zgłaszania incydentów. W tym celu pojedynczy punkt kontaktowy ma służyć jako wspólny kanał przekazywania powiadomień na podstawie kilku aktów prawnych ([35]). Jak już wcześniej stwierdził EBC, zdecydowanie popiera on wymianę informacji między organami, aby umożliwić międzysektorowy proces uczenia się, przyczynić się do zapobiegania cyberatakom i skutecznego zarządzania nimi oraz promować spójną ocenę ryzyka związanego z technologiami teleinformatycznymi w całej Unii ([36]). W tym kontekście EBC popiera wprowadzenie pojedynczego punktu kontaktowego w kontekście zgłaszania naruszeń ochrony danych osobowych.

3.8. Stosując mechanizm pojedynczego punktu kontaktowego do wspólnych czynności przetwarzania prowadzonych przez EBC we współpracy z KBC (i właściwymi organami krajowymi), KBC odniosłyby korzyść na mocy proponowanego rozporządzenia z pojedynczego punktu kontaktowego do przyjmowania powiadomień o incydentach. Z drugiej strony EBC, jako instytucja Unii, nadal korzystałby na mocy proponowanego rozporządzenia z kanału zgłaszania ustanowionego w rozporządzenia 2018/1725, w ramach którego zgłasza incydenty Europejskiemu Inspektorowi Ochrony Danych (EIOD) ([37]).

3.9. EBC ponownie podkreśla potrzebę usprawnienia, przyspieszenia i maksymalizacji wymiany informacji na temat incydentów oraz zapewnienia spójności między rozporządzeniem RODO a rozporządzeniem 2018/1725. W związku z tym rozporządzenie 2018/1725 należy włączyć do aktów prawnych Unii, w odniesieniu do których zachodzi obowiązek stosowania pojedynczego punktu kontaktowego do zgłaszania naruszeń ochrony danych osobowych.

([34]) Zgodnie z wymogami art. 34 rozporządzenia 2018/1725.

([35]) Należą do nich między innymi rozporządzenie RODO oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 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) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj); rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj) oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj) (dyrektywa CER).

([36]) Zob. pkt 3.3.1 opinii Europejskiego Banku Centralnego CON/2022/14 z dnia 11 kwietnia 2022 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 (Dz.U. C 233 z 16.6.2022, s. 22).

([37]) Zgodnie z wymogami art. 34 rozporządzenia 2018/1725.

3.10. W odniesieniu do pojedynczego zgłaszania naruszeń ochrony danych w przypadkach współadministrowania EBC utrzymuje, że współadministratorzy powinni mieć swobodę decydowania, czy korzystają z tej możliwości i na jakich warunkach. EIOD potwierdził niedawno, że do celów ustalenia, czy EBC ma obowiązek powiadomienia EIOD o naruszeniu ochrony danych osobowych, nie ma znaczenia, czy EBC, jako współadministrator, jest odpowiedzialny za to naruszenie. Sam fakt, że EBC jest współadministratorem operacji przetwarzania, w związku z którą doszło do naruszenia ochrony danych osobowych, wystarcza do powstania obowiązku powiadomienia EIOD, jeżeli spełnione są odpowiednie warunki określone w rozporządzeniu 2018/1725 ([38]).

3.11. Należy zauważyć, że w wielu przypadkach, w których obowiązuje porozumienie o współadministrowaniu zawarte między EBC a wszystkimi KBC Eurosystemu, pojedyncze naruszenie ochrony danych osobowych mogłoby skutkować nawet 22 powiadomieniami, których treść najprawdopodobniej byłaby podobna lub identyczna. Taki system byłby sprzeczny z celem, jakim jest uproszczenie obciążeń administracyjnych dla organów publicznych. W związku z tym właściwe jest umożliwienie współadministratorom zgłaszania naruszeń ochrony danych osobowych za pośrednictwem pojedynczego punktu kontaktowego właściwym organom nadzorczym tylko raz. Zgodnie z celem, jakim jest uproszczenie, taki system zgłaszania nie miałby zastosowania w przypadkach, gdy mało prawdopodobne jest, że dane naruszenie ochrony danych osobowych spowoduje zagrożenie dla praw i wolności osób fizycznych ([39]).

3.12. Z tych powodów EBC zaleca pozostawienie współadministratorom decyzji, czy chcą skorzystać z możliwości złożenia jednego powiadomienia w imieniu wszystkich współadministratorów w ramach konkretnego porozumienia o współadministrowaniu oraz na jakich warunkach. Takie powiadomienie byłoby składane jednorazowo za pośrednictwem pojedynczego punktu kontaktowego, a tym samym kierowane do wszystkich odpowiednich organów nadzorczych, bez uszczerbku dla roli, jaką obowiązki w zakresie powiadamiania odgrywają w zapewnianiu pełnej przejrzystości i kompleksowej wymiany informacji.

4. **Zgłaszanie incydentów**

4.1. Jak zauważono w pkt 1.3, EBC z zadowoleniem przyjmuje inicjatywę mającą na celu uproszczenie i ujednolicenie procedur zgłaszania incydentów związanych z ICT oraz wdrożenie scentralizowanego systemu zgłaszania poważnych incydentów związanych z ICT. Powinno to jednak w każdym przypadku zmniejszyć obciążenia administracyjne dla nadzorowanych instytucji kredytowych, instytucji płatniczych, instytucji pieniądza elektronicznego oraz organów publicznych. W związku z tym należy przyznać, że dzięki wdrożeniu rozporządzenia DORA w sektorze finansowym osiągnięto już pewien stopień uproszczenia procedur zgłaszania. Rozporządzenie DORA skutecznie zastąpiło różne wymogi w zakresie zgłaszania incydentów związanych z ICT obowiązujące podmioty finansowe ([40]), co pozwoliło znacznie zmniejszyć obciążenie sprawozdawcze, któremu podlegały, oraz wdrożyć skuteczne i wydajne mechanizmy koordynacji między różnymi właściwymi organami ([41]). Rozporządzenie DORA osiągnęło ten cel dzięki zdefiniowaniu wspólnych taksonomii, wzorów i procedur dokonywania zgłoszeń oraz określeniu pojedynczego punktu wprowadzania tych zgłoszeń.

4.2. Chociaż EBC popiera te wysiłki na rzecz uproszczenia, ma również zastrzeżenia co do niektórych aspektów środków dotyczących zgłaszania incydentów związanych z ICT zawartych w proponowanym rozporządzeniu z trzech głównych powodów.

4.3. Po pierwsze, propozycja utworzenia pojedynczego punktu kontaktowego nie przyczynia się skutecznie do zmniejszenia obciążenia związanego ze zgłaszaniem incydentów dla podmiotów finansowych i innych przedsiębiorstw, które podlegają wymogom w tym zakresie. Chociaż pojedynczy punkt kontaktowy zapewnia istnienie jednego portalu na potrzeby zgłaszania incydentów, nie zmienia to faktu, że nadal istnieją różne taksonomie, wzory i procedury dla każdego zgłoszenia incydentu na podstawie przepisów ram prawnych niż rozporządzenie DORA. Aby zgłosić incydent, podmiot finansowy musi przygotować różne zgłoszenia zgodnie z różnymi przepisami (np. na mocy rozporządzenia RODO i rozporządzenia DORA). Samo umożliwienie

([38]) Opinia nadzorcza EIOD 18/2025 w sprawie projektu porozumienia o współadministrowaniu między Europejskim Bankiem Centralnym a właściwymi organami krajowymi w kontekście Jednolitego Mechanizmu Nadzorczego (sprawa 2024-1002), dostępna na stronie internetowej EIOD pod adresem www.edps.europa.eu.

([39]) Art. 34 rozporządzenia (UE) 2018/1725.

([40]) Zob. w tym kontekście motywy 16, 18, 19 i 23 rozporządzenia DORA.

([41]) Umożliwiło to rozwiązanie kwestii równoległego dokonywania zgłoszeń na mocy rozporządzenia DORA, dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337, 23.12.2015, s. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj) oraz odpowiednich wytycznych EUNB, jak wskazano w pkt 4.2.2 opinii Europejskiego Banku Centralnego CON/2021/20 z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (Dz.U. C 343 z 26.8.2021, s. 1).

przekazywania tych zgłoszeń jednemu odbiorcy nie zmniejsza w znaczący sposób obciążenia administracyjnego. Z tego powodu wskazane jest należyte uwzględnienie regulacyjnych standardów technicznych przyjętych na mocy rozporządzenia DORA w celu usprawnienia i uproszczenia procesów zgłaszania incydentów ([42]). EBC z zadowoleniem przyjąłby również dalsze ujednolicenie i, w stosownych przypadkach, połączenie taksonomii, wzorów i procedur zgłaszania incydentów wynikających z różnych ram prawnych w celu osiągnięcia rzeczywistego uproszczenia.

4.4. Po drugie, zgłoszenie incydentu na podstawie rozporządzenia DORA uruchamia procesy, w których czas ma kluczowe znaczenie i które mogą wiązać się z uruchomieniem procedur kryzysowych. Włączenie nowego podmiotu i systemu do procesu przyjmowania tych zgłoszeń wiąże się z dodatkowym ryzykiem w zakresie dostępności i terminowego przekazywania wymaganych informacji. Z tego powodu najskuteczniejszym i niezawodnym rozwiązaniem jest przesyłanie tych zgłoszeń bezpośrednio do właściwego organu, zgodnie z założeniami rozporządzenia DORA ([43]), w celu uniknięcia nieuzasadnionych opóźnień w reakcji nadzorczej na potencjalnie krytyczną sytuację.

4.5. Po trzecie, należy uwzględnić wysiłki i nakłady poniesione już przez sektor finansowy w związku z wdrażaniem rozporządzenia DORA, które obowiązuje dopiero od 17 stycznia 2025 r. Nadzorowane instytucje kredytowe i właściwe organy zainwestowały znaczne zasoby we wdrożenie nowych ram. Z tej perspektywy korzystne byłoby opóźnienie integracji zgłaszania incydentów związanych z ICT za pośrednictwem pojedynczego punktu kontaktowego. Dałoby to więcej czasu na określenie potencjalnych usprawnień i sposobów dalszego uproszczenia obciążeń administracyjnych zarówno dla SSM, jak i nadzorowanych instytucji kredytowych.

4.6. Z tych powodów EBC proponuje wyłączenie rozporządzenia DORA z zakresu proponowanego rozporządzenia. Właściwe byłoby zdobycie doświadczenia odrębnie w zakresie nowego pojedynczego punktu kontaktowego (obejmującego inne rozporządzenia, w tym rozporządzenie 2018/1725) oraz nowo wdrożonego systemu zgłaszania incydentów na podstawie rozporządzenia DORA, a następnie przeanalizowanie, jak najlepiej je zintegrować na późniejszym etapie.

W przypadku gdy EBC zaleca zmianę proponowanego rozporządzenia, szczegółowe propozycje zmian wraz z ich uzasadnieniem zostały zawarte w odrębnym roboczym dokumencie o charakterze technicznym. Dokument roboczy o charakterze technicznym jest dostępny w języku angielskim na stronie internetowej EUR-Lex.

Sporządzono we Frankfurcie nad Menem dnia 10 marca 2026 r.

Prezes EBC
Christine LAGARDE

([42]) Zgodnie z motywem 54 proponowanego rozporządzenia.
([43]) Art. 19 rozporządzenia DORA.